Nr 30 2024
ISSN 2080-1335

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

ISSN 2080-1335
e-ISSN 2720-0841

Punkty MEiN: 20

Numer zamknięto i oddano do druku w kwietniu 2024 r.

Printed in April 2024

Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego

Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota"
ul. Nadwiślańczyków 2, 05-462 Wiązowna, Poland

Kontakt / Contact
tel. / phone (+48) 22 58 58 613
e-mail: wydawnictwo@abw.gov.pl
www.abw.gov.pl/wyd/

Druk / Print
Biuro Logistyki Agencji Bezpieczeństwa Wewnętrznego
ul. Rakowiecka 2A, 00-993 Warszawa, Poland
tel. (+48) 22 58 57 657

No. 30 2024
ISSN 2080-1335

INTERNAL SECURITY REVIEW

Recenzji są poddawane materiały zamieszczone w dziale Artykuły oraz artykuły recenzyjne zamieszczone w dziale Artykuły recenzyjne/recenzje

Material posted in the Articles section and review articles posted in the Review Articles/Reviews section are subject to peer-reviewed

Artykuły wyrażają poglądy autorów

Articles express the views of the authors

Deklaracja o wersji pierwotnej / Declaration of the original version

Wersja drukowana czasopisma jest jego wersją pierwotną

The printed version of the journal is the original version

Wersja online czasopisma jest dostępna na stronie: www.abw.gov.pl/wyd/

The online version of the journal is available at: www.abw.gov.pl/pub/

Indeksacja w bazach danych / Indexing in databases

„Przegląd Bezpieczeństwa Wewnętrznego" (PBW) znajduje się w bazach: Index Copernicus Journal Master List z liczbą 94,73 punktów, ERIH PLUS, Central European Journal of Social Science and Humanities i Polska Bibliografia Naukowa (PBN)

"Internal Security Review" can be found in the following databases: Index Copernicus Journal Master List with 94,73 points, ERIH PLUS, Central European Journal for Social Science and Humanities, Polish Scientific Bibliography

PBW jest dostępny w Portalu Czasopism Naukowych Uniwersytetu Jagiellońskiego pod adresem: https://www.ejournals.eu/PBW/

The journal is available on the Jagiellonian University Scientific Journals Portal at: https://www.ejournals.eu/PBW/

Materiały do PBW należy składać przez panel redakcyjny dostępny pod adresem: https://ojs.ejournals.eu/PBW/about/submissions

Articles should be submitted via the editorial tab available at: https://ojs.ejournals.eu/PBW/about/submissions

SPIS TREŚCI

PRACE KONKURSOWE

VARIA

ARTICLES

Szanowni Czytelnicy!

W 30. numerze „Przeglądu Bezpieczeństwa Wewnętrznego" mamy przyjemność zaprezentować Państwu kilka interesujących artykułów, które – ze względów geostrategicznych – koncentrują się na zagrożeniu bezpieczeństwa Rzeczpospolitej płynącym ze wschodu. Proponujemy m.in. ciekawą analizę dotyczącą tzw. buntu Prigożyna, stanowiącego jedną z największych zagadek wojny w Ukrainie, charakterystykę aktywności informacyjnej Federacji Rosyjskiej, opis metod obchodzenia przez to państwo unijnych sankcji finansowych, jak również próbę wyjaśnienia jednej z najbardziej makiawelicznych operacji w dziejach wywiadu w postaci przejęcia niemal całej kadry krymskiej Służby Bezpieczeństwa Ukrainy przez rosyjską służbę wewnętrzną. W tematykę zagrożeń zewnętrznych – pośrednio – wpisuje się także tekst poświęcony prawnym aspektom nowelizacji polskiego Kodeksu karnego w zakresie przestępstwa szpiegostwa.

Warto przypomnieć, że „Przegląd Bezpieczeństwa Wewnętrznego" obchodzi jubileusz 15-lecia istnienia. Od ponad dekady nasz półrocznik stara się być platformą wymiany myśli między społecznością służb specjalnych a światem akademickim. Jesteśmy jedynym czasopismem branżowym zajmującym się działalnością tych służb sensu largo i dysponujemy – jako periodyk wydawany przez największą służbę specjalną RP – potencjałem, by moderować dyskurs publiczny w tym obszarze, łącząc dorobek naukowy z praktycznym doświadczeniem. Agencja Bezpieczeństwa Wewnętrznego jest bowiem źródłem wiedzy na temat rzeczywistych zagrożeń bezpieczeństwa państwa. Bez nałożenia na te dane teorii naukowych trudno jednak wyciągać szersze wnioski i formułować prognozy. Z kolei badania naukowe pozbawione podstaw faktograficznych i wiedzy źródłowej nabierają charakteru spekulacyjnego i akademickiego, odrywając się od rzeczywistości. Połączenie tych dwóch perspektyw pozwala uzyskać efekt komplementarności i synergii. To dlatego przyświeca nam idea bycia

hubem integrującym różne środowiska zainteresowane problematyką bezpieczeństwa państwa i propagującym wiedzę w tym zakresie. Jesteśmy bowiem przekonani, że dla służby specjalnej najgorsze jest zastygnięcie w zastanych formach – bycie reaktywną, pozbawioną kreatywności i usztywnioną przez biurokratyczne procedury częścią administracji publicznej. „Przegląd Bezpieczeństwa Wewnętrznego" jest – w naszej ocenie – jednym z niezbędnych elementów stałego rozwoju tych służb oraz ewolucji paradygmatu ich działania zamiast bezrefleksyjnego powielania dogmatów operacyjno-analitycznych i organizacyjnych. Aby osiągnąć tak ambitny cel, staramy się maksymalnie poszerzać tematykę poruszaną na naszych łamach, zapraszając do współpracy specjalistów z wielu dziedzin, a nie tylko wąsko pojmowanych nauk o bezpieczeństwie. Wychodzimy z założenia, że problematyka związana ze służbami specjalnymi ex definitione jest multidyscyplinarna. W ciągu 15 lat udało się skupić wokół czasopisma grupę ludzi, którzy próbują implementować w działalności tych służb nowe podejścia teoretyczne, a także zasilać świat akademicki wiedzą czerpaną z doświadczeń oficerów operacyjnych i analitycznych. Mamy nadzieję, że to grono będzie się stale poszerzać i rozwijać platformę służącą intensyfikowaniu interakcji między służbami specjalnymi a środowiskami eksperckimi i naukowymi.

Jednocześnie składamy podziękowania wszystkim osobom, które przez te lata współtworzyły nasze czasopismo – redaktorom naczelnym, członkom Rady Naukowej, sekretarzom redakcji, recenzentom, autorom i członkom zespołu redakcyjnego. Bez Was, Waszej pracy i ogromnego zaangażowania nie byłoby „Przeglądu Bezpieczeństwa Wewnętrznego". To Wy byliście architektami jego dorobku i gwarantami wysokiej jakości. Dziękujemy również Czytelnikom, z których część towarzyszy nam niemal od początku. Wierzymy, że nasze czasopismo nadal będzie ważnym i potrzebnym głosem w dyskusji o służbach specjalnych demokratycznej Rzeczpospolitej.

Redaktor naczelny
dr Marek Świerczek

ARTYKUŁY

Bunt Prigożyna – przyczyny, przebieg i konsekwencje rebelii Grupy Wagnera

Prigozhin's mutiny - causes, course and consequences of the Wagner Group rebellion

FILIP BRYJKA

Instytut Studiów Politycznych Polskiej Akademii Nauk
Polski Instytut Spraw Międzynarodowych
https://orcid.org/0000-0002-8613-1030

Przegląd Bezpieczeństwa Wewnętrznego, 2024, nr 30: 13–48

https://doi.org/10.4467/20801335PBW.24.001.19603

ARTYKUŁ

Abstrakt

Autor poszukuje odpowiedzi na pytanie, w jaki sposób bunt Prigożyna wpłynął na pozycję Grupy Wagnera w Rosji. Uwzględnia przede wszystkim wydarzenia, do których doszło w nocy z 23 na 24 czerwca 2023 r., gdy najemnicy kierowani przez Jewgienija Prigożyna przeprowadzili tzw. marsz sprawiedliwości przeciwko Ministerstwu Obrony. Celem artykułu jest udzielenie odpowiedzi na trzy szczegółowe pytania badawcze: 1) jakie czynniki doprowadziły do rebelii Grupy Wagnera? 2) jaka była reakcja rosyjskich władz na te wydarzenia? 3) jakie są konsekwencje buntu Prigożyna dla stabilności reżimu Putina, a także kierownictwa Grupy Wagnera i całej formacji zbrojnej? Autor, poszukując odpowiedzi na te pytania, koncentruje się na relacjach Prigożyna z rosyjskimi elitami wojskowymi. Następnie przedstawia przebieg rebelii oraz reakcję Kremla na te wydarzenia. Omawia ponadto konsekwencje buntu zarówno wewnątrz Rosji, jak i w skali międzynarodowej.

Słowa kluczowe

Grupa Wagnera, najemnicy, zagrożenia hybrydowe, rosyjskie służby specjalne

Abstract

The author seeks answers to the question of how the Prighozin's mutiny affected the position of the Wagner Group in Russia. He mainly takes into account the events that took place on 23-24 June 2023, when the mercenaries led by Yevgeny Prigozhin carried out the so-called "march of justice" against the Russian Defense Ministry. The aim of the article is to answer three specific research questions: 1) what factors led to the Wagner Group's rebellion? 2) what was the reaction of the Russian government to these events? 3) what are the consequences of Prigozhin's rebellion for the stability of Putin's regime, the Wagner Group leadership and the organisation as a whole? In seeking answers to these questions, the author focuses on Prigozhin's relations with the Russian military elite. He then presents the course of the rebellion and the Kremlin's reaction to these events. The author further discusses the consequences of the rebellion both within Russia and internationally.

Keywords

Wagner Group, mercenaries, hybrid threats, Russian secret services

W nocy z 23 na 24 czerwca 2023 r. szef Grupy Wagnera Jewgienij Prigożyn przeprowadził rebelię przeciwko rosyjskiemu Ministerstwu Obrony (Министерство обороны Российской Федерации). Nieudana próba przejęcia kontroli nad resortem przez grupę najemników[1] była punktem kulminacyjnym narastającego od połowy 2022 r. konfliktu personalnego między Prigożynem a ministrem obrony gen. Siergiejem Szojgu i szefem Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (Генеральный штаб Вооружённых сил Российской Федерации)

[1] Autor celowo nazywa członków Grupy Wagnera najemnikami, by podkreślić ich finansową motywację. Z punktu widzenia prawa międzynarodowego wagnerowcy na ogół (zwłaszcza w Syrii i Afryce) spełniają kryteria pozwalające uznać ich za najemników zgodnie z art. 47 I protokołu dodatkowego do konwencji genewskich (*Protokoły dodatkowe do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół I) oraz dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych (Protokół II), sporządzone w Genewie dnia 8 czerwca 1977 r.*), i w związku z tym nie mają prawa do statusu kombatantów. W przypadku wojny w Ukrainie obywatele Rosji (strony konfliktu) z Grupy Wagnera mogą być kwalifikowani jako „milicja lub inna formacja ochotnicza należąca do strony konfliktu" zgodnie z art. 4 III konwencji genewskiej (*Konwencje o ochronie ofiar wojny, podpisane w Genewie dnia 12 sierpnia 1949 roku*). Uwzględniając liczne naruszenia praw człowieka i zbrodnie wojenne (np. mordowanie jeńców w Ołeniwce, współudział w masakrze w Buczy i czystki etniczne na terenach okupowanych), nie spełniają jednak warunku „przestrzegania w swych działaniach praw i zwyczajów wojny". W tym wypadku strona ukraińska może uznać ich za tzw. bezprawnych kombatantów (ang. *unlawful combatants*), co nie daje im przywilejów wynikających ze statusu kombatanta.

gen. Walerijem Gierasimowem[2]. Działania te można uznać za przejaw wygórowanych ambicji politycznych Prigożyna, niewłaściwej oceny własnej pozycji w strukturach władzy i próbę utrzymania niezależności od wojska kierowanej przez niego grupy paramilitarnej. W dniu 10 czerwca 2023 r. gen. Szojgu oznajmił, że od 1 lipca wszystkie nieregularne formacje zbrojne walczące w Ukrainie, czyli bataliony ochotnicze i tzw. prywatne firmy wojskowe, PFW (ang. Private Military Companies, PMCs; ros. Частная Военная Компания, ЧВК)[3] zostaną objęte bezpośrednią kontrolą Ministerstwa Obrony. Szef Grupy Wagnera konsekwentnie sprzeciwiał się podporządkowaniu ich armii i bezskutecznie próbował wynegocjować umowę pozwalającą na zachowanie pewnej autonomii operacyjnej.

Administracji prezydenta Władimira Putina przy mediacji Alaksandra Łukaszenki udało się zażegnać najpoważniejszy od czasów puczu Janajewa kryzys wewnętrzny w Rosji. Nieposłuszeństwo Prigożyna – wieloletniego protegowanego Putina – uwidoczniło pogłębiające się podziały w rosyjskich strukturach siłowych. Chociaż bunt wagnerowców był wymierzony w część elit wojskowych, to miał poważne konsekwencje wizerunkowe dla samego prezydenta i utworzonego przez niego systemu władzy. Rebelia jest także sygnałem tego, że rosnące koszty rosyjskiej inwazji na Ukrainę zaczynają negatywnie oddziaływać na stabilność reżimu, który zaostrza wewnętrzne mechanizmy kontroli i represji, aby nie okazać słabości.

Wbrew częstym opiniom publicystów i komentatorów[4] pucz i przerzucenie Grupy Wagnera na Białoruś nie były grą operacyjną rosyjskich służb specjalnych,

---

[2] A. Legucka, F. Bryjka, *Rywalizacja między rosyjską armią a Grupą Wagnera*, PISM, 6 VI 2023 r., https://www.pism.pl/publikacje/rywalizacja-miedzy-rosyjska-armia-a-grupa-wagnera [dostęp: 6 VI 2023].

[3] W przypadku Rosji tego rodzaju formacje najczęściej nie spełniają kryteriów pozwalających zakwalifikować je jako PFW, które zgodnie z Konstytucją FR (art. 13 § 5 i art. 71) oraz Kodeksem karnym (art. 208 i art. 359) są nielegalne. Rosja nie jest także sygnatariuszem dokumentu z Montreux, będącym próbą regulacji funkcjonowania PFW. Sformułowana w nim definicja mówi o defensywnym charakterze tego rodzaju podmiotów. Zakres zadań realizowanych przez kontraktorów powinien obejmować według niej „ochronę osób i obiektów (…), utrzymanie i obsługę systemów uzbrojenia; przetrzymywanie więźniów; doradztwo i szkolenie lokalnych sił bezpieczeństwa". Zadania realizowane przez Grupę Wagnera często wykraczają poza ten katalog i mają charakter ofensywny – polegają m.in. na destabilizowaniu innych państw, prowadzeniu tajnych operacji bojowych, paramilitarnych, wywiadowczych, dywersyjno-sabotażowych itp. Grupy Wagnera nie można traktować jako PFW również dlatego, że zatrudnia osoby karane. Zob. szerzej: F. Bryjka, *Grupa Wagnera – paramilitarne narzędzie rosyjskich operacji hybrydowych*, „Sprawy Międzynarodowe" 2022, t. 75, nr 2, s. 68–91. https://doi.org/10.35757/SM.2022.75.2.05.

[4] Przegląd wykluczających się hipotez sugerujących, że bunt Prigożyna mógł być operacją specjalną rosyjskiego wywiadu przedstawił Adam Jawor. Zob. tegoż, *Rosyjskie służby po buncie Prigożyna. Putin wyrównuje szeregi w kremlowskich wieżach*, InfoSecurity24, 31 VII 2023 r.,

lecz działaniem ad hoc, mającym ograniczyć koszty wizerunkowe rebelii. Pozwoliło także władzom na Kremlu uporządkować kwestie związane z przejęciem aktywów Prigożyna w Rosji, Syrii i Afryce. Śmierć szefa Grupy Wagnera w katastrofie lotniczej dokładnie dwa miesiące po tzw. marszu sprawiedliwości najprawdopodobniej nie była przypadkowa. Zdrada stanu i nielojalność w rosyjskiej kulturze strategicznej są rozliczane za pomocą operacji likwidacyjnych prowadzonych przez służby specjalne[5]. Według dziennikarzy „The Wall Street Journal" rozkaz pozbycia się przywódcy puczystów (za wiedzą i zgodą Putina) wydał Sekretarz Rady Bezpieczeństwa Federacji Rosyjskiej (FR) Nikołaj Patruszew[6].

Śmierć Prigożyna i głównego dowódcy wagnerowców Dmitrija Utkina ps. „Wagner" rozpoczęła proces głębokiej reorganizacji grupy. Istotne konsekwencje także dla bezpieczeństwa Polski może mieć rozmieszczenie rosyjskich najemników na Białorusi. Za ich pośrednictwem Rosja może bowiem zintensyfikować działania hybrydowe przeciwko państwom wschodniej flanki NATO.

Przyczyny buntu Prigożyna

Bezpośrednim powodem decyzji Prigożyna o marszu na Moskwę był atak rakietowy na pozycje wagnerowców we wschodniej Ukrainie. O jego zaplanowanie szef najemników oskarżył gen. Szojgu, a wykonawstwo przypisał rosyjskim siłom zbrojnym. Chociaż opublikowane nagranie z miejsca zdarzenia nie pozwala jednoznacznie stwierdzić, że celem ataku był obóz najemników, a uderzenie zostało przeprowadzone przez rosyjską armię, dało to pretekst do uzasadnienia rebelii[7]. Działaniom tym towarzyszyły tyrady Prigożyna wymierzone w elity wojskowe, które oskarżał o rozpoczęcie pełnoskalowej inwazji na Ukrainę w celu autopromocji, uzyskania awansów i korzyści materialnych[8]. Prigożyn zakwestionował przy tym

https://infosecurity24.pl/za-granica/rosyjskie-sluzby-po-buncie-prigozyna-putin-wyrownuje-szeregi-w-kremlowskich-wiezach [dostęp: 31 VII 2023].

5 M.R. Gordon i in., *Early Intelligence Suggests Prigozhin Was Assassinated, U.S. Officials Say*, The Wall Street Journal, 24 VIII 2023 r., https://www.wsj.com/world/russia/wagner-prigozhin-russia-assassinated-intelligence-3e456fab [dostęp: 24 VIII 2023].

6 T. Grove, A. Cullison, B. Pancevski, *How Putin's Right-Hand Man Took Out Prigozhin*, The Wall Street Journal, 22 XII 2023 r., https://www.wsj.com/world/russia/putin-patrushev-plan-prigozhin-assassination-428d5ed8?mod=hp_lead_pos7 [dostęp: 26 I 2024].

7 J. Prigożyn, wpis na kanale Telegram, https://t.me/Prigozhin_hat/3797 [dostęp: 23 VI 2023].

8 J. Prigożyn, wpis na kanale Telegram, https://t.me/prigozhin_2023_tg/1844 [dostęp: 23 VI 2023].

rozpowszechniane przez Kreml propagandowe uzasadnienie wojny w Ukrainie, podważając tezę, że (…) *NATO i Ukraina stanowią zagrożenie dla Rosji*[9].

Spór między szefem Grupy Wagnera a kierownictwem Ministerstwa Obrony narastał od połowy 2022 r. Prigożyn wykorzystał militarne niepowodzenia rosyjskiej agresji na Ukrainę do otwartej krytyki resortu i dowódców wojskowych lojalnych wobec gen. Szojgu. Wskazywał m.in. na błędy dowództwa w prowadzeniu operacji wojennej, złą sytuację słabo wyszkolonych i niewłaściwie wyposażonych jednostek. Do ataków informacyjnych wykorzystywał m.in. swoje farmy trolli i opłacanych blogerów wojskowych. Wypowiedzi Prigożyna były długo tolerowane przez Putina, co może świadczyć o tym, że prezydent traktował je jako krytykę braku sukcesów rosyjskiej armii i nacisk na Ministerstwo Obrony[10].

Personalny konflikt między Prigożynem a gen. Szojgu ma swój początek w interwencji Rosji w Syrii (2015–2019), w trakcie której Grupa Wagnera odgrywała rolę głównego komponentu lądowego. Problemem między najemnikami a armią były m.in. kwestie związane z zaopatrzeniem, ogólną niechęcią do współdziałania i rywalizacją o zyski z wydobywania ropy naftowej[11]. Zdaniem Prigożyna wagnerowcy nie zostali wystarczająco nagrodzeni za swój udział w operacji (np. za odbicie Palmiry z rąk dżihadystów). Punktem zapalnym były także wydarzenia z 2018 r., gdy rosyjskie dowództwo wojskowe nie powstrzymało amerykańskiego ataku na kolumnę najemników Grupy Wagnera szturmujących rafinerię Conoco, kontrolowaną przez Syryjskie Siły Demokratyczne. Szacuje się, że zginęło wówczas 200–300 wagnerowców[12]. Amerykański atak nie spotkał się z akcją odwetową ze strony rosyjskich władz, które wypierały się powiązań z najemnikami. W tym czasie gen. Szojgu pozbawił także firmy Prigożyna licznych kontraktów dla wojska, które w latach 2011–2018 przyniosły mu dochód w wysokości 2 mld dolarów. Minister obrony utworzył w 2018 r. własną firmę wojskową Patriot, która konkurowała z Grupą Wagnera o kontrakty w Syrii i Afryce[13].

---

[9] Zob. szerzej: *Sprawa Prigożyna a tuszowanie słabości Rosji i rys na jej wizerunku militarnej potęgi*, EUvsDisinfo, 29 VI 2023 r., https://euvsdisinfo.eu/pl/sprawa-prigozyna-a-tuszowanie-slabosci-rosji-i-rys-na-jej-wizerunku-militarnej-potegi/ [dostęp: 29 VI 2023].

[10] A.M. Dyner, *Znaczenie buntu Prigożyna dla rosyjskiej polityki bezpieczeństwa*, PISM, 26 VI 2023 r., https://www.pism.pl/publikacje/znaczenie-buntu-prigozyna-dla-rosyjskiej-polityki-bezpieczenstwa [dostęp: 26 VI 2023].

[11] Zob. szerzej: M. Gabidullin, *Wagnerowiec. Spowiedź byłego dowódcy tajnej armii Putina*, Kraków 2022.

[12] R. Blakely, *Russian mercenaries killed by US troops in Syria gun battle*, The Times, 14 II 2018 r., https://www.thetimes.co.uk/article/russia-mercenaries-killed-by-us-troops-in-syria-gun-battle-g5zswflfg [dostęp: 19 I 2024].

[13] S. Sukhankin, *Russia's New PMC Patriot: The Kremlin's Bid for a Greater Role in Africa?*, The Jamestown Foundation, 1 VIII 2018 r., https://jamestown.org/program/russias-new-pmc-patriot-the-kremlins-bid-for-a-greater-role-in-africa/ [dostęp: 12 V 2023].

Konflikt między tą organizacją a Ministerstwem Obrony zaostrzył się w połowie 2022 r. wraz z rosnącym zaangażowaniem najemników w wojnę w Ukrainie. Początkowo inwazję wspierało ok. 400 najemników, których zadaniem było zamordowanie prezydenta Wołodymyra Zełenskiego w celu utworzenia rządu marionetkowego w Kijowie[14]. Według rosyjskich dziennikarzy śledczych z portali Meduza i The Insider byli to jednak dawni wagnerowcy, którzy dołączyli do konkurencyjnej firmy wojskowej Redut założonej przez zastępcę Głównego Zarządu Wywiadowczego Sztabu Generalnego Sił Zbrojnych FR (Главное разведывательное управление Генерального штаба Вооружённых сил Российской Федерации, GRU) gen. Władimira Aleksiejewa. Od sierpnia 2021 r. firma Redut zaczęła intensywnie przejmować zasoby kadrowe wagnerowców na potrzeby wojny w Ukrainie, co doprowadziło do sporu między Prigożynem a gen. Aleksiejewem[15]. Szef Grupy Wagnera miał nie być informowany o przygotowaniach do inwazji, początkowo nie przewidywano też udziału jego formacji w działaniach wojennych[16]. Sytuacja zmieniła się jednak już w pierwszym miesiącu wojny, gdy wskutek wysokich strat w ludziach i sprzęcie, a także licznych dezercji, część rosyjskich oddziałów utraciła zdolność do prowadzenia operacji ofensywnych. Gdy w kwietniu 2022 r. okazało się, że rosyjska armia nie jest w stanie przełamać ukraińskich linii obronnych w Donbasie, udział Grupy Wagnera wyniósł ok. 1500 najemników, a miesiąc później już 7000. Werbowano ich m.in. za pośrednictwem stowarzyszeń zrzeszających weteranów (np. Ligi Ochrony Interesów Weteranów Lokalnych Wojen i Konfliktów Zbrojnych – tzw. Liga, Лига защиты интересов ветеранов локальных войн и военных конфликтов czy Ochotniczego Towarzystwa Wspierania Armii, Lotnictwa i Marynarki Wojennej – DOSAAF, Добровольное общество содействия армии, авиации и флоту, ДОСААФ), klubów sportowych, a także ponad 60 regionalnych centrów rekrutacji[17]. We wrześniu 2022 r. za zgodą rosyjskich władz wagnerowcy rozpoczęli masową rekrutację w więzieniach i koloniach karnych

[14] M. Rana, *Volodymyr Zelensky: Russian mercenaries ordered to kill Ukraine's president*, The Times, 28 II 2022 r., https://www.thetimes.co.uk/article/volodymyr-zelensky-russian-mercenaries-ordered-to-kill-ukraine-president-cvcksh79d [dostęp: 19 I 2024].

[15] *Жаба и Минобороны. Как поссорились Евгений Викторович с Сергеем Кужугетовичем*, The Insider, 12 V 2023 r., https://theins.ru/politika/261683 [dostęp: 12 V 2023].

[16] *Грубо говоря, мы начали войну Как отправка ЧВК Вагнера на фронт помогла Пригожину наладить отношения с Путиным – и что такое «собянинский полк». Расследование «Медузы» о наемниках на войне в Украине*, Meduza, 13 VII 2022 r., https://meduza.io/feature/2022/07/13/grubo-govorya-my-nachali-voynu [dostęp: 13 VII 2022].

[17] K. Hird i in., *Russian Offensive Campaign Assessment, March 10, 2023*, Institute for the Study of War, 10 III 2023 r., https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-march-10-2023 [dostęp: 10 III 2023].

(tzw. Projekt K). Skazańcom oprócz korzyści finansowych obiecano – po wypełnieniu sześciomiesięcznego kontraktu[18] – ułaskawienie (bez względu na wyrok) przez prezydenta Putina. W ten sposób Grupa Wagnera pozyskała blisko 40 000 przestępców dopuszczających się zbrodni wojennych (w tym gwałtów, tortur i morderstw na ludności cywilnej). Ze względu na braki w amunicji artyleryjskiej dowództwo tej organizacji traktowało kryminalistów jak mięso armatnie. Przyjęta taktyka ciągłych szturmów niewielkich grup piechoty na wybrane odcinki frontu powodowała straty wśród skazańców sięgające 90% i przynosiła niewielkie rezultaty[19].

Wagnerowcy początkowo walczyli głównie w obwodzie ługańskim, gdzie latem 2022 r. odegrali ważną rolę w zajęciu Popasnej, Siewierodoniecka i Łysyczańska. Następnie zostali przerzuceni do obwodu donieckiego, gdzie 10 stycznia 2023 r. ogłosili zajęcie Sołedaru[20]. Putin publicznie uznał to za sukces (…) *wszystkich sił biorących udział w wojnie w Ukrainie*[21], a nie samej Grupy Wagnera, co można interpretować jako sygnał ostrzegawczy dla rosnących ambicji politycznych Prigożyna. Szef wagnerowców planował ubiegać się o stanowisko mera Petersburga z ramienia Sprawiedliwej Rosji Siergieja Mironowa, a tym samym odebrać urząd Aleksandrowi Biegłowowi – wieloletniemu zaufanemu współpracownikowi Putina. Po wygranych wyborach w 2019 r. Biegłow uniemożliwił Prigożynowi realizację jego inwestycji infrastrukturalnych na obrzeżach miasta i w Zatoce Fińskiej. W odwecie Prigożyn usiłował wymusić na Federalnej Służbie Bezpieczeństwa FR (Федеральная служба безопасности Российской Федерации, FSB) i prokuraturze wszczęcie postępowania przeciwko merowi Petersburga w sprawie defraudacji publicznych pieniędzy,

[18] Ci, którzy zostali ułaskawieni przez Putina i wrócili do Rosji, często dopuszczali się kolejnych zbrodni, zwłaszcza morderstw i gwałtów. Zob. *Против двоих боевиков ЧВК «Вагнер» в разных регионах России возбудили дела об изнасиловании 13-летних девочек*, Важные истории, 30 VIII 2023 r., https://storage.googleapis.com/istories/news/2023/08/30/protiv-dvoikh-boevikov-chvk-vagner-v-raznikh-regionakh-rossii-vozbudili-dela-ob-iznasilovanii-13-letnikh-devochek/index.html [dostęp: 30 VIII 2023].

[19] J. Ber, *Od Popasnej do Bachmutu. Grupa Wagnera w wojnie rosyjsko-ukraińskiej*, OSW, 28 IV 2023 r., https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2023-04-28/od-popasnej-do-bachmutu-grupa-wagnera-w-wojnie-rosyjsko [dostęp: 28 IV 2023]; Y. Chornogor, P. Rad, A. Chernysh, *Anatomy of "Wagner PMC": creation, war in Ukraine and ways of countering the group*, Ukrainian PRISM, kwiecień 2023 r., https://prismua.org/wp-content/uploads/2023/05/PMC_Wagner_eng.pdf, s. 9 [dostęp: 28 IV 2023].

[20] S. Walker, P. Beaumont, D. Sabbagh, *Head of Russia's Wagner group says his troops have taken control of Soledar*, The Guardian, 11 I 2023 r., https://www.theguardian.com/world/2023/jan/10/head-of-wagner-group-says-his-troops-have-taken-control-of-soledar [dostęp: 1 I 2024].

[21] K. Stepanenko i in., *Russian offensive campaign assessment, January 16, 2023*, Institute for the Study of War, 16 I 2023 r., https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-january-16-2023 [dostęp: 19 I 2024]. Tłumaczenia w artykule pochodzą od autora (dop. red.).

zdrady stanu i niszczenia miejsc kultury[22]. W trakcie inwazji na Ukrainę Biegłow utrudniał Grupie Wagnera możliwość prowadzenia rekrutacji w regionie, co przyczyniało się do zaostrzania sporu między nimi.

Rola, jaką wagnerowcy odegrali na froncie w Ukrainie, doprowadziła do zmiany narracji Kremla na temat tej organizacji. Do 2021 r. zaprzeczano jej istnieniu i jakimkolwiek powiązaniom z rosyjskim aparatem państwowym. Sukcesy wagnerowców spowodowały, że kontrolowana przez Kreml stacja RT wyprodukowała filmy propagandowe, w których ujawniono m.in. utrzymywany wcześniej w tajemnicy udział Grupy Wagnera w agresji na Ukrainę w 2014 r., oraz kulisy operacji na Bliskim Wschodzie i w Afryce. Rosyjskie władze zgodziły się także na częściową instytucjonalizację działalności wagnerowców[23]. W listopadzie 2022 r. powstało w Petersburgu Centrum Grupy Wagnera i klub młodzieżowy Wagnerenok (Вагнеренок). W styczniu 2023 r. zarejestrowano Grupę Wagnera jako podmiot gospodarczy świadczący „usługi doradcze". Prigożynowi nie udało się jednak doprowadzić do legalizacji PFW w Rosji, co starał się uczynić za pośrednictwem lobbingu partii Sprawiedliwa Rosja[24]. W związku z udziałem najemników w inwazji na Ukrainę rosyjskie władze utraciły całkowitą zdolność do wiarygodnego zaprzeczania (ang. *plausible deniability*) powiązaniom państwa z tą organizacją, co wcześniej i tak miało ograniczoną skuteczność[25].

Polityka Kremla wobec Grupy Wagnera umacniała przekonanie szefa tej organizacji o jego rosnącej pozycji w systemie władzy i zachęcała go do dalszej konfrontacji z wojskiem. Sygnałem ostrzegawczym dla rosnących ambicji Prigożyna było zamordowanie rosyjskiego blogera Maksima Fomina (alias Władlena Tatarskiego), który był jednym z wielu powiązanych z Grupą Wagnera propagandzistów wojennych i krytyków Ministerstwa Obrony. Do zamachu bombowego doszło 2 kwietnia 2023 r. w trakcie spotkania autorskiego Tatarskiego w centrum Petersburga w barze należącym do Prigożyna. Miejsce to pełniło także funkcję klubu dyskusyjnego grupy Cyber Front Z[26]. O przeprowadzenie zamachu oficjalnie oskarżono Ukrainę, jednak

---

[22] Y. Chornogor, P. Rad, A. Chernysh, *Anatomy of "Wagner PMC"*…, s. 20–21.

[23] K.P. Larsen, *From mercenary to legitimate actor? Russian discourses on private military companies*, „Post-Soviet Affairs" 2023, t. 39, nr 6, s. 420–439. https://doi.org/10.1080/1060586X.2023.2247782.

[24] F. Bryjka, *Transformacja Grupy Wagnera w związku z wojną na Ukrainie*, PISM, 7 III 2023 r., https://www.pism.pl/publikacje/transformacja-grupy-wagnera-w-zwiazku-z-wojna-na-ukrainie [dostęp: 7 III 2023].

[25] P. Stronski, *Implausible Deniability: Russia's Private Military Companies*, Carnegie Endowment for International Peace, 2 VI 2020 r., https://carnegieendowment.org/2020/06/02/implausible-deniability-russia-sprivate-military-companies-pub-81954 [dostęp: 2 VI 2020].

[26] *В кафе Петербурга на «творческом вечере» «военкора» Владлена Татарского (у него полмиллиона подписчиков в телеграме) произошел взрыв. Блогер погиб*, Meduza, 2 IV 2023 r., https://meduza.io/feature/2023/04/02/v-peterburge-v-kafe-evgeniya-prigozhina-proizoshel-

biorąc pod uwagę kontekst ówczesnych relacji między szefem najemników a Ministerstwem Obrony, można założyć, że była to operacja likwidacyjna rosyjskich służb specjalnych.

Rywalizacja pomiędzy wagnerowcami a wojskiem zaostrzyła się 11 stycznia 2023 r., gdy Putin powierzył funkcję dowódcy wojsk okupacyjnych w Ukrainie bezpośrednio gen. Gierasimowowi. Zastąpił on współpracującego z Grupą Wagnera gen. Siergieja Surowikina. Ministerstwo Obrony próbowało osłabić Prigożyna i wagnerowców walczących pod Bachmutem przez ograniczanie dostaw amunicji i przejęcie kontroli nad procesem werbunku w koloniach karnych (do maja 2023 r. armia pozyskała w ten sposób 10 000 osób). W odwecie Prigożyn miał zaproponować ukraińskiemu wywiadowi wojskowemu (Головне управління розвідки Міністерства Оборони України) informacje na temat pozycji rosyjskich wojsk w Donbasie w zamian za oddanie Bachmutu[27]. Strona ukraińska nie przyjęła tej propozycji, obawiając się podstępu. Szef najemników obarczył Ministerstwo Obrony i Sztab Generalny winą za wysokie straty (szacowane na 20 000–30 000 osób) w walkach o Bachmut[28], a także groził oddaniem zajętych pozycji Ukrainie. Kwestię „głodu amunicyjnego" rozwiązano z udziałem gen. Surowikina, który był pośrednikiem w rozmowach między wagnerowcami a armią. Mimo że 20 maja 2023 r. Putin pogratulował Grupie Wagnera zajęcia Bachmutu, zaznaczył, że w operacji brały udział także jednostki regularnej armii[29]. Prigożyn zdeprecjonował ten fakt i przypisał sukces wyłącznie swoim najemnikom. Następnie oznajmił, że do końca maja Grupa Wagnera przekaże wszystkie zajęte pozycje rosyjskim siłom zbrojnym, wycofa się z Ukrainy i przez dwa miesiące będzie odbudowywać zdolność bojową[30]. Ministerstwo Obrony wykorzystało ten moment, by podporządkować sobie wszystkie nieregularne formacje zbrojne walczące w Ukrainie. Szef wagnerowców bezskutecznie usiłował nie dopuścić do utraty autonomii operacyjnej i podporządkowania się wojsku, co doprowadziło do tzw. marszu sprawiedliwości.

-vzryv-vo-vremya-tvorcheskogo-vechera-voenkora-vladlena-tatarskogo-po-predvaritelnym-dannym-on-pogib [dostęp: 2 IV 2023].

[27] S. Harris, I. Khurshudyan, *Wagner chief offered to give Russian troop locations to Ukraine*, The Washington Post, 15 V 2023 r., https://www.washingtonpost.com/national-security/2023/05/14/prigozhin-wagner-ukraine-leaked-documents/ [dostęp: 15 V 2023].

[28] Na temat roli Grupy Wagnera w walkach o Bachmut zob. szerzej: K. Stepanenko, *The Kremlin's Pyrrhic Victory in Bakhmut: A Retrospective on the Battle for Bakhmut*, Institute for the Study of War, 24 V 2023 r., https://www.understandingwar.org/backgrounder/kremlin%E2%80%99s-pyrrhic-victory-bakhmut-retrospective-battle-bakhmut [dostęp: 24 V 2023].

[29] *Путин поздравил российских военных с освобождением Артемовска*, Tacc, 20 V 2023 r., https://tass.ru/politika/17804025 [dostęp: 19 I 2024].

[30] J. Prigożyn, wpis na kanale Telegram, https://t.me/concordgroup_official/1002 [dostęp: 20 V 2023].

Przebieg rebelii Grupy Wagnera

W nocy z 23 na 24 czerwca 2023 r. Prigożyn oświadczył, że Grupa Wagnera przekroczyła ukraińsko-rosyjską granicę w obwodzie rostowskim i kieruje się na Moskwę. Szef najemników podkreślał, że prowadzona przez niego operacja to nie zamach stanu przeciwko Putinowi, lecz tzw. marsz sprawiedliwości przeciwko ministrowi obrony gen. Szojgu. Wagnerowcy bez oporu dotarli do kwatery głównej Południowego Okręgu Wojskowego (POW) w Rostowie nad Donem, która pełni także funkcję dowództwa „specjalnej operacji wojskowej" w Ukrainie. Na miejscu spotkali się z pozytywną reakcją lokalnej społeczności[31]. Prigożyn rozmawiał z wiceministrem obrony gen. Junus-Biekiem Jewkurowem i pierwszym zastępcą szefa GRU gen. Aleksiejewem. Żądania lidera puczystów dotyczące rozmowy z gen. Szojgu i gen. Gierasimowem zostały odrzucone, co wpłynęło na decyzję o kontynuacji marszu. Prigożyn wezwał całą rosyjską armię, by przyłączyła się do buntowników. Nie spotkało się to jednak z oczekiwaną przez niego reakcją wojskowych. Nawet gen. Surowikin, który w trakcie pełnienia funkcji dowódcy operacji wojennej w Ukrainie przyczynił się do wzrostu pozycji Grupy Wagnera, potępił pucz i wezwał wagnerowców do niewykonywania rozkazów Prigożyna. Buntowników nie poparły też władze federalne i regionalne, struktury siłowe czy elity biznesowe.

Kolumny najemników kierujące się w stronę Moskwy składały się z ok. 1000 jednostek sprzętu i pojazdów wojskowych (w tym wozów opancerzonych Tigr i bojowych wozów piechoty, czołgów T-80 i T-90, wyrzutni rakietowych BM-21 Grad, a także systemów ziemia-powietrze Pancyr S-1)[32]. Prigożyn deklarował, że kierowane przez niego siły składają się z 25 000 najemników. Możliwe, że miał na myśli cały personel Grupy Wagnera – także ten prowadzący operacje w Afryce i przebywający na leczeniu w Rosji. W rebelii uczestniczyło najprawdopodobniej 5000–10 000 wagnerowców[33]. W odpowiedzi na bunt Komitet Śledczy FSB wszczął postępowanie karne przeciwko Prigożynowi na podstawie art. 279 Kodeksu karnego FR, który mówi o organizacji rebelii, za co grozi 20 lat więzienia. W Moskwie wzmocniono środki bezpieczeństwa. Federalna Służba Wojsk Gwardii Narodowej FR (Федеральная служба войск национальной гвардии Российской Федерации, Rosgwardia), Oddział Mobilny Specjalnego Przeznaczenia (Отряд мобильный особого

[31] P. Ivanova, A. Stognei, M. Seddon, *Russian insurrection: Prigozhin's failed mutiny and the fallout*, Financial Times, 23 VI 2023 r., https://www.ft.com/content/34f3a349-a05f-4672-b059-6980ecc27adf [dostęp: 23 VI 2023].

[32] M. Galeotti, *Russia's coup d'état – Nature and Implications*, In Moscow's Shadows, 27 VI 2023 r., https://inmoscowsshadows.wordpress.com/2023/06/27/scss10-26-june-2023-russias-coup-detat-nature-and-implications/ [dostęp: 27 VI 2023].

[33] Tamże.

назначения, OMON) i Specjalny Oddział Szybkiego Reagowania (Специальный Отряд Быстрого Реагирования, SOBR) zostały postawione w stan najwyższej gotowości[34]. Personel wojskowy i organy ścigania utworzyły posterunki wojskowe i punkty kontrolne w pobliżu kwatery głównej POW w Rostowie nad Donem. Federalna Służba Bezpieczeństwa i jednostki SOBR przygotowały także blokady drogowe wzdłuż trasy Moskwa–Woroneż–Rostów[35]. Wagnerowcy na ogół nie napotykali oporu ze strony wojska czy służb bezpieczeństwa, jednak w wyniku nielicznych starć strącili sześć śmigłowców i samolot Ił-22M. Zginęło 13 pilotów[36].

Negocjacji z Prigożynem podjął się Łukaszenka, który wezwał przywódcę wagnerowców do zaprzestania działań zbrojnych, by uniknąć dalszego rozlewu krwi. Zgodnie z oficjalnym przekazem[37] prowadził je w porozumieniu z Putinem, który odrzucił propozycję rozmowy telefonicznej lub spotkania z Prigożynem. Ważną rolę mediatorów odegrali także gen. Jewkurow i szef FSB Aleksandr Bortnikow. Podczas negocjacji Prigożyn odstąpił od planowanego rajdu na Ministerstwo Obrony. Kolumny Grupy Wagnera zatrzymały się ok. 200 km przed Moskwą i zawróciły w kierunku Donbasu. W zamian rosyjskie władze odstąpiły od ścigania puczystów, a prezydent Rosji dał Prigożynowi bliżej nieokreślone gwarancje bezpieczeństwa pod warunkiem, że wraz z buntownikami przeniesie się na Białoruś[38].

Rosyjskie władze przyznały, że 29 czerwca 2023 r. Putin spotkał się z Prigożynem i 35 dowódcami Grupy Wagnera[39]. W trakcie trzygodzinnego spotkania na Kremlu prezydent Rosji ocenił dotychczasową rolę najemników podczas wojny w Ukrainie, przedstawił swoją ocenę zbrojnej rebelii, a także wysłuchał wyjaśnień i zapewnień wagnerowców o ich lojalności wobec państwa i jego prezydenta. Najemnikom zaproponowano trzy możliwości:

1) podpisanie kontraktu z rosyjskim Ministerstwem Obrony i kontynuowanie walk w Ukrainie,

---

[34] *В Москве усилили меры безопасности*, Tacc, 23 VII 2023 r., https://tass.ru/proisshestviya/18103225 [dostęp: 23 VII 2023].

[35] *В Ростове-на-Дону рядом со штабом ЮВО выставили посты*, Tacc, 23 VII 2023 r., https://tass.ru/bezopasnost/18103205 [dostęp: 23 VII 2023].

[36] S. Mitzer, J. Janovsky, *Chef's Special – Documenting Equipment Losses During The 2023 Wagner Group Mutiny*, Oryx, 24 VI 2023 r., https://www.oryxspioenkop.com/2023/06/chefs-special-documenting-equipment.html [dostęp: 24 VI 2023].

[37] Y. Preiherman, *What Does Lukashenka's Role as Mediator in Russian Crisis Imply? – Analysis*, Eurasia Review, 29 VI 2023 r., https://www.eurasiareview.com/29062023-what-does-lukashenkas-role-as-mediator-in-russian-crisis-imply-analysis/ [dostęp: 29 VI 2023].

[38] *Вручение генеральских погон высшему офицерскому составу*, Президент Республики Беларусь, 27 VII 2023 r., https://president.gov.by/ru/events/vruchenie-pogon-vysshemu-oficerskomu-sostavu [dostęp: 27 VII 2023].

[39] Tamże.

2) udanie się za swoim przywódcą na Białoruś,
3) rozwiązanie kontraktu i powrót do Rosji bez konsekwencji prawnych za udział w buncie[40].

Jednocześnie Putin stwierdził, że taki podmiot jak Grupa Wagnera nie istnieje, ponieważ działalność PFW w Rosji jest zakazana przez prawo[41].

Chociaż rebelia Prigożyna była wymierzona w gen. Szojgu, a szef wagnerowców wielokrotnie podkreślał swoją lojalność wobec Putina, to fakt, że tzw. marsz sprawiedliwości się odbył, wywołał poważne (negatywne) konsekwencje dla prezydenta Rosji. Przede wszystkim podważył jego autorytet jako silnego i sprawnego przywódcy, gdyż został zmuszony do negocjacji z buntownikiem. Osłabiło to wizerunek prezydenta wśród elit władzy[42]. Putin określił bunt Prigożyna „zdradą" i „ciosem nożem w plecy". Szefa najemników nazwał skorumpowanym kłamcą, który zniszczył reputację Grupy Wagnera. Marsz na Moskwę określił jako (…) *śmiertelne zagrożenie dla państwa* i zapewnił, że (…) *wszyscy, którzy uczestniczyli w przygotowaniu rebelii, poniosą surową karę*[43]. Według „The Washington Post" prezydent Rosji miał otrzymywać informacje wywiadowcze dotyczące przygotowań do rebelii na 2–3 dni przed buntem[44]. Doniesienia te zdaje się potwierdzać rozmieszczenie jednostek specjalnych FSB „Alfa" do ochrony kwatery głównej na Łubiance[45]. Mimo to Putin miał nie wydać ani jednego rozkazu i pozostawić decyzję w sprawie tego, jak reagować na tzw. marsz sprawiedliwości, regionalnym organom wojskowym i służbom bezpieczeństwa. Rebelia wagnerowców ujawniła, że służby nie potrafią skutecznie zneutralizować takich działań. Ich bezczynność była przy tym spowodowana brakiem konkretnych rozkazów i przekonaniem, że szef Grupy Wagnera znajduje się pod kuratelą Kremla, a aktywność jego najemników jest kontrolowana

---

[40] *Песков подтвердил встречу Путина с Пригожиным и командирами «Вагнера» 29 июня*, Интерфакс, 10 VII 2023 r., https://www.interfax.ru/russia/910904 [dostęp: 10 VII 2023].

[41] *Putin says Wagner Group doesn't legally exist*, Meduza, 14 VII 2023 r., https://meduza.io/en/news/2023/07/14/putin-says-wagner-group-no-longer-legally-exists [dostęp: 14 VII 2023].

[42] A. Legucka, *Konsekwencje buntu Prigożyna dla systemu putinowskiego w Rosji*, PISM, 26 VI 2023 r., https://www.pism.pl/publikacje/konsekwencje-buntu-prigozyna-dla-systemu-putinowskiego-w-rosji [dostęp: 26 VI 2023]; M. Komin, *"Fighting spirit": Russia's technocrat elite after the Wagner mutiny*, European Council on Foreign Relations, 24 VII 2023 r., https://ecfr.eu/article/fighting-spirit-russias-technocrat-elite-after-the-wagner-mutiny/ [dostęp: 24 VII 2023].

[43] *Обращение к гражданам России*, Kremlin.ru, 24 VI 2023 r., https://web.archive.org/web/20230628083145/https://kremlin.ru/events/president/news/71496 [dostęp: 24 VI 2023].

[44] C. Belton, S. Harris, G. Miller, *Putin appeared paralyzed and unable to act in first hours of rebellion*, The Washington Post, 25 VII 2023 r., https://www.washingtonpost.com/world/2023/07/25/putin-prigozhin-rebellion-kremlin-disarray/ [dostęp: 25 VII 2023].

[45] M. Weiss, *Russia's Spies Say Putin Faces More Coups*, The Insider, 20 VII 2023 r., https://theins.ru/en/politics/263596 [dostęp: 20 VII 2023].

przez władze. W zażegnaniu kryzysu prezydenta miał wspierać gubernator regionu Tula, oficer FSB i GRU odpowiedzialny w przeszłości m.in. za bezpieczeństwo Putina – gen. płk Aleksiej Diumin[46]. Przez wielu komentatorów był on wskazywany jako potencjalny następca gen. Szojgu.

By ustabilizować reżim i ugruntować własną pozycję, Putin zdecydował się wzmocnić Gwardię Narodową odpowiedzialną za bezpieczeństwo wewnętrzne i dowodzoną przez lojalnego wobec prezydenta gen. Wiktora Zołotowa[47]. Dnia 19 lipca 2023 r. Duma Państwowa FR przyjęła ustawę zezwalającą tej formacji na posiadanie ciężkiego sprzętu wojskowego do odzyskiwania zakładników, ochrony obywateli, urzędników i personelu wojskowego, zapewnienia bezpieczeństwa podczas zamieszek i w sytuacjach awaryjnych, zwalczania samolotów bezzałogowych, a także działalności nielegalnych grup zbrojnych[48]. Najprawdopodobniej specjalistyczny sprzęt wojskowy trafił do pułku Opłot (pol. Twierdza). Rosgwardii podporządkowano także elitarną jednostkę Grom, która wcześniej wchodziła w skład Federalnej Służby Obrotu Narkotykami (Федеральная служба Российской Федерации по контролю за оборотом наркотиков)[49]. Wzmacnianie Rosgwardii stanowiącej pewnego rodzaju kordon bezpieczeństwa prezydenta świadczy o tym, że Putin obawia się kolejnych zamachów, których może być celem.

Rebelia wagnerowców spowodowała także czystki w rosyjskiej armii. Aresztowano kilkunastu generałów, m.in. byłego wiceministra obrony ds. logistyki gen. Michaiła Mizincewa, który najpierw został usunięty ze stanowiska w Ministerstwie Obrony za dostarczanie wagnerowcom amunicji, a następnie podpisał kontrakt

---

[46] Generał płk Aleksiej Diumin (ur. 28 VIII 1972 r. w Kursku) – w 1994 r. ukończył Wyższą Wojskową Szkołę Inżynierii Radioelektronicznej w Woroneżu. Następnie do 1996 r. pracował jako inżynier w Centralnym Ośrodku Zintegrowanej Kontroli Technicznej Rosyjskich Sił Powietrznych. W latach 1996–2013 służył w FSB, gdzie odpowiadał m.in. za bezpieczeństwo prezydenta. W 2009 r. ukończył z wyróżnieniem Rosyjską Akademię Administracji Publicznej (Służby Cywilnej) przy Prezydencie FR, a w 2013 r. Wojskową Akademię Sztabu Generalnego Sił Zbrojnych FR. W latach 2013–2016 był zastępcą szefa GRU, szefem Sztabu Generalnego i pierwszym zastępcą naczelnego dowódcy wojsk lądowych, a następnie wiceministrem obrony FR. Od 2016 r. pełni funkcję gubernatora regionu Tula. Zob. Д. Дурова, *В России уже нашли нового министра обороны для Пригожина: в сети назвали имя*, Oboz.ua, 25 VI 2023 r., https://news.obozrevatel.com/russia/v-rossii-uzhe-nashli-novogo-ministra-oboronyi-dlya-prigozhina-v-seti-nazvali-imya.htm [dostęp: 25 VI 2023].

[47] J. Darczewska, *Rosgwardia. Siły specjalnego przeznaczenia*, „Punkt Widzenia OSW" 2020, nr 78, s. 5.

[48] *State Duma passes bill allowing Russia's National Guard troops to use heavy military equipment*, Meduza, 19 VII 2023 r., https://meduza.io/en/news/2023/07/19/state-duma-passes-bill-allowing-russia-s-national-guard-troops-to-use-heavy-military-equipment [dostęp: 19 VII 2023].

[49] М. Солопов, *Силовые ведомства прорабатывают вопрос о переподчинении полицейского спецназа «Гром» Росгвардии*, Ведомости, 4 VII 2023 r., https://www.vedomosti.ru/politics/articles/2023/07/04/983567-vedomstva-prorabativayut-vopros-o-perepodchinenii-politseiskogo-spetsnaza-rosgvardii [dostęp: 4 VII 2023].

z Grupą Wagnera. Kolejną osobą jest gen. Surowikin, dzięki któremu wagnerowcy stali się kluczową siłą szturmową w walkach miejskich w Donbasie. W dniu śmierci Prigożyna gen. Surowikina usunięto ze stanowiska dowódcy rosyjskich wojsk powietrzno-kosmicznych[50]. Z czasem został on jednak zwolniony z aresztu domowego i objął stanowisko szefa Komitetu Koordynacyjnego ds. Obrony Powietrznej w ramach Rady Ministrów Obrony Wspólnoty Niepodległych Państw[51].

Władze na Kremlu podjęły także działania mające na celu uciszenie krytyków. Aresztowano Igora Girkina ps. „Striełkow" – byłego pułkownika Specnazu FSB i samozwańczego ministra obrony Donieckiej Republiki Ludowej (Донецкая Народная Республика, DNR). W swojej aktywności w mediach społecznościowych przekraczał on granice krytyki akceptowalne przez Kreml. Założył nawet Klub Wściekłych Patriotów zrzeszający nacjonalistów otwarcie wyrażających swoje niezadowolenie ze sposobu prowadzenia wojny w Ukrainie[52]. Rosyjski Komitet Śledczy postawił mu, a także Pawłowi Gubariewowi (w przeszłości samozwańczemu liderowi DNR i przewodniczącemu Klubu Wściekłych Patriotów) zarzuty dotyczące działalności ekstremistycznej[53]. Główną przyczyną zatrzymania Girkina były jego ambicje polityczne. Swoją popularność wśród środowisk nacjonalistycznych planował wykorzystać przez start w wyborach prezydenckich wiosną 2024 r.[54] Dnia 25 stycznia 2024 r. sąd w Moskwie skazał go na 4 lata pozbawienia wolności pod zarzutem nawoływania do ekstremizmu[55].

---

[50] Zastąpił go gen. płk Wiktor Afzałow, który od sierpnia 2018 r. pełnił funkcję szefa sztabu Sił Powietrznych FR. Zob. *Источник: врио главкома ВКС назначили генерала Афзалова*, Риа Новости, 23 VIII 2023 r., https://ria.ru/20230823/afzalova-1891645152.html [dostęp: 23 VIII 2023].

[51] *Генерал Суровикин возглавил координационный комитет СНГ по вопросам ПВО Подробнее*, EurAsia Daily, 10 X 2023 r., https://eadaily.com/ru/news/2023/09/10/general-surovikin-vozglavil--koordinacionnyy-komitet-sng-po-voprosam-pvo [dostęp: 10 X 2023].

[52] Oprócz Girkina do aresztu trafili m.in. były płk FSB Michaił Poliakow i były płk GRU Władimir Kwaczkow. Wszyscy prowadzili kanały w serwisie Telegram wykorzystywane do otwartej krytyki Kremla, Ministerstwa Obrony i Sztabu Generalnego Sił Zbrojnych FR. Zob. K. Kirillova, *Propaganda and Repression Turn Against Their Creators in Russia*, The Jamestown Foundation, 25 VII 2023 r., https://jamestown.org/program/propaganda-and-repression-turn-against-their-creators-in-russia/ [dostęp: 25 VII 2023].

[53] *Pavel Gubarev, associate of Igor Strelkov, reportedly investigated for extremism*, Meduza, 23 VII 2023 r., https://meduza.io/en/news/2023/07/23/pavel-gubarev-associate-of-igor-strelkov-reportedly-investigated-for-extremism [dostęp: 23 VII 2023].

[54] *Jailed former 'Donetsk People's Republic' militia leader to run for president*, Novaya Gazeta Europe, 31 VIII 2023 r., https://novayagazeta.eu/articles/2023/08/31/jailed-former-donetsk-peoples-republic-militia-leader-to-run-for-president-en-news [dostęp: 31 VIII 2023].

[55] *Russia sentences former separatist commander and pro-war blogger Igor Strelkov to four years in prison*, Meduza, 25 I 2024 r., https://meduza.io/en/news/2024/01/25/russia-sentences-former-separatist--commander-and-pro-war-blogger-igor-strelkov-to-four-years-in-prison [dostęp: 25 I 2024].

Grupa Wagnera na Białorusi

W wyniku mediacji Łukaszenki Putin udzielił Prigożynowi i jego najemnikom bliżej nieokreślonych gwarancji bezpieczeństwa pod warunkiem przeniesienia członków Grupy Wagnera na Białoruś. Proces rozmieszczania wagnerowców rozpoczął się w trakcie szczytu NATO w Wilnie 11 lipca 2023 r. Białoruskie władze udostępniły im infrastrukturę wojskową we wsi Cel k. Osipowicz w obwodzie mohylewskim, gdzie na terenie dawnej bazy wojsk rakietowych (jednostka wojskowa nr 61732) powstał główny obóz wagnerowców. W dniu 27 czerwca zaczęto tam rozstawiać namioty mogące pomieścić łącznie ok. 8000 osób[56]. Pod koniec lipca zlikwidowano dotychczasową bazę Grupy Wagnera w rosyjskim Molkino, która znajdowała się przy terenie 10 Brygady Specjalnego Przeznaczenia GRU[57].

Dnia 18 lipca w obozie wagnerowców pojawili się Prigożyn oraz Utkin. W swoich wypowiedziach podkreślili rozpoczęcie nowego rozdziału w historii organizacji. Jej głównym zadaniem na Białorusi jest szkolenie żołnierzy i jednostek Ministerstwa Spraw Wewnętrznych[58]. Nowa lokalizacja pozwalała na zorganizowanie zaplecza logistycznego operacji Grupy Wagnera w Afryce. Prigożyn nie wykluczał przy tym możliwości powrotu najemników do Ukrainy[59]. Kolejnego dnia szef wagnerowców zarejestrował na Białorusi spółkę córkę Concord Management and Consulting, która oficjalnie miała zajmować się zarządzaniem nieruchomościami[60]. Dowódcą zgrupowania Grupy Wagnera na Białorusi został Siergiej Czubko

---

[56] Oprócz bazy we wsi Cel wagnerowcy mają także dysponować mniejszą infrastrukturą we wsi Sosnowij k. Osipowicz i mieście Narowla (obwód homelski). Zob. *Вагнерівці продовжують прибувати у білорусь*, Центр Національного спротиву, 22 VII 2023 r., https://sprotyv.mod.gov.ua/vagnerivtsi-prodovzhuyut-prybuvaty-u-bilorus/ [dostęp: 22 VII 2023].

[57] *Наемники ЧВК Вагнера объявили, что закрывают свою главную базу в краснодарском Молькино*, Meduza, 17 VII 2023 r., https://meduza.io/news/2023/07/17/naemniki-chvk-vagnera-ob-yavili-chto-zakryvayut-svoyu-glavnuyu-bazu-v-krasnodarskom-molkino [dostęp: 17 VII 2023].

[58] Grupa Wagnera szkoli głównie siły operacji specjalnych, oddziały obrony przed bronią masowego rażenia, wojska zmechanizowane, wojska inżynieryjne i wojska łączności, a także obronę terytorialną. Szkolenia odbywają się m.in. na poligonie brzeskim znajdującym się w pobliżu polskiej granicy. Zob. A.M. Dyner, *Grupa Wagnera na Białorusi – potencjalne zagrożenia dla Polski*, PISM, 27 VII 2023 r., https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-potencjalne-zagrozenia-dla-polski [dostęp: 27 VII 2023].

[59] *'Welcome to hell' Prigozhin reappears in Belarus, rallying Wagner Group mercenaries for future work in Africa (but not yet in Ukraine)*, Meduza, 19 VII 2023 r., https://meduza.io/en/feature/2023/07/19/welcome-to-hell [dostęp: 19 VII 2023].

[60] *Евгений Пригожин зарегистрировал компанию в Осиповичском районе*, Reformation, 22 VII 2023 r., https://reform-by.cdn.ampproject.org/c/s/reform.by/evgenij-prigozhin-zaregistriroval-kompaniju-v-osipovichskom-rajone/amp [dostęp: 22 VII 2023].

ps. „Pionier" – weteran operacji w Syrii, Republice Środkowoafrykańskiej (RŚA), Sudanie, Mali i Libii, odznaczony pięcioma Medalami za Odwagę[61].

Według aktywistów z projektu „Hajun" do 1 sierpnia na Białoruś wjechało 14 konwojów (łącznie ok. 930 pojazdów) z najemnikami, których liczbę szacowano na 4000–5000 osób. Wagnerowcy trafili tam jednak bez ciężkiego sprzętu wojskowego, ponieważ ponad 2000 sztuk (w tym czołgi, pojazdy opancerzone, artylerię i systemy rakietowe), 2500 ton amunicji i ok. 20 000 sztuk broni strzeleckiej zostało przejęte 12 lipca przez rosyjską armię[62]. Z tego względu Grupa Wagnera jako samodzielna formacja zbrojna dysponująca jedynie bronią strzelecką nie stanowiła zagrożenia militarnego dla państw granicznych NATO. Niejasny status prawny Grupy Wagnera, doświadczenie bojowe oraz międzynarodowa rozpoznawalność dały jednak Białorusi i Rosji dodatkowy instrument oddziaływania hybrydowego w tzw. szarej strefie, w której trudno ocenić charakter zagrożenia oraz przypisać jednoznaczną odpowiedzialność za różne formy agresji. Polska i państwa bałtyckie obawiały się, że Białoruś i Rosja posłużą się wagnerowcami do atakowania służb chroniących granicę i znajdującej się tam infrastruktury, zwiększenia presji migracyjnej[63], umieszczania wśród migrantów swojej agentury, infiltracji terytorium

[61] Siergiej Czubko (ur. 27 X 1976 r. w Czerniowicach w Ukrainie, wówczas ZSRR) – wywodzi się z rodziny o wojskowych tradycjach. Jego ojciec walczył w Afganistanie w trakcie radzieckiej inwazji. Po rozpadzie ZSRR rodzina przeprowadziła się do Noworosyjska. W latach 1994–2002 Czubko służył w rosyjskiej armii (w tym w wojskach powietrzno-desantowych) i brał udział w wojnach czeczeńskich. Po zakończeniu służby przeszedł do sektora prywatnego. W 2003 r. mimo braku wyższego wykształcenia niespodziewanie stanął na czele administracji miejskiej w Noworosyjsku (2003 r. – przewodniczący Komisji ds. Młodzieży w administracji Noworosyjska; 2005 r. – zastępca szefa administracji Rejonu Wiejskiego Myschak). Następnie ponownie został ochroniarzem w prywatnej firmie. W 2011 r. chciano go pozbawić rosyjskiego obywatelstwa ze względu na podejrzenia o posiadanie ukraińskiego obywatelstwa. W 2014 r. pomógł utworzyć zrzeszenie kozaków w Noworosyjsku, co może wskazywać na jego udział w aneksji Krymu lub walkach w Donbasie (lecz nie ma na to potwierdzenia). Do Grupy Wagnera dołączył w 2017 r., brał udział w działaniach w Syrii. Po roku służby został dowódcą operacji grupy we wschodniej Syrii. W 2020 r. przeniesiono go do Libii, gdzie kierował sztabem Grupy Wagnera. Zob. *Journalists identify head of Wagner Group forces in Belarus as 46-year-old Ukraine native*, Meduza, 26 VII 2023 r., https://meduza.io/en/news/2023/07/26/journalists-identify-head-of-wagner-forces-in-belarus-as-46-year-old-ukraine-native [dostęp: 26 VII 2023]; *Кто такой Сергей «Пионер» – глава «Вагнера» в Беларуси?*, Reformation, 19 VII 2023 r., https://reform.by/kto-takoj-sergej-pioner-glava-vagnera-belarusi [dostęp: 19 VII 2023].

[62] *Wagner Group reportedly hands over military equipment and ammunition to Russia's Defense Ministry*, Meduza, 12 VII 2023 r., https://meduza.io/en/news/2023/07/12/wagner-group-reportedly-hands-over-military-equipment-and-ammunition-to-russia-s-defense-ministry [dostęp: 12 VII 2023].

[63] A. Sari, *Hybrid CoE Paper 17: Instrumentalized migration and the Belarus crisis: Strategies of legal coercion*, Hybrid CoE, 25 IV 2023 r., https://www.hybridcoe.fi/publications/hybrid-coe-paper-17-instrumentalized-migration-and-the-belarus-crisis-strategies-of-legal-coercion/ [dostęp: 25 IV 2023].

przez grupy dywersyjno-rozpoznawcze, rozpoznawania infrastruktury krytycznej i przygotowania aktów sabotażu[64].

Obecność rosyjskich najemników na Białorusi była wykorzystywana w prowadzonych przez Rosję operacjach psychologiczno-dezinformacyjnych. Przewodniczący Komisji ds. Obrony Dumy Państwowej FR Andriej Kartapołow zasugerował, że rozmieszczenie wagnerowców oznacza przygotowania Rosji do zajęcia tzw. przesmyku suwalskiego oddzielającego Białoruś od rosyjskiej eksklawy (obwodu królewieckiego)[65]. Łukaszenka ostrzegał, że wagnerowcy chcieliby wkroczyć na terytorium Polski w celu przeprowadzenia akcji zbrojnych w Warszawie oraz w Rzeszowie, gdzie znajduje się główny hub logistyczny przeznaczony do zaopatrywania Ukrainy w pomoc wojskową udzielaną przez państwa zachodnie. Putin stwierdził natomiast, że Polska ma agresywne plany wobec Ukrainy i Białorusi, a Rosja jest gotowa odpowiedzieć na nie „wszelkimi dostępnymi środkami"[66]. Skoordynowane działania w sferze informacyjnej miały zastraszyć polskie społeczeństwo i wpłynąć na polskie władze tak, by zmieniły one politykę względem Białorusi i Rosji na mniej konfrontacyjną oraz zaprzestały wspierania Ukrainy. Działania te były także wyraźnym ostrzeżeniem, że wagnerowcy mogą zostać wykorzystani do prowokacji, która wymusi nieproporcjonalną reakcję państw granicznych NATO i UE. W ten sposób Rosja i Białoruś stwarzały poczucie zagrożenia oraz zwiększonego napięcia w NATO i liczyły, że pogłębi to podziały polityczne między sojusznikami co do oceny charakteru zagrożenia i jego możliwych konsekwencji, a przez to utrudni im skuteczne reagowanie[67].

Aby zniechęcić Białoruś i Rosję do nasilania prowokacji i wzmocnić swoje poczucie bezpieczeństwa, Polska zwiększyła wsparcie dla Straży Granicznej o kilkuset policjantów (w tym kontrterrorystów), rozmieściła na granicy dodatkowe oddziały wojskowe (do 4000 żołnierzy) i utworzyła zgrupowanie zadaniowe w operacji pod

---

Na temat stosowania inżynierii przymusowej migracji (ang. *coercive engineered migration*) przez Rosję zob. M. Wojnowski, *Geneza, teoria i praktyka rosyjskiej inżynierii przymusowej migracji. Przyczynek do badań nad kryzysem migracyjnym na wschodniej flance NATO*, „Przegląd Bezpieczeństwa Wewnętrznego" 2022, nr 26, s. 11–49. https://doi.org/10.4467/20801335PBW.21.034.15694.

64 A.M. Dyner, W. Lorenz, F. Bryjka, *Grupa Wagnera na Białorusi – konsekwencje dla NATO i UE*, PISM, 7 IX 2023 r., https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-konsekwencje-dla-nato-i-ue [dostęp: 7 IX 2023].

65 *Celem wagnerowców na Białorusi będzie „przejęcie Przesmyku Suwalskiego" – rosyjski deputowany*, Belsat, 16 VII 2023 r., https://belsat.eu/pl/news/16-07-2023-celem-wagnerowcow-na-bialorusi-bedzie-przejecie-przesmyku-suwalskiego-rosyjski-deputowany [dostęp: 16 VII 2023].

66 P. Żochowski, *Rosja i Białoruś oskarżają Polskę o plany agresji*, OSW, 24 VII 2023 r., https://www.osw.waw.pl/pl/publikacje/analizy/2023-07-24/rosja-i-bialorus-oskarzaja-polske-o-plany-agresji [dostęp: 24 VII 2023].

67 A.M. Dyner, W. Lorenz, F. Bryjka, *Grupa Wagnera na Białorusi – konsekwencje dla NATO i UE*…

kryptonimem „RENGAW" (6000 żołnierzy) utrzymywane w odwodzie[68]. W związku z ryzykiem infiltracji terytorium przez wagnerowców posługujących się białoruskimi paszportami Litwa zamknęła cztery z sześciu przejść granicznych z Białorusią. Państwa regionu ostrzegły, że mogą całkowicie zamknąć granice z Białorusią, co odcięłoby ją od możliwości wymiany handlowej z UE, która – mimo nałożonych sankcji na to państwo – pozostaje jej drugim (po Rosji) największym partnerem handlowym. Wezwały też białoruskie władze do natychmiastowego usunięcia Grupy Wagnera z terytorium państwa, a także do wycofania z obszarów przygranicznych migrantów wykorzystywanych przez białoruskie służby do destabilizowania granicy[69].

Istotnym elementem rosyjsko-białoruskich działań psychologicznych z wykorzystaniem Grupy Wagnera było oddziaływanie na polskie społeczeństwo. Według sondażu Instytutu Badań Rynkowych i Społecznych ponad połowa Polaków (50,6% respondentów) postrzegała obecność wagnerowców na Białorusi jako zagrożenie bezpieczeństwa Polski[70]. Aparat dezinformacyjno-propagandowy Rosji i Białorusi starał się podtrzymywać te nastroje, m.in. rozpowszechniając grafikę przedstawiającą najemnika trzymającego w ręku nóż i widelec oraz obejmującego polskich żołnierzy na tle słupka granicznego i napisu „Widelec należy trzymać w lewej ręce, nóż w prawej, a Polaków w strachu". W sieci pojawiło się także przerobione zdjęcie polskiego żołnierza z doklejonym znakiem rozpoznawczym Grupy Wagnera i rosyjską flagą. Inne grafiki ukazywały słupki graniczne Polski i Białorusi z doklejoną ręką najemnika z naszywką Grupy Wagnera, co miało sugerować, że członkowie tej organizacji infiltrują terytorium Polski. Analiza obrazów jednoznacznie wykazała jednak, że zostały one zmanipulowane. Podobne działania prowadzono wobec Litwy i Łotwy. W dniu 11 sierpnia 2023 r. ABW zatrzymała dwóch Rosjan, którzy na zlecenie rosyjskiego wywiadu kolportowali na terenie Krakowa i Warszawy materiały propagandowe Grupy Wagnera[71].

---

[68] *Operacja RENGAW. Na granicy polsko-białoruskiej rozpoczyna działanie wojskowe zgrupowanie zadaniowe*, gov.pl, 12 VIII 2023 r., https://www.gov.pl/web/obrona-narodowa/operacja-rengaw-na-granicy-polsko--bialoruskiej-rozpoczyna-dzianie-wojskowe-zgrupowanie-zadaniowe [dostęp: 26 I 2024].

[69] A.M. Dyner, W. Lorenz, F. Bryjka, *Grupa Wagnera na Białorusi – konsekwencje dla NATO i UE…*

[70] I. Kacprzak, *Wagnerowcy sieją zamęt na granicy. Ponad połowa Polaków uważa, że stanowią zagrożenie*, Rzeczpospolita, 1 VIII 2023 r., https://www.rp.pl/spoleczenstwo/art38884031-wagnerowcy-sieja--zamet-na-granicy-ponad-polowa-polakow-uwaza-ze-stanowia-zagrozenie [dostęp: 1 VIII 2023].

[71] *ABW zatrzymała 2 obywateli Rosji*, gov.pl, 14 VIII 2023 r., https://www.gov.pl/web/sluzby-specjalne/abw-zatrzymala-2-obywateli-rosji [dostęp: 14 VIII 2023].

Rozpad imperium Prigożyna

Rosyjscy dziennikarze śledczy zidentyfikowali ponad 400 firm powiązanych z Prigożynem[72]. Aktywa te są przejmowane przez oligarchów lojalnych wobec Putina, jednak szczegóły tego procesu nie są w pełni znane. Rozgrywka koncentruje się na dwóch segmentach kryminalno-biznesowej działalności Prigożyna:

1) imperium medialnym wykorzystywanym do prowadzenia operacji wpływu, szerzenia propagandy i dezinformacji oraz ingerowania w procesy polityczne państw Zachodu,
2) spółkach wykorzystywanych do eksploatacji surowców naturalnych w Afryce i Syrii, gdzie w zamian za świadczenie usług wojskowych przez Grupę Wagnera, firmy Prigożyna otrzymywały kontrakty na wydobycie m.in. ropy naftowej, złota, diamentów czy na wycinkę lasów.

Według dziennikarzy „The New York Times" pierwszy sektor został przejęty przez Służbę Wywiadu Zagranicznego FR (Служба Внешней Разведки Российской Федерации, SWR), a drugi znajduje się pod kontrolą GRU i Ministerstwa Obrony[73].

Jeszcze w trakcie tzw. marszu sprawiedliwości na Moskwę Federalna Służba ds. Nadzoru w Sferze Łączności, Technologii Informacyjnych i Komunikacji Masowej, Roskomnadzor (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, Роскомнадзор) zablokowała komunikaty ze strony rosyjskiej organizacji medialnej Patriot Media Group, którą następnie rozwiązano[74]. Należała do niej m.in. agencja RIA FAN, w której Prigożyn pełnił funkcję szefa rady nadzorczej. Ponadto w skład medialnych aktywów Prigożyna od 2013 r. wchodziły farmy trolli i botów, kanały w serwisie Telegram oraz blogerzy biorący udział w rosyjskich operacjach dezinformacyjnych. Media Prigożyna zostały najprawdopodobniej przejęte przez państwowe korporacje, kierowane m.in. przez holding Jurija Kowalczuka lub jednego z dyrektorów państwowego Rostechu Wasilija Browkę[75].

---

[72] *Прошлое и будущее Пригожина. Как владелец ЧВК «Вагнер» создал свою армию – и что будет делать после мятежа*, Досье, 6 VII 2023 r., https://dossier.center/wagner-fall/ [dostęp: 6 VII 2023].

[73] A. Troianovski i in., *After Prigozhin's Death, a High-Stakes Scramble for His Empire*, The New York Times, 8 IX 2023 r., https://www.nytimes.com/2023/09/08/world/europe/prigozhin-wagner-russia-africa.html [dostęp: 8 IX 2023].

[74] *Yevgeny Prigozhin reportedly dissolving Patriot Media Group, home of his 'troll factory'*, Meduza, 30 VI 2023 r., https://meduza.io/en/news/2023/06/30/prigozhin-reportedly-dissolving-patriot-media-group-home-of-his-troll-factory [dostęp: 30 VI 2023].

[75] J. Czerep, A. Legucka, *Przyszłość „imperium" Prigożyna*, PISM, 17 VII 2023 r., https://www.pism.pl/publikacje/przyszlosc-imperium-prigozyna [dostęp: 17 VII 2023]; A. Stognei, M. Seddon, *Yevgeny*

W trakcie przejmowania aktywów medialnych Prigożyna przedstawiciele rosyjskich władz (m.in. Siergiej Ławrow i Dmitrij Pieskow) zapewniali, że Grupa Wagnera będzie kontynuować swoje operacje w Afryce, gdzie przebywa 4000–5000 najemników[76]. W rzeczywistości jednak GRU i Ministerstwo Obrony podejmowały działania przygotowujące grunt do przejęcia tej sfery imperium Prigożyna. W Syrii członkowie Grupy Wagnera byli przymuszani do podpisywania kontraktów z Ministerstwem Obrony[77]. Następnie odebrano im dostęp do wojskowej bazy lotniczej Humajmim, wykorzystywanej do zaopatrywania operacji w Syrii i RŚA, gdzie jest rozmieszczonych 1900 najemników[78].

W połowie sierpnia na targach zbrojeniowych Armia-2023 pod Moskwą gen. Szojgu namawiał przedstawicieli państw afrykańskich, by nie korzystali z usług Grupy Wagnera, lecz współpracowali wyłącznie z firmami podporządkowanymi Ministerstwu Obrony. Groził przy tym zerwaniem współpracy wojskowo-technicznej i wycofaniem wsparcia dyplomatycznego Rosji w ONZ[79]. W przededniu swojej śmierci szef wagnerowców opublikował filmy nagrane w jednym z państw w Afryce

Prigozhin's 'toxic' media empire left in Kremlin limbo, Financial Times, 14 VII 2023 r., https://www.ft.com/content/723a967f-213b-45b4-8ca6-792aa8e10ba0?shareType=nongift [dostęp: 14 VII 2023].

[76] Zob. szerzej: J. Stanyard, T. Vircoulon, J. Rademeyer, *The Grey Zone: Russia's military, mercenary and criminal engagement in Africa*, Global Initiative Against Transnational Organized Crime, 16 II 2023 r., https://globalinitiative.net/analysis/russia-in-africa/ [dostęp: 16 II 2023]; *Guns for gold: the Wagner Network exposed*, House of Commons Foreign Affairs Committee, 26 VII 2023 r., https://committees.parliament.uk/publications/41073/documents/200048/default/ [dostęp: 26 VII 2023]; E. Pokalova, *The Wagner Group in Africa: Russia's Quasi-State Agent of Influence*, „Studies in Conflict & Terrorism". https://doi.org/10.1080/1057610X.2023.2231642; M. Weiss, P. Vaux, *The Company You Keep: Yevgeny Prigozhin's Influence Operations in Africa*, Free Russia Foundation, Washington 2020, https://www.4freerussia.org/wp-content/uploads/sites/3/2020/09/The-Company-You-Keep-Yevgeny-Prigozhins-Influence-Operations-in-Africa.pdf [dostęp: 16 II 2023]; L. Serwat, H. Nsaibia, N. Gurcov, *Moving Out of the Shadows: Shifts in Wagner Group Operations Around the World*, The Armed Conflict Location & Event Data Project (ACLED), 2 VIII 2023 r., https://acleddata.com/2023/08/02/moving-out-of-the-shadows-shifts-in-wagner-group-operations-around-the-world/#exec [dostęp: 2 VIII 2023]; G. Kuczyński, *Wagnerowcy. Psy wojny Putina*, Warszawa 2022.

[77] S. Al-Khalidi, M. Gebeily, *Syria brought Wagner fighters to heel as mutiny unfolded in Russia*, Reuters, 7 VII 2023 r., https://www.reuters.com/world/syria-brought-wagner-group-fighters-heel-mutiny-unfolded-russia-2023-07-07/ [dostęp: 7 VII 2023].

[78] Na początku lipca najprawdopodobniej wycofano z RŚA ok. 1/4 (500–600) najemników. Zob. J. Yongo, *Central African Republic says Wagner troop movement is rotation not departure*, Reuters, 8 VII 2023 r., https://www.reuters.com/world/africa/central-african-republic-says-wagner-troop-movement-is-rotation-not-departure-2023-07-08/ [dostęp: 8 VII 2023].

[79] G. De Vries, *The Russian Ministry of Defense forces the countries at the Army 2023 forum to refuse to cooperate with PMC Wagner*, Savanna News, 15 VI 2023 r., https://savannanews.com/the-russian-ministry-of-defense-forces-the-countries-at-the-army-2023-forum-to-refuse-to-cooperate-with-pmc-wagner/ [dostęp: 15 VI 2023].

(najprawdopodobniej RŚA lub Mali), w których zapewniał o kontynuacji operacji na tym kontynencie[80]. W tym samym czasie jednak gen. Jewkurow rozpoczął serię wizyt dyplomatycznych w Afryce i na Bliskim Wschodzie (do połowy września był m.in. w Libii, Syrii, Burkina Faso, Mali, Algierii, Sudanie i Nigrze), gdzie omawiał nowe reguły współpracy wojskowej z Rosją. Najprawdopodobniej dotyczyły one m.in. kwestii świadczenia usług wojskowych przez firmy nadzorowane przez Ministerstwo Obrony[81].

W spotkaniach tych często uczestniczył zastępca szefa wywiadu wojskowego GRU gen. Andriej Awerjanow – dowódca Służby Działań Specjalnych GRU (jednostka nr 29155), odpowiedzialnej m.in. za próbę otrucia Siergieja Skripala w Wielkiej Brytanii, ingerencje w wybory w USA, a także działania wywrotowe w Europie (m.in. w Czechach, Bułgarii, Mołdawii i Czarnogórze)[82]. Według doniesień medialnych to właśnie gen. Awerjanow opracował plan całkowitego przejęcia afrykańskich aktywów Prigożyna. Plan ten zawierał m.in. koncepcję stworzenia liczącego 20 000 najemników Rosyjskiego Korpusu Ekspedycyjnego, którego trzon mają stanowić żołnierze Specnazu[83]. W tym procesie miał uczestniczyć także handlarz bronią Wiktor But, który jest związany z GRU i ma duże doświadczenie w działalności wojskowo-biznesowej w Afryce. Prigożyn przeciwstawiał się tym planom, a jego wzmożona aktywność na tym kontynencie była próbą utrzymania realizowanych kontraktów.

Proces rozpadu imperium Prigożyna przypieczętowała jego śmierć w katastrofie samolotowej, do której doszło 23 sierpnia 2023 r. w obwodzie twerskim. Według Federalnej Agencji Transportu Lotniczego na pokładzie prywatnego odrzutowca Embraer Legacy 600 nr RA-02795 lecącego z Moskwy do Petersburga znajdowało się siedem osób z kierownictwa Grupy Wagnera, w tym szef najemników Prigożyn, główny dowódca wojskowy Utkin i szef ds. bezpieczeństwa Walerij Czekałow. Zginęli wszyscy pasażerowie i trzyosobowa załoga. W dniu 27 sierpnia rosyjski

[80] *Russia's Prigozhin posts first video since mutiny, hints he is in Africa*, Reuters, 22 VIII 2023 r., https://www.reuters.com/world/africa/russias-prigozhin-posts-first-video-since-mutiny-hints-hes-africa-2023-08-21/ [dostęp: 22 VIII 2023].

[81] *ЧВК «Вагнер» предложила бойцам найти другую работу из-за конкуренции с Минобороны и Росгвардией в Африке и на Ближнем Востоке*, Важные истории, 30 VIII 2023 r., https://storage.googleapis.com/istories/news/2023/08/30/chvk-vagner-predlozhila-boitsam-naiti-druguyu-rabotu-iz-za-konkurentsii-s-minoboroni-i-rosgvardiei-v-afrike-i-na-blizhnem-vostoke/index.html [dostęp: 30 VIII 2023].

[82] M. Schwirtz, *Top Secret Russian Unit Seeks to Destabilize Europe*, The New York Times, 8 X 2019 r., https://www.nytimes.com/2019/10/08/world/europe/unit-29155-russia-gru.html [dostęp: 8 X 2019].

[83] *Putin Moves to Seize Control of Wagner's Mercenary Empire*, Bloomberg, 31 VIII 2023 r., https://www.bloomberg.com/news/articles/2023-08-31/russia-moves-to-seize-control-of-wagner-empire-after-yevgeny-prigozhin-s-death#xj4y7vzkg [dostęp: 31 VIII 2023].

Komitet Śledczy stwierdził, że badania genetyczne potwierdziły, że wśród ofiar byli Prigożyn i Utkin[84].

Wyeliminowanie kierownictwa Grupy Wagnera ma związek z nieudanym buntem przeprowadzonym w nocy z 23 na 24 czerwca 2023 r. i było korzystne dla rosyjskiej armii i samego Putina. Przez dokonanie osobistej zemsty prezydent umocnił swoją pozycję, ustabilizował system władzy oparty na strachu, a także wysłał jasny komunikat do potencjalnych buntowników. Wzmocnienie jego autorytetu było ważne w obliczu braku postępów na ukraińskim froncie, spadku wartości rubla oraz w perspektywie wyborów prezydenckich w 2024 r. Bunt Prigożyna, niezależnie od jego losów, unaocznił rosyjskim elitom władzy słabość systemu putinowskiego, który nie gwarantuje im bezpieczeństwa i przychodów[85].

Pogrzeb Prigożyna miał charakter zamknięty. Odbył się 29 sierpnia na cmentarzu Porochowskim w Petersburgu bez ceremoniału wojskowego. Putin nie uczestniczył w uroczystości, a jedynie publicznie odniósł się do znajomości z Prigożynem sięgającej lat 90. XX w. Swojego protegowanego scharakteryzował jako osobę, która miała „trudny los" i „popełniła poważne błędy". Podkreślił jednak „lojalność Prigożyna, aż do śmierci" i „zasługi dla wspólnej sprawy"[86]. Władze do ostatniej chwili trzymały w tajemnicy, kiedy i gdzie zostanie pochowany szef najemników. Protokół wydarzenia był uzgadniany między Kremlem a FSB. Zdecydowano, że pogrzeb nie będzie otwarty, by nie tworzyć mitu Prigożyna jako męczennika. Jeden z funkcjonariuszy FSB miał stwierdzić, że (…) *Prigożyn był bohaterem ludu, a my nie potrzebujemy bohaterów, którzy maszerowali na Moskwę*[87].

W celu zamaskowania prawdopodobnego udziału Kremla w eliminacji buntownika rosyjskie kanały dezinformacyjne rozpowszechniały kłamstwa sugerujące, że za śmierć Prigożyna odpowiadają zachodnie i ukraińskie służby specjalne, które przeprowadziły „zamach terrorystyczny"[88]. Nie wierzą w to jednak nawet sami

---

[84] *Russia says genetic tests confirm Prigozhin died in plane crash*, Reuters, 27 VIII 2023 r., https://www.reuters.com/world/europe/russias-investigators-confirm-wagner-mercenary-chief-prigozhin-died-plane-crash-2023-08-27/ [dostęp: 27 VIII 2023].

[85] A. Legucka, F. Bryjka, *Konsekwencje śmierci Jewgienija Prigożyna*, PISM, 24 VIII 2023 r., https://www.pism.pl/publikacje/konsekwencje-smierci-jewgienija-prigozyna [dostęp: 24 VIII 2023].

[86] *Putin breaks silence over Prigozhin's reported death*, BBC, 24 VIII 2023 r., https://www.bbc.com/news/world-europe-66609678 [dostęp: 26 I 2024].

[87] '*We don't need heroes who marched on Moscow*': *Kremlin and FSB decided to bury Yevgeny Prigozhin secretly, without military honors*, Meduza, 30 VIII 2023 r., https://meduza.io/en/news/2023/08/30/we-don-t-need-heroes-who-marched-on-moscow-kremlin-and-fsb-decided-to-bury-yevgeny-prigozhin-secretly-without-military-honors [dostęp: 30 VIII 2023].

[88] *DISINFO: The West is behind the terrorist attack on Prigozhin*, EUvsDisinfo, 29 VIII 2023 r., https://euvsdisinfo.eu/report/the-west-is-behind-the-terrorist-attack-on-prigozhin [dostęp: 29 VIII 2023].

Rosjanie. Według badań sondażowych przeprowadzonych przez Centrum Lewady[89] zaledwie 14% Rosjan zgadza się z oficjalną linią narracyjną Kremla. Większość respondentów (26%) zdarzenie w obwodzie twerskim nazwała tragicznym wypadkiem, a 20% wprost sądzi, że Prigożyn został zamordowany przez władze za tzw. marsz sprawiedliwości na Moskwę. Doniesieniom tym zaprzeczył rzecznik Kremla Pieskow, określając je „absolutnym kłamstwem"[90]. Z kolei 16% respondentów to zwolennicy teorii spiskowych (rozpowszechnianych m.in. w serwisie Telegram przez kanały powiązane z Grupą Wagnera) sugerujących, że Prigożyn „żyje gdzieś w Afryce", a katastrofa samolotu została zainscenizowana. Prawie 1/4 respondentów (22%) miała trudności z udzieleniem odpowiedzi. Jednym z czynników wpływających na odporność na dezinformację Kremla w tym konkretnym przypadku może być wysokie poparcie dla działań Prigożyna, które w sierpniu 2023 r. wynosiło 39%[91].

Śmierć szefa najemników i ich dowódcy doprowadziła do głębokich zmian w kierownictwie Grupy Wagnera i postawiła pod znakiem zapytania przyszłość tej formacji zbrojnej. Według kanałów związanych z wagnerowcami po śmierci Prigożyna dowodzenie przejął Anton Jelizarow ps. „Lotos" – oficer Specnazu, pod którego dowództwem wagnerowcy zdobyli Sołedar[92]. Został on usunięty z armii za fałszowanie dokumentów. Wśród potencjalnych następców Prigożyna i Utkina wymieniano osoby odpowiadające za operacje wojskowe, biznesowe i polityczne w Afryce (Witalij Pierfiljew, Dmitrij Sytyj, Maksim Szugalej), a także ze ścisłego dowództwa, jak Aleksandr Kuzniecow ps. „Ratibor" czy Andriej Bogatow ps. „Brodyaga". Inne źródła wskazywały, że aktywami Grupy Wagnera zarządza syn Prigożyna – Paweł[93].

Po śmierci Prigożyna zlikwidowano ok. 1/3 obozu wagnerowców w Osipowiczach na Białorusi[94]. Część białoruskiego kontyngentu została przerzucona do

---

[89] *Запомнившиеся события августа, смерть Пригожина*, Левада Центр, 1 IX 2023 r., https://www.levada.ru/2023/09/01/zapomnivshiesya-sobytiya-avgusta-smert-prigozhina/ [dostęp: 1 IX 2023].

[90] *Песков опроверг утверждения о причастности Кремля к крушению самолета Пригожина*, Интерфакс, 25 VIII 2023 r., https://www.interfax.ru/russia/917796 [dostęp: 25 VIII 2023].

[91] *Запомнившиеся события августа, смерть Пригожина*…

[92] *Anton Yelizarov from „Wagner". He commanded the offensive on Soledar, killing many of Ukrainian soldiers*, Molfar, https://molfar.com/en/blog/komanduvav-nastupom-na-soledar-vbiv-bagato-nashih-deanon-ielizarova-z-vagnera [dostęp: 26 I 2024].

[93] M. Droin, T. Dolbaia, *Post-Prigozhin Russia in Africa. Regaining or Losing Control?*, Center for Strategic and International Studies, 20 IX 2023 r., https://www.csis.org/analysis/post-prigozhin-russia-africa-regaining-or-losing-control [dostęp: 20 IX 2023].

[94] *Satellite Images Show Wagner Camp In Belarus Being Dismantled*, Radio Free Europe/Radio Liberty, 24 VIII 2023 r., https://www.rferl.org/a/belarus-satellite-images-wagner-camp-dismantled/32563104.html [dostęp: 24 VIII 2023].

Afryki, a pozostali wrócili do Rosji. Według ukraińskiego wywiadu wojskowego na Białorusi pozostaje co najwyżej 1000 wagnerowców, z czego 200–500 w roli instruktorów[95]. Nie można wykluczyć, że docelowo zostaną oni oficjalnie wcieleni do białoruskiej armii jako szkoleniowcy. Pod koniec grudnia 2023 r. pojawiły się także niepotwierdzone informacje wskazujące na to, że wagnerowcy trafili do nowej jednostki sił specjalnych wojsk wewnętrznych „Tarnada" (pol. Tornado), która powstała do walki z grupami dywersyjno-rozpoznawczymi i nielegalnymi grupami zbrojnymi[96]. Część z nich może także otrzymać ofertę pracy w Afryce od białoruskiej firmy wojskowej Guard Service, która jest powiązana z bliskim współpracownikiem Łukaszenki – Wiktorem Szejmanem[97].

Na początku listopada 2023 r. Kartapołow stwierdził, że Grupa Wagnera została w całości rozwiązana[98]. Jej aktywa są przejmowane przez firmy kontrolowane przez Ministerstwo Obrony (głównie Redut i Korpus Afrykański). Ich aktywność operacyjna w Afryce opiera się jednak (przynajmniej częściowo) na infrastrukturze i zasobach ludzkich Grupy Wagnera. Byli wagnerowcy powracają także na front ukraiński, gdzie walczą m.in. w rejonie Awdijiwki i Bachmutu[99] w strukturach Brygady Międzynarodowej DNR (tzw. Piętnastki) oraz Rosgwardii, w tym czeczeńskiego specnazu „Achmat" (jednostka Kamerton)[100]. Nadzór nad „formacjami ochotniczymi" – jak rosyjskie władze eufemistycznie określają półprywatne firmy wojskowe walczące w Ukrainie – sprawuje Andriej Troszew ps. „Siedoj", który przez lata był zastępcą Utkina i szefem sztabu Grupy Wagnera[101]. Wcześniej pełnił on funkcję łącznika między wagnerowcami a Kremlem i rosyjską armią. Zarządzał

---

[95] *В Білорусі лишилось менше 1000 терористів з «пвк «вагнер»*, Центр Національного спротиву, 18 IX 2023 r., https://sprotyv.mod.gov.ua/v-bilorusi-lyshylos-menshe-1000-terorystiv-z-pvk-vagner/ [dostęp: 18 IX 2023].

[96] *Najemnicy z Grupy Wagnera zasilili białoruski specnaz*, Belsat, 16 XII 2023 r., https://belsat.eu/pl/news/16-12-2023-najemnicy-z-grupy-wagnera-zasilili-bialoruski-specnaz [dostęp: 26 I 2024].

[97] *Вагнерівці, які підписали контракт з білоруською ПВК, відправляють в Африку*, Центр Національного спротиву, 12 IX 2023 r., https://sprotyv.mod.gov.ua/vagnerivtsi-yaki-pidpysaly-kontrakt-z-biloruskoyu-pvk-vidpravlyayut-v-afryku/ [dostęp: 12 IX 2023].

[98] *Картаполов заявил об окончательном расформировании ЧВК «Вагнер»*, РБК, 2 XI 2023 r., https://www.rbc.ru/politics/02/11/2023/6543d4389a794741e8fa258e [dostęp: 3 XI 2023].

[99] А. Степура, *Колишні бійці «Вагнера» справді перебувають на Бахмутському напрямку, це психологічна операція*, Суспільне Новини, 27 IX 2023 r., https://suspilne.media/581703-kolisni-bijci-vagnera-spravdi-perebuvaut-na-bahmutskomu-napramku-ce-psihologicna-operacia-evlas/ [dostęp: 27 IX 2023].

[100] *В «Ахмате» рассказали о массовом пополнении из экс-бойцов «Вагнера»*, Риа Новости, 28 X 2023 r., https://ria.ru/20231028/akhmat-1905834455.html [dostęp: 28 X 2023].

[101] *Встреча с Юнус-Беком Евкуровым и Андреем Трошевым*, Kremlin.ru, 29 IX 2023 r., https://kremlin.ru/events/president/news/72391 [dostęp: 29 IX 2023].

także stowarzyszeniem Liga zrzeszającym weteranów, które było jednym z kanałów rekrutacji. Troszew nie poparł buntu Prigożyna i wraz z grupą dziesięciu dowódców Grupy Wagnera podpisał kontrakt z Ministerstwem Obrony[102] i firmą wojskową Redut współfinansowaną przez Giennadija Timczenkę i Olega Dieripaskę.

Podsumowanie

Bunt Prigożyna był najpoważniejszym dotychczas przejawem niestabilności reżimu Putina. Niepowodzenie tej rebelii wynika przede wszystkim z tego, że nie poparły jej elity polityczne, struktury siłowe czy część armii. Pozostawieni sami sobie wagnerowcy nie byli przy tym wystarczająco zdeterminowani, by zrealizować swoje cele. Mimo że główną przyczyną rebelii Grupy Wagnera był konflikt między szefem najemników a elitami wojskowymi, zbrojny marsz wagnerowców na Moskwę osłabił wizerunek prezydenta, od lat 90. XX w. utrzymującego bliskie relacje z Prigożynem. Nielojalność protegowanego, który odważył się zawiązać spisek przeciwko rosyjskiemu państwu, nie została wybaczona, a udzielone buntownikowi gwarancje bezpieczeństwa okazały się zupełnie niewiarygodne. W ciągu dwóch miesięcy od buntu do śmierci Prigożyna rosyjskie władze dokonały punktowych czystek w wojsku, nie przeprowadziły jednak gruntownych zmian kadrowych. W celu ustabilizowania sytuacji wewnętrznej wzmocniono Rosgwardię oraz usunięto z przestrzeni informacyjnej część ultranacjonalistycznych krytyków Kremla i Ministerstwa Obrony. Mimo chwilowego kryzysu reżim Putina umacnia się oraz zaostrza mechanizmy kontroli i represji wobec przeciwników. Nie należy zatem zakładać, że w najbliższej perspektywie dojdzie do istotnych rozłamów w rosyjskiej elicie władzy.

Dla Grupy Wagnera bunt Prigożyna okazał się z kolei początkiem końca jej działalności. Sprawne przejmowanie zasobów wagnerowców przez konkurencyjne firmy wojskowe kontrolowane przez Ministerstwo Obrony i GRU można uznać za sukces pozwalający odbudować wizerunek władzy po rebelii. Podział aktywów Prigożyna między kilka podmiotów ma najprawdopodobniej zapobiec monopolizacji sektora usług wojskowych przez jedną z firm. Podporządkowanie ich Ministerstwu Obrony ułatwi sprawowanie nad nimi kontroli operacyjnej, jednak osłabi rosyjskie zdolności do wiarygodnego zaprzeczania związkom z nimi. Mimo rebelii wagnerowców – zdaniem autora – Rosja nie zrezygnuje z korzystania z usług półprywatnych

[102] *Wagner's second-in-command Troshev sided against Prigozhin during the coup – report*, The New Voice of Ukraine, 18 VII 2023 r., https://news.yahoo.com/wagner-second-command-troshev-sided-015200321.html [dostęp: 18 VII 2023].

firm zbrojnych w Ukrainie, na Bliskim Wschodzie czy w Afryce. Z polskiej perspektywy najważniejsza jest sprawa obecności rosyjskich najemników na Białorusi, gdzie mogą być angażowani w destabilizację sytuacji na granicy. Dlatego w interesie Polski leży wzmocnienie komunikacji strategicznej NATO w tej kwestii. Sojusz powinien wysyłać wyraźny sygnał, że wszelkie prowokacje z udziałem Grupy Wagnera i ich następców mogą zostać uznane za agresję. NATO powinno przygotować elastyczną koncepcję odpowiedzi na różne formy ich działań destabilizujących jego wschodnią flankę i państwa Globalnego Południa.

Bibliografia

Bryjka F., *Grupa Wagnera – paramilitarne narzędzie rosyjskich operacji hybrydowych*, „Sprawy Międzynarodowe" 2022, t. 75, nr 2, s. 68–91. https://doi.org/10.35757/SM.2022.75.2.05.

Darczewska J., *Rosgwardia. Siły specjalnego przeznaczenia*, „Punkt Widzenia OSW" 2020, nr 78.

Gabidullin M., *Wagnerowiec. Spowiedź byłego dowódcy tajnej armii Putina*, Kraków 2022.

Kuczyński G., *Wagnerowcy. Psy wojny Putina*, Warszawa 2022.

Larsen K.P., *From mercenary to legitimate actor? Russian discourses on private military companies*, „Post-Soviet Affairs" 2023, t. 39, nr 6, s. 420–439. https://doi.org/10.1080/1060586X.2023.2247782.

Pokalova E., *The Wagner Group in Africa: Russia's Quasi-State Agent of Influence*, „Studies in Conflict & Terrorism". https://doi.org/10.1080/1057610X.2023.2231642.

Wojnowski M., *Geneza, teoria i praktyka rosyjskiej inżynierii przymusowej migracji. Przyczynek do badań nad kryzysem migracyjnym na wschodniej flance NATO*, „Przegląd Bezpieczeństwa Wewnętrznego" 2022, nr 26, s. 11–49. https://doi.org/10.4467/20801335PBW.21.034.15694.

Źródła internetowe

ABW zatrzymała 2 obywateli Rosji, gov.pl, 14 VIII 2023 r., https://www.gov.pl/web/sluzby-specjalne/abw-zatrzymala-2-obywateli-rosji [dostęp: 14 VIII 2023].

Al-Khalidi S., Gebeily M., *Syria brought Wagner fighters to heel as mutiny unfolded in Russia*, Reuters, 7 VII 2023 r., https://www.reuters.com/world/syria-brought-wagner-group-fighters-heel-mutiny-unfolded-russia-2023-07-07/ [dostęp: 7 VII 2023].

Anton Yelizarov from „Wagner". He commanded the offensive on Soledar, killing many of Ukrainian soldiers, Molfar, https://molfar.com/en/blog/komanduvav-nastupom-na-soledar-vbiv-bagato-nashih-deanon-ielizarova-z-vagnera [dostęp: 26 I 2024].

Belton C., Harris S., Miller G., *Putin appeared paralyzed and unable to act in first hours of rebellion*, The Washington Post, 25 VII 2023 r., https://www.washingtonpost.com/world/2023/07/25/putin-prigozhin-rebellion-kremlin-disarray/ [dostęp: 25 VII 2023].

Ber J., *Od Popasnej do Bachmutu. Grupa Wagnera w wojnie rosyjsko-ukraińskiej*, OSW, 28 IV 2023 r., https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2023-04-28/od-popasnej-do-bachmutu-grupa-wagnera-w-wojnie-rosyjsko [dostęp: 28 IV 2023].

Blakely R., *Russian mercenaries killed by US troops in Syria gun battle*, The Times, 14 II 2018 r., https://www.thetimes.co.uk/article/russia-mercenaries-killed-by-us-troops-in-syria-gun-battle-g5zswflfg [dostęp: 19 I 2024].

Bryjka F., *Transformacja Grupy Wagnera w związku z wojną na Ukrainie*, PISM, 7 III 2023 r., https://www.pism.pl/publikacje/transformacja-grupy-wagnera-w-zwiazku-z-wojna-na-ukrainie [dostęp: 7 III 2023].

Celem wagnerowców na Białorusi będzie „przejęcie Przesmyku Suwalskiego" – rosyjski deputowany, Belsat, 16 VII 2023 r., https://belsat.eu/pl/news/16-07-2023-celem-wagnerowcow-na-bialorusi-bedzie-przejecie-przesmyku-suwalskiego-rosyjski-deputowany [dostęp: 16 VII 2023].

Chornogor Y., Rad P., Chernysh A., *Anatomy of "Wagner PMC": creation, war in Ukraine and ways of countering the group*, Ukrainian PRISM, kwiecień 2023 r., https://prismua.org/wp-content/uploads/2023/05/PMC_Wagner_eng.pdf [dostęp: 28 IV 2023].

Czerep J., Legucka A., *Przyszłość „imperium" Prigożyna*, PISM, 17 VII 2023 r., https://www.pism.pl/publikacje/przyszlosc-imperium-prigozyna [dostęp: 17 VII 2023].

De Vries G., *The Russian Ministry of Defense forces the countries at the Army 2023 forum to refuse to cooperate with PMC Wagner*, Savanna News, 15 VI 2023 r., https://savannanews.com/the-russian-ministry-of-defense-forces-the-countries-at-the-army-2023-forum-to-refuse-to-cooperate-with-pmc-wagner/ [dostęp: 15 VI 2023].

DISINFO: The West is behind the terrorist attack on Prigozhin, EUvsDisinfo, 29 VIII 2023 r., https://euvsdisinfo.eu/report/the-west-is-behind-the-terrorist-attack-on-prigozhin [dostęp: 29 VIII 2023].

Droin M., Dolbaia T., *Post-Prigozhin Russia in Africa. Regaining or Losing Control?*, Center for Strategic and International Studies, 20 IX 2023 r., https://www.csis.org/analysis/post-prigozhin-russia-africa-regaining-or-losing-control [dostęp: 20 IX 2023].

Dyner A.M., *Grupa Wagnera na Białorusi – potencjalne zagrożenia dla Polski*, PISM, 27 VII 2023 r., https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-potencjalne-zagrozenia-dla-polski [dostęp: 27 VII 2023].

Dyner A.M., *Znaczenie buntu Prigożyna dla rosyjskiej polityki bezpieczeństwa*, PISM, 26 VI 2023 r., https://www.pism.pl/publikacje/znaczenie-buntu-prigozyna-dla-rosyjskiej-polityki-bezpieczenstwa [dostęp: 26 VI 2023].

Dyner A.M., Lorenz W., Bryjka F., *Grupa Wagnera na Białorusi – konsekwencje dla NATO i UE*, PISM, 7 IX 2023 r., https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-konsekwencje-dla-nato-i-ue [dostęp: 7 IX 2023].

Galeotti M., *Russia's coup d'état – Nature and Implications*, In Moscow's Shadows, 27 VI 2023 r., https://inmoscowsshadows.wordpress.com/2023/06/27/scss10-26-june-2023-russias-coup-detat-nature-and-implications/ [dostęp: 27 VI 2023].

Gordon M.R. i in., *Early Intelligence Suggests Prigozhin Was Assassinated, U.S. Officials Say*, The Wall Street Journal, 24 VIII 2023 r., https://www.wsj.com/world/russia/wagner-prigozhin-russia-assassinated-intelligence-3e456fab [dostęp: 24 VIII 2023].

Grove T., Cullison A., Pancevski B., *How Putin's Right-Hand Man Took Out Prigozhin*, The Wall Street Journal, 22 XII 2023 r., https://www.wsj.com/world/russia/putin-patrushev-plan-prigozhin-assassination-428d5ed8?mod=hp_lead_pos7 [dostęp: 26 I 2024].

Guns for gold: the Wagner Network exposed, House of Commons Foreign Affairs Committee, 26 VII 2023 r., https://committees.parliament.uk/publications/41073/documents/200048/default/ [dostęp: 26 VII 2023].

Harris S., Khurshudyan I., *Wagner chief offered to give Russian troop locations to Ukraine*, The Washington Post, 15 V 2023 r., https://www.washingtonpost.com/national-security/2023/05/14/prigozhin-wagner-ukraine-leaked-documents/ [dostęp: 15 V 2023].

Hird K. i in., *Russian Offensive Campaign Assessment, March 10, 2023*, Institute for the Study of War, 10 III 2023 r., https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-march-10-2023 [dostęp: 10 III 2023].

Ivanova P., Stognei A., Seddon M., *Russian insurrection: Prigozhin's failed mutiny and the fallout*, Financial Times, 23 VI 2023 r., https://www.ft.com/content/34f3a349-a05f-4672-b059-6980ecc27adf [dostęp: 23 VI 2023].

Jailed former 'Donetsk People's Republic' militia leader to run for president, Novaya Gazeta Europe, 31 VIII 2023 r., https://novayagazeta.eu/articles/2023/08/31/jailed-former-donetsk-peoples-republic-militia-leader-to-run-for-president-en-news [dostęp: 31 VIII 2023].

Jawor A., *Rosyjskie służby po buncie Prigożyna. Putin wyrównuje szeregi w kremlowskich wieżach*, InfoSecurity24, 31 VII 2023 r., https://infosecurity24.pl/za-granica/rosyjskie-sluzby-po-buncie-prigozyna-putin-wyrownuje-szeregi-w-kremlowskich-wiezach [dostęp: 31 VII 2023].

Journalists identify head of Wagner Group forces in Belarus as 46-year-old Ukraine native, Meduza, 26 VII 2023 r., https://meduza.io/en/news/2023/07/26/journalists-identify-head-of-wagner-forces-in-belarus-as-46-year-old-ukraine-native [dostęp: 26 VII 2023].

Kacprzak I., *Wagnerowcy sieją zamęt na granicy. Ponad połowa Polaków uważa, że stanowią zagrożenie*, Rzeczpospolita, 1 VIII 2023 r., https://www.rp.pl/spoleczenstwo/art38884031-wagnerowcy-sieja-zamet-na-granicy-ponad-polowa-polakow-uwaza-ze-stanowia-zagrozenie [dostęp: 1 VIII 2023].

Kirillova K., *Propaganda and Repression Turn Against Their Creators in Russia*, The Jamestown Foundation, 25 VII 2023 r., https://jamestown.org/program/propaganda-and-repression-turn-against-their-creators-in-russia/ [dostęp: 25 VII 2023].

Komin M., *"Fighting spirit": Russia's technocrat elite after the Wagner mutiny*, European Council on Foreign Relations, 24 VII 2023 r., https://ecfr.eu/article/fighting-spirit-russias-technocrat-elite-after-the-wagner-mutiny/ [dostęp: 24 VII 2023].

Legucka A., *Konsekwencje buntu Prigożyna dla systemu putinowskiego w Rosji*, PISM, 26 VI 2023 r., https://www.pism.pl/publikacje/konsekwencje-buntu-prigozyna-dla-systemu-putinowskiego-w-rosji [dostęp: 26 VI 2023].

Legucka A., Bryjka F., *Konsekwencje śmierci Jewgienija Prigożyna*, PISM, 24 VIII 2023 r., https://www.pism.pl/publikacje/konsekwencje-smierci-jewgienija-prigozyna [dostęp: 24 VIII 2023].

Legucka A., Bryjka F., *Rywalizacja między rosyjską armią a Grupą Wagnera*, PISM, 6 VI 2023 r., https://www.pism.pl/publikacje/rywalizacja-miedzy-rosyjska-armia-a-grupa-wagnera [dostęp: 6 VI 2023].

Mitzer S., Janovsky J., *Chef's Special – Documenting Equipment Losses During The 2023 Wagner Group Mutiny*, Oryx, 24 VI 2023 r., https://www.oryxspioenkop.com/2023/06/chefs-special-documenting-equipment.html [dostęp: 24 VI 2023].

Najemnicy z Grupy Wagnera zasilili białoruski specnaz, Belsat, 16 XII 2023 r., https://belsat.eu/pl/news/16-12-2023-najemnicy-z-grupy-wagnera-zasilili-bialoruski-specnaz [dostęp: 26 I 2024].

Operacja RENGAW. Na granicy polsko-białoruskiej rozpoczyna działanie wojskowe zgrupowanie zadaniowe, gov.pl, 12 VIII 2023 r., https://www.gov.pl/web/obrona-narodowa/operacja-rengaw-na-granicy-polsko--bialoruskiej-rozpoczyna-dzianie-wojskowe-zgrupowanie--zadaniowe [dostęp: 26 I 2024].

Pavel Gubarev, associate of Igor Strelkov, reportedly investigated for extremism, Meduza, 23 VII 2023 r., https://meduza.io/en/news/2023/07/23/pavel-gubarev-associate-of-igor-strelkov-reportedly-investigated-for-extremism [dostęp: 23 VII 2023].

Preiherman Y., *What Does Lukashenka's Role as Mediator in Russian Crisis Imply? – Analysis*, Eurasia Review, 29 VI 2023 r., https://www.eurasiareview.com/29062023-what-does-lukashenkas-role-as-mediator-in-russian-crisis-imply-analysis/ [dostęp: 29 VI 2023].

Prigożyn J., wpis na kanale Telegram, https://t.me/concordgroup_official/1002 [dostęp: 20 V 2023].

Prigożyn J., wpis na kanale Telegram, https://t.me/prigozhin_2023_tg/1844 [dostęp: 23 VI 2023].

Prigożyn J., wpis na kanale Telegram, https://t.me/Prigozhin_hat/3797 [dostęp: 23 VI 2023].

Putin breaks silence over Prigozhin's reported death, BBC, 24 VIII 2023 r., https://www.bbc.com/news/world-europe-66609678 [dostęp: 26 I 2024].

Putin Moves to Seize Control of Wagner's Mercenary Empire, Bloomberg, 31 VIII 2023 r., https://www.bloomberg.com/news/articles/2023-08-31/russia-moves-to-seize-control-of-wagner-empire-after-yevgeny-prigozhin-s-death#xj4y7vzkg [dostęp: 31 VIII 2023].

Putin says Wagner Group doesn't legally exist, Meduza, 14 VII 2023 r., https://meduza.io/en/news/2023/07/14/putin-says-wagner-group-no-longer-legally-exists [dostęp: 14 VII 2023].

Rana M., *Volodymyr Zelensky: Russian mercenaries ordered to kill Ukraine's president*, The Times, 28 II 2022 r., https://www.thetimes.co.uk/article/volodymyr-zelensky-russian--mercenaries-ordered-to-kill-ukraine-president-cvcksh79d [dostęp: 19 I 2024].

Russia says genetic tests confirm Prigozhin died in plane crash, Reuters, 27 VIII 2023 r., https://www.reuters.com/world/europe/russias-investigators-confirm-wagner-mercenary-chief-prigozhin-died-plane-crash-2023-08-27/ [dostęp: 27 VIII 2023].

Russia sentences former separatist commander and pro-war blogger Igor Strelkov to four years in prison, Meduza, 25 I 2024 r., https://meduza.io/en/news/2024/01/25/russia-sentences--former-separatist-commander-and-pro-war-blogger-igor-strelkov-to-four-years-in-prison [dostęp: 25 I 2024].

Russia's Prigozhin posts first video since mutiny, hints he is in Africa, Reuters, 22 VIII 2023 r., https://www.reuters.com/world/africa/russias-prigozhin-posts-first-video-since-mutiny-hints-hes-africa-2023-08-21/ [dostęp: 22 VIII 2023].

Sari A., *Hybrid CoE Paper 17: Instrumentalized migration and the Belarus crisis: Strategies of legal coercion*, Hybrid CoE, 25 IV 2023 r., https://www.hybridcoe.fi/publications/hybrid-coe-paper-17-instrumentalized-migration-and-the-belarus-crisis-strategies-of-legal-coercion/ [dostęp: 25 IV 2023].

Satellite Images Show Wagner Camp In Belarus Being Dismantled, Radio Free Europe/Radio Liberty, 24 VIII 2023 r., https://www.rferl.org/a/belarus-satellite-images-wagner-camp-dismantled/32563104.html [dostęp: 24 VIII 2023].

Schwirtz M., *Top Secret Russian Unit Seeks to Destabilize Europe*, The New York Times, 8 X 2019 r., https://www.nytimes.com/2019/10/08/world/europe/unit-29155-russia-gru.html [dostęp: 8 X 2019].

Serwat L., Nsaibia H., Gurcov N., *Moving Out of the Shadows: Shifts in Wagner Group Operations Around the World*, The Armed Conflict Location & Event Data Project (ACLED), 2 VIII 2023 r., https://acleddata.com/2023/08/02/moving-out-of-the-shadows-shifts-in-wagner-group-operations-around-the-world/#exec [dostęp: 2 VIII 2023].

Sprawa Prigożyna a tuszowanie słabości Rosji i rys na jej wizerunku militarnej potęgi, EUvsDisinfo, 29 VI 2023 r., https://euvsdisinfo.eu/pl/sprawa-prigozyna-a-tuszowanie-slabosci-rosji-i-rys-na-jej-wizerunku-militarnej-potegi/ [dostęp: 29 VI 2023].

Stanyard J., Vircoulon T., Rademeyer J., *The Grey Zone: Russia's military, mercenary and criminal engagement in Africa*, Global Initiative Against Transnational Organized Crime, 16 II 2023 r., https://globalinitiative.net/analysis/russia-in-africa/ [dostęp: 16 II 2023].

State Duma passes bill allowing Russia's National Guard troops to use heavy military equipment, Meduza, 19 VII 2023 r., https://meduza.io/en/news/2023/07/19/state-duma-passes-bill-allowing-russia-s-national-guard-troops-to-use-heavy-military-equipment [dostęp: 19 VII 2023].

Stepanenko K., *The Kremlin's Pyrrhic Victory in Bakhmut: A Retrospective on the Battle for Bakhmut*, Institute for the Study of War, 24 V 2023 r., https://www.understandingwar.org/backgrounder/kremlin%E2%80%99s-pyrrhic-victory-bakhmut-retrospective-battle-bakhmut [dostęp: 24 V 2023].

Stepanenko K. i in., *Russian offensive campaign assessment, January 16, 2023*, Institute for the Study of War, 16 I 2023 r., https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-january-16-2023 [dostęp: 19 I 2024].

Stognei A., Seddon M., *Yevgeny Prigozhin's 'toxic' media empire left in Kremlin limbo*, Financial Times, 14 VII 2023 r., https://www.ft.com/content/723a967f-213b-45b4-8ca6-792aa8e-10ba0?shareType=nongift [dostęp: 14 VII 2023].

Stronski P., *Implausible Deniability: Russia's Private Military Companies*, Carnegie Endowment for International Peace, 2 VI 2020 r., https://carnegieendowment.org/2020/06/02/implausible-deniability-russia-sprivate- military-companies-pub-81954 [dostęp: 2 VI 2020].

Sukhankin S., *Russia's New PMC Patriot: The Kremlin's Bid for a Greater Role in Africa?*, The Jamestown Foundation, 1 VIII 2018 r., https://jamestown.org/program/russias-new-pmc-patriot-the-kremlins-bid-for-a-greater-role-in-africa/ [dostęp: 12 V 2023].

Troianovski i in., *After Prigozhin's Death, a High-Stakes Scramble for His Empire*, The New York Times, 8 IX 2023 r., https://www.nytimes.com/2023/09/08/world/europe/prigozhin-wagner-russia-africa.html [dostęp: 8 IX 2023].

Wagner Group reportedly hands over military equipment and ammunition to Russia's Defense Ministry, Meduza, 12 VII 2023 r., https://meduza.io/en/news/2023/07/12/wagner-group-reportedly-hands-over-military-equipment-and-ammunition-to-russia-s-defense-ministry [dostęp: 12 VII 2023].

Wagner's second-in-command Troshev sided against Prigozhin during the coup – report, The New Voice Ukraine, 18 VII 2023 r., https://news.yahoo.com/wagner-second-command-troshev-sided-015200321.html [dostęp: 18 VII 2023].

Walker S., Beaumont P., Sabbagh D., *Head of Russia's Wagner group says his troops have taken control of Soledar*, The Guardian, 11 I 2023 r., https://www.theguardian.com/world/2023/jan/10/head-of-wagner-group-says-his-troops-have-taken-control-of-soledar [dostęp: 1 I 2024].

'We don't need heroes who marched on Moscow': Kremlin and FSB decided to bury Yevgeny Prigozhin secretly, without military honors, Meduza, 30 VIII 2023 r., https://meduza.io/en/news/2023/08/30/we-don-t-need-heroes-who-marched-on-moscow-kremlin-and-fsb-decided-to-bury-yevgeny-prigozhin-secretly-without-military-honors [dostęp: 30 VIII 2023].

Weiss M., *Russia's Spies Say Putin Faces More Coups*, The Insider, 20 VII 2023 r., https://theins.ru/en/politics/263596 [dostęp: 20 VII 2023].

Weiss M., Vaux P., *The Company You Keep: Yevgeny Prigozhin's Influence Operations in Africa*, Free Russia Foundation, Washington 2020, https://www.4freerussia.org/wp-content/uploads/sites/3/2020/09/The-Company-You-Keep-Yevgeny-Prigozhins-Influence-Operations-in-Africa.pdf [dostęp: 16 II 2023].

'Welcome to hell' Prigozhin reappears in Belarus, rallying Wagner Group mercenaries for future work in Africa (but not yet in Ukraine), Meduza, 19 VII 2023 r., https://meduza.io/en/feature/2023/07/19/welcome-to-hell [dostęp: 19 VII 2023].

Yevgeny Prigozhin reportedly dissolving Patriot Media Group, home of his 'troll factory', Meduza, 30 VI 2023 r., https://meduza.io/en/news/2023/06/30/prigozhin-reportedly-dissolving-patriot-media-group-home-of-his-troll-factory [dostęp: 30 VI 2023].

Yongo J., *Central African Republic says Wagner troop movement is rotation not departure*, Reuters, 8 VII 2023 r., https://www.reuters.com/world/africa/central-african-republic-says-wagner-troop-movement-is-rotation-not-departure-2023-07-08/ [dostęp: 8 VII 2023].

Żochowski P., *Rosja i Białoruś oskarżają Polskę o plany agresji*, OSW, 24 VII 2023 r., https://www.osw.waw.pl/pl/publikacje/analizy/2023-07-24/rosja-i-bialorus-oskarzaja-polske-o-plany-agresji [dostęp: 24 VII 2023].

Rosyjskie i ukraińskie źródła internetowe

В „Ахмате" рассказали о массовом пополнении из экс-бойцов „Вагнера", Риа Новости, 28 X 2023 r., https://ria.ru/20231028/akhmat-1905834455.html [dostęp: 28 X 2023].

Вагнерівці продовжують прибувати у білорусь, Центр Національного спротиву, 22 VII 2023 r., https://sprotyv.mod.gov.ua/vagnerivtsi-prodovzhuyut-prybuvaty-u-bilorus/ [dostęp: 22 VII 2023].

Вагнерівці, які підписали контракт з білоруською ПВК, відправляють в Африку, Центр Національного спротиву, 12 IX 2023 r., https://sprotyv.mod.gov.ua/vagnerivtsi-yaki-pidpysaly-kontrakt-z-biloruskoyu-pvk-vidpravlyayut-v-afryku/ [dostęp: 12 IX 2023].

В Білорусі лишилось менше 1000 терористів з «пвк «вагнер», Центр Національного спротиву, 18 IX 2023 r., https://sprotyv.mod.gov.ua/v-bilorusi-lyshylos-menshe-1000-terorystiv-z-pvk-vagner/ [dostęp: 18 IX 2023].

В кафе Петербурга на «творческом вечере» «военкора» Владлена Татарского (у него полмиллиона подписчиков в телеграме) произошел взрыв. Блогер погиб, Meduza, 2 IV 2023 r., https://meduza.io/feature/2023/04/02/v-peterburge-v-kafe-evgeniya-prigozhina-proizoshel-vzryv-vo-vremya-tvorcheskogo-vechera-voenkora-vladlena-tatarskogo-po-predvaritelnym-dannym-on-pogib [dostęp: 2 IV 2023].

В Москве усилили меры безопасности, Tacc, 23 VII 2023 r., https://tass.ru/proisshestviya/18103225 [dostęp: 23 VII 2023].

В Ростове-на-Дону рядом со штабом ЮВО выставили посты, Tacc, 23 VII 2023 r., https://tass.ru/bezopasnost/18103205 [dostęp: 23 VII 2023].

Вручение генеральских погон высшему офицерскому составу, Президент Республики Беларусь, 27 VII 2023 r., https://president.gov.by/ru/events/vruchenie-pogon-vysshemu-oficerskomu-sostavu [dostęp: 27 VII 2023].

Встреча с Юнус-Беком Евкуровым и Андреем Трошевым, Kremlin.ru, 29 IX 2023 r., https://kremlin.ru/events/president/news/72391 [dostęp: 29 IX 2023].

Генерал Суровикин возглавил координационный комитет СНГ по вопросам ПВО Подробнее, EurAsia Daily, 10 X 2023 r., https://eadaily.com/ru/news/2023/09/10/general-surovikin-vozglavil-koordinacionnyy-komitet-sng-po-voprosam-pvo [dostęp: 10 X 2023].

Грубо говоря, мы начали войну Как отправка ЧВК Вагнера на фронт помогла Пригожину наладить отношения с Путиным – и что такое «собянинский полк». Расследование «Медузы» о наемниках на войне в Украине, Meduza, 13 VII 2022 r., https://meduza.io/feature/2022/07/13/grubo-govorya-my-nachali-voynu [dostęp: 13 VII 2022].

Дурова Д., *В России уже нашли нового министра обороны для Пригожина: в сети назвали имя*, Oboz.ua, 25 VI 2023 r., https://news.obozrevatel.com/russia/v-rossii-uzhe-nashli-novogo-ministra-oboronyi-dlya-prigozhina-v-seti-nazvali-imya.htm [dostęp: 25 VI 2023].

Евгений Пригожин зарегистрировал компанию в Осиповичском районе, Reformation, 22 VII 2023 r., https://reform-by.cdn.ampproject.org/c/s/reform.by/evgenij-prigozhin-zaregistriroval-kompaniju-v-osipovichskom-rajone/amp [dostęp: 22 VII 2023].

Жаба и Минобороны. Как поссорились Евгений Викторович с Сергеем Кужугетовичем, The Insider, 12 V 2023 r., https://theins.ru/politika/261683 [dostęp: 12 V 2023].

Запомнившиеся события августа, смерть Пригожина, Левада-Центр, 1 IX 2023 r., https://www.levada.ru/2023/09/01/zapomnivshiesya-sobytiya-avgusta-smert-prigozhina/ [dostęp: 1 IX 2023].

Источник: врио главкома ВКС назначили генерала Афзалова, Риа Новости, 23 VIII 2023 r., https://ria.ru/20230823/afzalova-1891645152.html [dostęp: 23 VIII 2023].

Картаполов заявил об окончательном расформировании ЧВК «Вагнер», РБК, 2 XI 2023 r., https://www.rbc.ru/politics/02/11/2023/6543d4389a794741e8fa258e [dostęp: 3 XI 2023].

Кто такой Сергей «Пионер» – глава «Вагнера» в Беларуси? Источник, Reformation, 19 VII 2023 r., https://reform.by/kto-takoj-sergej-pioner-glava-vagnera-belarusi [dostęp: 19 VII 2023].

Наемники ЧВК Вагнера объявили, что закрывают свою главную базу в краснодарском Молькино, Meduza, 17 VII 2023 r., https://meduza.io/news/2023/07/17/naemniki-chvk-vagnera-ob-yavili-chto-zakryvayut-svoyu-glavnuyu-bazu-v-krasnodarskom-molkino [dostęp: 17 VII 2023].

Обращение к гражданам России, Kremlin.ru, 24 VI 2023 r., https://web.archive.org/web/20230628083145/https://kremlin.ru/events/president/news/71496 [dostęp: 24 VI 2023].

Песков опроверг утверждения о причастности Кремля к крушению самолета Пригожина, Интерфакс, 25 VIII 2023 r., https://www.interfax.ru/russia/917796 [dostęp: 25 VIII 2023].

Песков подтвердил встречу Путина с Пригожиным и командирами «Вагнера» 29 июня, Интерфакс, 10 VII 2023 r., https://www.interfax.ru/russia/910904 [dostęp: 10 VII 2023].

Против двоих боевиков ЧВК «Вагнер» в разных регионах России возбудили дела об изнасиловании 13-летних девочек, Важные истории, 30 VIII 2023 r., https://storage.googleapis.com/istories/news/2023/08/30/protiv-dvoikh-boevikov-chvk-vagner-v-raznikh-regionakh-rossii-vozbudili-dela-ob-iznasilovanii-13-letnikh-devochek/index.html [dostęp: 30 VIII 2023].

Прошлое и будущее Пригожина. Как владелец ЧВК «Вагнер» создал свою армию – и что будет делать после мятежа, Досье, 6 VII 2023 r., https://dossier.center/wagner-fall/ [dostęp: 6 VII 2023].

Путин поздравил российских военных с освобождением Артемовска, Тасс, 20 V 2023 r., https://tass.ru/politika/17804025 [dostęp: 19 I 2024].

Солопов М., *Силовые ведомства прорабатывают вопрос о переподчинении полицейского спецназа «Гром» Росгвардии*, Ведомости, 4 VII 2023 r., https://www.vedomosti.ru/politics/articles/2023/07/04/983567-vedomstva-prorabativayut-vopros-o-perepodchinenii-politseiskogo-spetsnaza-rosgvardii [dostęp: 4 VII 2023].

Степура А., *Колишні бійці «Вагнера» справді перебувають на Бахмутському напрямку, це психологічна операція*, Суспільне Новини, 27 IX 2023 r., https://suspilne.media/581703-kolisni-bijci-vagnera-spravdi-perebuvaut-na-bahmutskomu-napramku-ce-psihologicna-operacia-evlas/ [dostęp: 27 IX 2023].

ЧВК «Вагнер» предложила бойцам найти другую работу из-за конкуренции с Минобороны и Росгвардией в Африке и на Ближнем Востоке, Важные истории, 30 VIII 2023 r., https://storage.googleapis.com/istories/news/2023/08/30/chvk-vagner-predlozhila-boitsam-naiti-druguyu-rabotu-iz-za-konkurentsii-s-minoboroni-i-rosgvardiei-v-afrike-i-na-blizhnem-vostoke/index.html [dostęp: 30 VIII 2023].

Akty prawne

Konwencje o ochronie ofiar wojny, podpisane w Genewie dnia 12 sierpnia 1949 roku (DzU z 1956 r. nr 38 poz. 171).

Protokoły dodatkowe do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół I) oraz dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych (Protokół II), sporządzone w Genewie dnia 8 czerwca 1977 r. (DzU z 1992 r. nr 41 poz. 175).

Dr Filip Bryjka

Politolog i doktor nauk społecznych w dyscyplinie nauki o bezpieczeństwie. Adiunkt w Instytucie Studiów Politycznych PAN i analityk w Polskim Instytucie Spraw Międzynarodowych w Warszawie. Specjalizuje się w problematyce zagrożeń hybrydowych, zwłaszcza rosyjskiej dezinformacji i grupach paramilitarnych. Absolwent nauk politycznych na Uniwersytecie Wrocławskim i bezpieczeństwa narodowego w Akademii Sztuki Wojennej. Uczestnik międzynarodowych projektów badawczych poświęconych przeciwdziałaniu dezinformacji sfinansowanych z grantów Kwatery Głównej NATO i Unii Europejskiej.

Kontakt: bryjka@pism.pl

Przestępstwo szpiegostwa po nowemu, czyli w świetle nowelizacji Kodeksu karnego z 17 sierpnia 2023 roku

The crime of espionage in new terms, i.e. in light of amendment to the Criminal Code of 17 August 2023

PIOTR BURCZANIUK

Instytut Nauk Prawnych,
Uniwersytet Kardynała Stefana Wyszyńskiego
https://orcid.org/0000-0002-6685-8769

Przegląd Bezpieczeństwa Wewnętrznego, 2024, nr 30: 49–78

https://doi.org/10.4467/20801335PBW.24.002.19604

ARTYKUŁ

Abstrakt

W opracowaniu dokonano analizy zakresu zmian w penalizacji przestępstwa szpiegostwa w Polsce, jakie nastąpiły wraz z nowelizacją Kodeksu karnego z 17 sierpnia 2023 r., a także zmian systemowych w ośmiu innych ustawach, w tym w ustawach kompetencyjnych wszystkich polskich służb specjalnych. Zmiany zostały wprowadzone w celu zwiększenia uprawnień służących zwalczaniu tego rodzaju przestępstw. Głównym celem analizy była próba odpowiedzi na pytanie, czy zakres tych zmian odpowiada postulatom zgłaszanym przez doktrynę prawniczą i praktyków zajmujących się zwalczaniem szpiegostwa w Polsce i dostosowuje stan prawny do aktualnej sytuacji geopolitycznej, związanej głównie z agresywnymi działaniami niemilitarnymi opisywanymi w doktrynach wojennych. Analizę wprowadzonych zmian ukazano na tle procesu legislacyjnego omawianej ustawy, a zwłaszcza towarzyszącej mu dyskusji, bez której właściwe zrozumienie tych zmian nie byłoby możliwe.

Słowa kluczowe

szpiegostwo, działalność wywiadowcza, służby specjalne

Abstract

The study analysed the scope of changes in the criminalisation of the crime of espionage in Poland that took place with the amendment to the Criminal Code of 17 August 2023, as well as the systemic changes introduced by it in eight other laws, including the competency laws of all Polish special services. The amendments were introduced to increase the powers to combat this type of crime. The primary objective of the analysis was an attempt to answer the question of whether the scope of the changes introduced corresponds to the demands made by legal doctrine as well as practitioners involved in combating espionage in Poland, consequently adjusting the legal state to the current geopolitical situation, mainly related to aggressive non-military actions described in the doctrines of war. The analysis of the introduced changes was shown against the background of the legislative process of the indicated law, and especially the discussion that took place within its framework, without which a proper understanding of the changes would not be possible.

Keywords

espionage, intelligence activities, secret services

Dnia 17 sierpnia 2023 r. Sejm Rzeczypospolitej Polskiej uchwalił ustawę o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (dalej: ustawa), która fundamentalnie zmieniła sposób penalizacji przestępstwa szpiegostwa w Polsce. Jak wskazano w uzasadnieniu do ustawy:

> (…) głównym celem proponowanego projektu jest potrzeba dostosowania przepisów Kodeksu karnego dotyczących przestępstwa szpiegostwa do stale zmieniającej się sytuacji geopolitycznej, postępu technologicznego, jak i ciągłych modyfikacji sposobu działania potencjalnych sprawców czynów zabronionych opisanych obecnie w art. 130 k.k. Nie bez znaczenia jest również aktualne wysokie zagrożenie nowymi otwartymi konfliktami zbrojnymi oraz agresywnymi działaniami niemilitarnymi, co nasila podejmowanie przez obcy wywiad i nie tylko, działań o charakterze szpiegowskim[1].

[1] Uzasadnienie do *Poselskiego projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw*, druk nr 3232 z 17 IV 2023 r., https://orka.sejm.gov.pl/Druki9ka.nsf/0/F53D07E65F8EC17AC12589B1003F2A96/%24File/3232.pdf, s. 13 [dostęp: 28 VIII 2023].

Poza nowelizacją przepisów karnych za pomocą tej ustawy dokonano systemowych zmian w ośmiu innych ustawach, w tym w ustawach kompetencyjnych wszystkich polskich służb specjalnych. Potrzeba zmian w zakresie penalizacji przestępstwa szpiegostwa oraz kompetencji i uprawnień służb specjalnych w tym zakresie, nakierowanych na skuteczną neutralizację tego rodzaju przestępstw, była od ponad dziesięciu lat postulowana zarówno przez doktrynę prawniczą (w tym autora niniejszego opracowania), jak i przez praktyków zajmujących się zwalczaniem tego czynu zabronionego.

Celem niniejszego opracowania jest analiza zakresu wprowadzonych zmian i próba odpowiedzi na pytanie, czy jest on adekwatny do zgłaszanych postulatów i wychodzi naprzeciw praktycznym problemom, z którymi zetknęły się polskie organy ścigania, rozpoznając przestępstwo szpiegostwa. Ważne miejsce w tych rozważaniach zajmuje analiza przebiegu procesu legislacyjnego. Dyskusja, która mu towarzyszyła, jest bowiem istotna dla właściwego rozumienia – jako swoista wykładnia autentyczna – nowej regulacji.

Uzasadnienie wprowadzonych zmian

W formułowanych postulatach dotyczących zmian regulacyjnych przestępstwa szpiegostwa wskazywano, że sposób określenia znamion czynu zabronionego, zawarty w dotychczasowym brzmieniu art. 130 *Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny* (dalej: k.k.), w wielu wymiarach jest niezbyt trafny, często niewystarczający, a przede wszystkim niejasny i mało precyzyjny. Sprzyjało to odmiennym interpretacjom znamion tego przestępstwa przez doktrynę i często prowadziło do różnej kwalifikacji przez prokuraturę dokonywanych czynów. Zmienione właśnie uregulowanie przestępstwa szpiegostwa korespondowało wprost z zagrożeniami bezpieczeństwa zewnętrznego Polski identyfikowanymi w latach 90. XX w. Bazowały one na wypracowanej jeszcze w okresie zimnej wojny koncepcji dwubiegunowości systemu międzynarodowego, opartego na dwóch przeciwstawnych sobie blokach państw prowadzących rywalizację z wykorzystaniem środków militarnych. Z tej perspektywy zakres znamion czynu zabronionego ujętego w tym przepisie nie odpowiadał wyzwaniom związanym z współczesnymi zagrożeniami bezpieczeństwa zewnętrznego państwa, w tym zjawiskom określanym zbiorczo mianem zagrożeń asymetrycznych.

Podczas debaty sejmowej nad projektem ustawy poseł Jarosław Krajewski słusznie zauważył, że (…) *przestępstwo szpiegostwa, jest jednym z najcięższych przestępstw przeciwko Rzeczypospolitej Polskiej, a jeżeli popełnione jest przez obywatela polskiego jest de facto zdradą naszego kraju.* (…) *Jest to szczególnie istotne*

z perspektywy obecnej sytuacji geopolitycznej, która również zmienia modus operandi obcych służb wywiadowczych, które działają przeciwko naszemu państwu[2]. Do tej sytuacji geopolitycznej odwołują się także polskie dokumenty strategiczne, w tym *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*. Wskazano w niej m.in., że:

> (…) najpoważniejsze zagrożenie stanowi neoimperialna polityka władz Federacji Rosyjskiej, realizowana również przy użyciu siły militarnej. (…) Federacja Rosyjska prowadzi również działania poniżej progu wojny (o charakterze hybrydowym), niosące ryzyko wybuchu konfliktu (w tym niezamierzonego, wynikającego z gwałtownej eskalacji w rezultacie incydentu, szczególnie militarnego), a także podejmuje wszechstronne i kompleksowe działania za pomocą środków pozamilitarnych (w tym: cyberataki, dezinformacja) celem destabilizacji struktur państw i społeczeństw zachodnich oraz wywoływania podziałów wśród państw sojuszniczych. Należy przyjąć, że Federacja Rosyjska będzie kontynuowała politykę podważania obecnego ładu międzynarodowego, opartego na prawie międzynarodowym, w celu odbudowy pozycji mocarstwowej i stref wpływów[3].

Wskazane są w tej strategii działania poniżej progu wojny, nazywane też wojną czwartej generacji, wojną hybrydową, wojną nieliniową, wojną specjalną, konfliktem asymetrycznym jak również doktryną Gierasimowa[4]. Zakłada ona, że:

> (…) same „zasady wojny" uległy znacznej zmianie. Wzrosła rola metod pozamilitarnych w osiąganiu celów politycznych i strategicznych, które w niektórych przypadkach znacznie przewyższyły skuteczność broni. Metody konfrontacji przesuwają się w kierunku szerokiego stosowania środków politycznych, ekonomicznych, informacyjnych, humanitarnych i innych środków niemilitarnych, wdrażanych z wykorzystaniem potencjału protestacyjnego ludności. Wszystko to jest uzupełniane niejawnymi środkami wojskowymi, w tym wdrażaniem informacyjnych środków zaradczych i działaniami sił

[2] Wystąpienie Jarosława Krajewskiego 13 VI 2023 r. podczas pierwszego czytania poselskiego projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (druki nr 3232 i 3232-A), iTV Sejm – transmisje archiwalne, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?page=9#1C429C6BE7B92E29C12588FB0033AB2F [dostęp: 28 VIII 2023].

[3] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, s. 6 [dostęp: 28 VIII 2023].

[4] Nazwa wywodzi się od nazwiska szefa Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej gen. Walerija Gierasimowa, który w artykule *Ценность науки в предвидении* opublikowanym 27 II 2013 r. w gazecie „Военно-промышленный курьер" zreferował koncepcję wojny nowej generacji. Tłumaczenia w artykule pochodzą od autora (dop. red.).

operacji specjalnych. Jawne użycie siły jest często stosowane pod przykrywką utrzymania pokoju i zarządzania kryzysowego tylko na pewnym etapie, głównie w celu osiągnięcia ostatecznego sukcesu w konflikcie[5].

W tej koncepcji środki niemilitarne mają nie tylko tworzyć i zapewniać warunki do skutecznego użycia siły militarnej, lecz często nawet je zastępować. Oś przedstawionej koncepcji stanowi więc skoordynowane użycie – w celu pokonania przeciwnika lub uzyskania nad nim przewagi – pełnego spektrum środków niemilitarnych, w tym dyplomatycznych, politycznych, ekonomicznych, technologicznych, humanitarnych i informacyjnych, przy jednoczesnym wykorzystaniu szerokiej sfery psychologicznego oraz socjologicznego oddziaływania na ludność atakowanego państwa. Jest to (…) *wizja wojny partyzanckiej prowadzonej na wszystkich frontach za pomocą najróżniejszych narzędzi i osób: hakerów, mediów, biznesmenów, przecieków informacji, a także – oczywiście – fałszywych newsów i tradycyjnych, konwencjonalnych i asymetrycznych środków militarnych*[6]. Środki asymetryczne, o charakterze pozawojskowym, nie służą zatem wyłącznie wspieraniu działań militarnych, lecz stanowią filar prezentowanej koncepcji wojny nowej generacji. Są one traktowane jako element działań wojennych, który ma wywołać chaos przez podtrzymywanie u przeciwnika stanu permanentnego niepokoju i napięć społecznych, i stanowią zakładany cel strategiczny nakierowany na odniesienie zwycięstwa w wojnie. Jednocześnie zmieniają się zasady użycia siły militarnej. Przyjęto założenie, że (…) *frontalne starcia dużych zgrupowań wojsk (sił) na poziomie strategicznym i operacyjnym stopniowo odchodzą do przeszłości* (…) *wypierane są one przez bezkontaktowe, precyzyjne uderzenia dalekiego zasięgu, połączone z działaniami sił specjalnych w połączeniu z siłami wewnętrznej opozycji*[7].

W naukach o bezpieczeństwie podkreśla się, że nie istnieje jeden wzorzec wojny hybrydowej, szczególnie w jej praktycznym wydaniu. Można co najwyżej mówić o pewnych ramach, w których są realizowane konkretne przedsięwzięcia dostosowywane do zmieniających się okoliczności oraz sytuacji zewnętrznej i wewnętrznej państwa będącego celem podejmowanych działań. W te działania jest

[5] В. Герасимов, *Ценность науки в предвидении*, „Военно-промышленный курьер", 27 II 2013 r., https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html [dostęp: 28 VIII 2023].

[6] M.K. McKew, *Doktryna Gierasimowa, czyli rosyjski sposób na wojnę: chaos, a nie bomby*, Onet, 6 IX 2017 r., https://wiadomosci.onet.pl/swiat/doktryna-gierasimowa-czyli-rosyjski-sposob-na-wojne--chaos-a-nie-bomby/svh4p0h [dostęp: 28 VIII 2023].

[7] П. Фельгенгауэр, *Добиться превосходства над остальным человечеством. Начальник российского Генштаба формулирует программу подготовки к масштабной войне*, Новая газета, 9 III 2019 r., https://novayagazeta.ru/articles/2019/03/09/79808-dobitsya-prevoshodstva-nad--ostalnym-chelovechestvom [dostęp: 28 VIII 2023].

zaangażowanych – w różnym stopniu – wiele instytucji i organów danego państwa lub podmiotów od niego zależnych, z oczywistą, wiodącą rolą służb specjalnych. Co ważne, rola tych służb nie sprowadza się wyłącznie do zbierania informacji, lecz obejmuje również aktywne działania wywiadowcze określane mianem operacji wpływu. Zbieranie informacji, w tym przypadku, jest połączone z dezinformacją i propagandą oraz niekiedy z działaniami noszącymi znamiona dywersji i sabotażu, w postaci ataków cybernetycznych, potajemnych akcji o charakterze prowokacji, służących destabilizacji sytuacji społeczno-politycznej czy wprowadzaniu chaosu. Dynamiczny postęp technologiczny, zwłaszcza w obszarze komunikacji, środków masowego przekazu i mediów społecznościowych, bez wątpienia ułatwia prowadzenie takich działań[8]. *Dzięki internetowi i mediom społecznościowym możliwe są dziś działania, o których dawni radzieccy specjaliści od wojny psychologicznej mogli tylko marzyć: zmiana polityki wewnętrznej innych państw za pomocą samej tylko informacji*[9].

W kontekście opisanej zmiany sposobu funkcjonowania obcych służb specjalnych pojawił się istotny problem ich kwalifikowania w ramach obowiązującego w Polsce opisu znamion przestępstwa szpiegostwa. Uchylona regulacja art. 130 k.k. obejmowała bowiem wyłącznie cztery typy tego przestępstwa:

- typ podstawowy, kryminalizujący branie udziału w działalności obcego wywiadu (art. 130 § 1),
- typ kwalifikowany, w którym okolicznością kwalifikującą było udzielanie, podczas brania udziału w obcym wywiadzie lub działaniu na jego rzecz, obcemu wywiadowi wiadomości, których przekazanie mogło wyrządzić szkodę RP (art. 130 § 2),
- typ kwalifikowany, w którym surowsza odpowiedzialność jest związana z faktem organizowania działalności obcego wywiadu lub kierowania nią (art. 130 § 4),
- typ uprzywilejowany, polegający na gromadzeniu, przechowywaniu lub wchodzeniu do systemu informatycznego, aby uzyskać informacje w celu udzielenia ich obcemu wywiadowi, lub zgłaszaniu gotowości działania na rzecz obcego wywiadu przeciwko RP (art. 130 § 3).

[8] Zob. szerzej: M. Wojnowski, *Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, wydanie specjalne: *Wojna hybrydowa*, s. 25; Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, wydanie specjalne: *Wojna hybrydowa*, s. 46–47.

[9] M.K. McKew, *Doktryna Gierasimowa*…

Doktryna prawnicza i orzecznictwo wypracowały dość jednoznaczne rozumienie najważniejszych pojęć – „brania udziału w działalności obcego wywiadu" oraz „działania na rzecz obcego wywiadu". Jak wskazuje Piotr Kardas:

> (…) przez branie udziału rozumieć należy wszelkie postaci aktywnej współpracy z obcym wywiadem, polegającej na przynależności do struktur organizacyjnych wywiadu (…) „udziałem" w działalności wywiadu jest zarówno wykonywanie funkcji agenta lub rezydenta obcego wywiadu, jak i wykonywanie każdej innej funkcji w jego strukturach organizacyjnych, np. funkcji osoby werbującej współpracowników, prowadzącej szkolenie agentów, dostarczającej lub przygotowującej środki techniczne wykorzystywane w działalności wywiadu, zbierającej i opracowującej informacje, obsługującej tzw. punkty kontaktowe lub punkty przerzutowe, zaopatrującej siatkę szpiegowską w materiały i środki wykorzystywane do działalności wywiadowczej itd.[10]

Z kolei (…) *działanie na rzecz obcego wywiadu oznacza wszelkie formy aktywnej współpracy z obcym wywiadem, która nie przybiera jeszcze postaci funkcjonowania w jego strukturach organizacyjnych, dającej się określić jako branie w nim udziału. Działanie na rzecz obcego wywiadu nie wymaga istnienia więzi organizacyjnej łączącej sprawcę z obcym wywiadem*[11]. Istotne jest, że z punktu widzenia znamion przestępstwa przewidzianego wcześniej w art. 130 § 2 k.k. było penalizowane tylko takie działanie na rzecz obcego wywiadu, które przyjmowało postać udzielania mu wiadomości określonych w tym przepisie. Z uwagi na zakres regulacyjny tak zredagowanego art. 130 k.k. pojawił się ważki praktyczny problem dotyczący kwalifikowania zachowań sprawczych, które nie wypełniały przytoczonej definicji „brania udziału w działalności obcego wywiadu". Nie zawierały bowiem elementów aktywnej współpracy z obcym wywiadem połączonej z przynależnością do struktur organizacyjnych tego wywiadu (lub takich, w których tej przynależności nie udało się uprawdopodobnić materiałem dowodowym, co w przypadku działalności szpiegowskiej – z założenia prowadzonej niejawnie – jest zadaniem praktycznie niewykonalnym), a które to działania faktycznie przyjmowały postać „działania na rzecz obcego wywiadu", przy czym nie były połączone z przekazywaniem w ramach tej współpracy wiadomości obcemu wywiadowi (co było penalizowane przez Kodeks karny), lecz obejmowały podejmowanie różnego rodzaju innych działań, w tym nazywanych operacjami wpływu, zgodnych z opisaną powyżej doktryną

[10] P. Kardas, w: *Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-211a* (cz. 1), W. Wróbel, A. Zoll (red.), Warszawa 2017, art. 130.

[11] Tamże.

Gierasimowa. Podczas debaty w Senacie nad ustawą senator Magdalena Kochan wskazała, że:

> (…) nikt z nas na tej sali nie może sobie pozwolić na lekceważenie służb specjalnych Rosji. Nikt z nas kto wie, przeczytał (…) zapoznał się z doktryną Gierasimowa, nie może lekceważyć tej doktryny i dezinformacji, która leży u podstaw tej doktryny. Wszyscy zdajemy sobie sprawę z jej roli w trakcie wyborów w Stanach Zjednoczonych, wiemy, jaką rolę odegrała ta dezinformacja w czasie brexitu, wiemy, jaką ogromną uwagą cieszy się zapewne Polska, bo z wielkomocarstwowych zapędów Rosji upadek ZSRR nie wyleczył. W związku z czym i w związku z toczącą się przy naszej granicy, tuż obok, wojną, żadnych zagrożeń związanych ze szpiegostwem w naszym kraju lekceważyć nie wolno[12].

Prace legislacyjne – rys historyczny

Dyskusję nad potrzebą zmian regulacyjnych przestępstwa szpiegostwa zapoczątkował już w grudniu 2016 r. Piotr Pogonowski, ówczesny szef Agencji Bezpieczeństwa Wewnętrznego. Przedstawione przez niego założenia stały się podstawą do wypracowania w pierwszej połowie 2017 r., we współpracy z ministrem sprawiedliwości, projektu zmian. Po pierwsze, zakładał on uzupełnienie określonego w art. 130 § 1 k.k. znamienia czynu zabronionego w postaci „brania udziału w działalności obcego wywiadu" o znamię „prowadzenia działalności wywiadowczej", definiowanego jako czynność lub zespół czynności podejmowanych, choćby pośrednio, w interesie obcego państwa lub zagranicznej organizacji. Działalność ta polega na pozyskiwaniu lub przekazywaniu informacji, których ujawnienie lub wykorzystanie może naruszyć interesy państwa w zakresie obejmującym w szczególności ochronę niepodległości, integralności terytorialnej, bezpieczeństwa zewnętrznego i wewnętrznego, obronności, polityki zagranicznej, środowiska naturalnego lub dziedzictwa kulturowego oraz potencjału naukowego lub gospodarczego państwa, lub prowadzenie działań przeciwko temu interesowi. Po drugie, zakładał on wprowadzenie do Kodeksu karnego problematyki tzw. zagrożeń hybrydowych przez dodanie definicji przestępstwa sabotażu państwowego oraz aktu agresji. Ponadto projekt przewidywał objęcie karalnością działalności szpiegowskiej prowadzonej na terytorium RP i niewymierzonej przeciwko niej. Zakładał również dodanie do k.k. art. 113a, który regulowałby

[12] Wystąpienie Magdaleny Kochan 26 VII 2023 r. podczas debaty na 65. posiedzeniu Senatu RP X kadencji, https://av8.senat.pl/10Sen651 [dostęp: 28 VIII 2023].

kwestię stosowalności Kodeksu w odniesieniu do przestępstw popełnianych przy użyciu systemu teleinformatycznego, bez względu na geograficzną lokalizację sprawcy bądź wykorzystywany przez niego system teleinformatyczny. W odniesieniu do przestępstwa szpiegostwa w projekcie wprowadzono rozwiązanie sugerowane przez autora niniejszego artykułu[13], polegające na oddzieleniu pojęcia rzeczywistego prowadzenia działalności wywiadowczej, czyli wykonywania określonych działań (element przedmiotowy), od pojęcia brania udziału w działalności obcego wywiadu, rozumianego jako formalna przynależność do struktur tego wywiadu (element podmiotowy). Projektodawca objął więc założeniem karalności zarówno zachowanie sprowadzające się do wykonywania określonych czynności w interesie obcego państwa lub zagranicznej organizacji, bez potrzeby wiązania ich bezpośrednio z wyodrębnionym strukturalnie podmiotem – służbą wywiadowczą, jak i samą przynależność do takich struktur. Zaprezentowana definicja „działalności wywiadowczej" korespondowała z tzw. modelem francuskim penalizacji szpiegostwa, ukształtowanym brzmieniem art. 411-4 i 411-5 Kodeksu karnego Republiki Francuskiej. Negatywne stanowisko wobec tego projektu przedstawiła jednak Prokuratura Krajowa[14], co mogło mieć wpływ na brak kontynuacji związanych z nim prac legislacyjnych. Powrócono do nich z inicjatywy sejmowej Komisji do Spraw Służb Specjalnych. Wspomniał o tym podczas debaty w Sejmie poseł Marek Biernacki, który przypomniał, że:

> (…) aktualna definicja szpiegostwa nie spełnia swoich wymogów, nie służy skutecznie dla działania – ochrony polskich interesów, nie służy państwu polskiemu, to już wiadomo od dawna. Wiemy też, że u innych naszych sąsiadów, naszych partnerów (Francuzi, inne państwa), pracują nad zmianą tych zapisów i myśmy też zaczęli pracować od 2018 r. w Komisji do Spraw Służb Specjalnych – przypominam, bo to jest ważne. Pracowaliśmy z ówczesnymi szefami ABW panem prof. Pogonowskim i panem płk. Lobą. Uczestniczyła w tym też prokuratura i sędziowie. Wszyscy wykazywali, że projekt ustawy jest potrzebny, że ustawa musi być zmieniona. Nagle z winy prokuratury prokurator krajowy wycofał ten projekt, wycofał prace[15].

---

[13] P. Burczaniuk, *Przestępstwo szpiegostwa – rys historyczny, aktualne regulacje na tle doświadczeń praktycznych i analizy prawno-porównawczej wybranych państw*, w: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, P. Burczaniuk (red.), Warszawa 2017, s. 106–107.

[14] Pismo z 21 VI 2017 r. nr PK I BP 0280.122.2017.

[15] Wystąpienie Marka Biernackiego w imieniu klubu 6 VII 2023 r. podczas rozpatrywania sprawozdania Komisji o poselskim projekcie ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (druki nr 3232, 3232-A i 3358), iTV Sejm – transmisje archiwalne, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?page=2#0CD6003114C05652C12588FB0033AD73 [dostęp: 28 VIII 2023].

Prace nad zmianami regulacyjnymi dotyczącymi przestępstwa szpiegostwa podjął ponownie pod koniec lutego 2022 r. minister sprawiedliwości, z uwagi na sytuację geopolityczną wywołaną zbrojną agresją Federacji Rosyjskiej przeciwko Ukrainie i związanym z tym zagrożeniem bezpieczeństwa Polski. Opracowany wówczas, we współpracy z Ministerstwem Spraw Wewnętrznych i Administracji, Prokuraturą Krajową oraz szefami służb specjalnych, projekt skoncentrował się na zaostrzeniu karalności przestępstwa szpiegostwa, dodaniu formy stadialnej przygotowania oraz wprowadzeniu jego formy nieumyślnej. Zaproponowane brzmienie przepisu art. 130 k.k. miało obejmować zakresem czynności sprawcze podmiotów biorących udział w działalności obcego wywiadu lub innej działalności wywiadowczej przeciwko RP. Jednocześnie projekt zakładał wprowadzenie definicji działalności wywiadowczej, rozumianej jako czynność lub zespół czynności podejmowanych w interesie lub na rzecz obcego państwa lub zagranicznego podmiotu przez osobę niebiorącą udziału w obcym wywiadzie. Czynności te miałyby polegać na: 1) pozyskiwaniu lub przekazywaniu wiadomości, których ujawnienie lub wykorzystanie narusza lub może naruszyć interes państwa w zakresie ochrony niepodległości, integralności terytorialnej, bezpieczeństwa zewnętrznego i wewnętrznego, obronności, polityki zagranicznej, pozycji międzynarodowej, potencjału naukowego lub gospodarczego, lub 2) prowadzeniu naruszających interes państwa w zakresie określonym w pkt 1 działań dezinformacyjnych lub propagandowych, nakierowanych na destabilizację ustroju lub gospodarki lub wywarcie nacisku na organy władzy publicznej w celu podjęcia lub zaniechania przez nie określonych działań. Co ważne, jak wskazywał minister sprawiedliwości, pojęcie działalności wywiadowczej odniesiono nie tylko do podmiotów stanowiących emanację obcego państwa, lecz także do innych form ją maskujących[16], jak spółki, fundacje i inne organizacje, formalnie niezwiązane ze strukturami państwowymi. Ponadto założono, że zagrożenie karą za szpiegostwo będzie mieć charakter prewencyjny, co miało uzasadniać doprecyzowanie oraz określenie wysokości sankcji na bardzo wysokim pułapie, obejmującym dożywotnie pozbawienie wolności w typie kwalifikowanym. Projekt zawierał również zmiany m.in. w *Ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (dalej: ustawa o ABW oraz AW) oraz w *Ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (dalej: ustawa AT), w których kompetencje ABW dotyczące zapobiegania i zwalczania przestępczości terrorystycznej miały zostać rozszerzone na przestępstwa o charakterze szpiegowskim. Zgodnie z założeniem Ministerstwa Sprawiedliwości projekt

[16] *Zmiany w Kodeksie karnym związane z zagrożeniem bezpieczeństwa państwa*, Ministerstwo Sprawiedliwości, 29 III 2022 r., https://www.gov.pl/web/sprawiedliwosc/zmiany-w-kodeksie-karnym-zwiazane-z-zagrozeniem-bezpieczenstwa-panstwa [dostęp: 28 VIII 2023].

miał być zgłoszony jako autopoprawka do rządowego projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (druk nr 2023), co jednak nie nastąpiło. Do tych prac wrócił w październiku 2022 r. wiceminister sprawiedliwości Marcin Warchoł, który wskazał: (…) *jesteśmy po uzgodnieniach między Ministerstwem Sprawiedliwości i MSWiA. Mamy wypracowany kształt rozwiązań gotowych do prac parlamentarnych. Mam nadzieję, że Sejm zajmie się nimi niezwłocznie. Decyzja w tej sprawie należy do marszałka Sejmu*[17]. Zgodnie z zapowiedzią propozycja miała mieć formę projektu poselskiego.

Materializacja tej zapowiedzi nastąpiła 17 kwietnia 2023 r., kiedy do Marszałka Sejmu wpłynął poselski projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (druk nr 3232), zgłoszony przez grupę posłów klubu Prawa i Sprawiedliwości (PiS), reprezentowanych przez posła Jarosława Krajewskiego. Analiza tego projektu prowadzi do wniosku, że kierunkowo był on zbieżny z procedowanymi wcześniej projektami, przy czym zawierał dwie istotne zmiany. Po pierwsze, rezygnował ze znamienia prowadzenia działalności wywiadowczej (i jej definiowania) jako elementu czynu zabronionego przestępstwa szpiegostwa. Po drugie, wprowadzał penalizację szczególnego rodzaju działalności wywiadowczej polegającej na dezinformacji, sabotażu, dywersji oraz działaniach o charakterze terrorystycznym. Projekt uzupełniono o zmiany do *Ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny* (dalej: ustawa o obronie Ojczyzny), zakładające zakaz fotografowania, filmowania oraz utrwalania wizerunku obiektów szczególnie istotnych dla bezpieczeństwa i obronności państwa, a także osób i ruchomości znajdujących się w tych obiektach.

Swoje stanowisko wobec projektu, w piśmie z 16 maja 2023 r., przedłożyła Fundacja Panoptykon oraz Helsińska Fundacja Praw Człowieka. Skrytykowano w nim przede wszystkim wprowadzenie do projektu odpowiedzialności karnej za nieumyślne szpiegostwo oraz karalność przygotowania do tego przestępstwa. Zgłoszone w tym zakresie wątpliwości prawdopodobnie zaważyły na wprowadzeniu w ramach pierwszego czytania projektu (13 czerwca 2023 r., 77. posiedzenie Sejmu) poprawek usuwających karalność szpiegostwa nieumyślnego oraz zawężenie przygotowania wyłącznie do czynu w zakresie sabotażu, dywersji lub określonego w art. 115 § 20 k.k. Swoje uwagi do projektu przedstawiły również Krajowa Rada

[17] M. Mikowski, *Wiceszef MS: zmiany ws. surowszych kar za szpiegostwo są już gotowe*, PAP, 23 X 2022 r., https://www.pap.pl/aktualnosci/news%2C1460354%2Cwiceszef-ms-zmiany-ws-surowszych-kar-za-szpiegostwo-sa-juz-gotowe.html [dostęp: 28 VIII 2023].

Sądownictwa[18] i Sąd Najwyższy[19], a ocenę skutków regulacji przekazało Biuro Analiz Sejmowych[20].

Dalsze sejmowe prace legislacyjne przebiegły bardzo sprawnie, gdyż już na 78. posiedzeniu Sejmu, 6 lipca 2023 r., rozpatrzono projekt w ramach drugiego czytania (przyjmując większość poprawek o charakterze legislacyjnym zgłoszonych przez klub PiS), a 7 lipca 2023 r. zdecydowaną większością głosów uchwalono ustawę[21]. W dniu 28 lipca 2023 r. ustawę rozpatrzył Senat RP[22] poprzez zgłoszenie pięciu poprawek, z których tylko jedną przyjęto podczas ponownego rozpatrzenia ustawy przez Sejm RP 17 sierpnia 2023 r. Przyjęcie tej poprawki poskutkowało formalnie ponownym uchwaleniem ustawy i zmianą jej daty na 17 sierpnia 2023 r. Ustawa została podpisana przez Prezydenta RP Andrzeja Dudę 28 sierpnia 2023 r. i weszła w życie 23 września 2023 r., z wyjątkiem wybranych przepisów, które weszły w życie 1 października 2023 r.

Zakres zmian w Kodeksie karnym

Nie budzi wątpliwości, że najistotniejszym merytorycznie elementem zmian objętych uchwaloną ustawą jest przedefiniowanie przestępstwa szpiegostwa przez nadanie nowego brzmienia całemu art. 130 k.k. Wszystkie pozostałe zmiany objęte przyjętą nowelizacją pozostają w związku systemowym z tą właśnie zmianą. Z tego powodu przyjęta ustawa podczas prac legislacyjnych często była nazywana ustawą antyszpiegowską.

Dla prawidłowej wykładni wskazanych zmian niezmiernie istotny jest wniosek, że wszystkie opisane powyżej projekty, przedkładane w latach 2016–2022, zakładały konieczność wprowadzenia do Kodeksu karnego jako elementu znamion przestępstwa szpiegostwa zachowania polegającego na prowadzeniu działalności wywiadowczej, przy jednoczesnym zdefiniowaniu tego pojęcia przez odwołanie się

[18] Opinia z 16 VI 2023 r.

[19] Uwagi Biura Studiów i Analiz Sądu Najwyższego z 12 VI 2023 r. nr BSA.II.021.29.2023.

[20] Ocena skutków regulacji z 22 V 2023 r. do druku nr 3232.

[21] Zgodnie z wynikami głosowania nr 46 na 78. posiedzeniu Sejmu za przyjęciem ustawy opowiedziało się 271 posłów (całość klubu PiS, większość z klubu Koalicji Polskiej oraz klubu Konfederacji), 1 był przeciw, a 179 wstrzymało się (klub Lewicy oraz większość klubu Koalicji Obywatelskiej), https://www.sejm.gov.pl/sejm9.nsf/agent.xsp?symbol=glosowania&NrKadencji=9&NrPosiedzenia=78&NrGlosowania=46 [dostęp: 28 VIII 2023].

[22] Podczas prac legislacyjnych swoje krytyczne stanowisko wobec ustawy zgłosił rzecznik praw obywatelskich (pismo z 19 VII 2023 r. nr II.510.565.2023.PZ), a uwagi przedstawił prezes Urzędu Ochrony Danych Osobowych (pismo z 21 VII 2023 r. nr DOL.401.362.2023.WL.RB).

do tzw. modelu francuskiego. Ten zabieg legislacyjny miał być remedium penalizacji czynności sprawczych związanych z aktywnością obcych służb specjalnych będącą elementem działań o charakterze hybrydowym. Uchwalona ustawa była pierwszym projektem, który tego rozwiązania nie zakładał. Zgodnie z ostatecznie przyjętym brzmieniem przepisu art. 130 § 1 k.k. przestępstwo szpiegostwa w typie podstawowym może przybrać postać: brania udziału w działalności obcego wywiadu albo działania na jego rzecz, przy czym w obu sytuacjach musi to być czynność sprawcza skierowana przeciwko RP. W związku z powyższym od 1 października 2023 r. typ podstawowy przestępstwa szpiegostwa wypełnia zachowanie przybierające postać aktywnej współpracy z obcym wywiadem, polegające na przynależności do jego struktur organizacyjnych (branie udziału), albo wszelką aktywną współpracę z obcym wywiadem, która nie przybiera jeszcze postaci funkcjonowania w jego strukturach organizacyjnych (działania na jego rzecz), o ile te aktywności są skierowane przeciwko RP, a więc zagrażają lub naruszają zewnętrzne lub wewnętrzne interesy państwa polskiego. Oczywiście chodzi o potencjalną – chociaż wykazaną w konkretnym stanie faktycznym – możliwość wyrządzenia szkody państwu polskiemu (na gruncie uchylonego brzmienia przyjmowano już brak konieczności wykazywania szkody rzeczywistej).

Przyjęte rozwiązanie należy ocenić jako krok w dobrym kierunku i wyjście naprzeciw zgłaszanym problemom praktycznym. Trudność stanowi jednak otwartość interpretacyjna przyjętego przepisu, który głównie z uwagi na domniemanie *in dubio pro reo* oraz towarzyszący mu zakaz stosowania w prawie karnym wykładni rozszerzającej może w toku rozpatrywania przez sądy indywidualnych spraw spotkać się z zawężającym rozumieniem użytych pojęć (głównie pojęcia współpracy z obcym wywiadem). Konsekwencją tego będzie brak możliwości penalizacji określonego spektrum zachowań rozpoznawanych przez służby jako zagrożenia hybrydowe prowadzone przez obce służby specjalne. Wydaje się, że definicja działalności wywiadowczej formułowana we wcześniejszych projektach była mniej podatna na takie ryzyko, ze względu na wyższy poziom określoności.

Drugą zasadniczą zmianą objętą ustawą jest znaczne podwyższenie wysokości sankcji karnej za poszczególne typy przestępstwa szpiegostwa. Jak wskazał projektodawca w uzasadnieniu do ustawy:

> Podwyższenie wymiarów sankcji karnej jest uzasadnione tym, że w przypadku przestępstwa szpiegostwa, zagrożenie karą ma mieć głównie walor prewencyjny. Szpiedzy „zawodowi" najczęściej analizują zagrożenie karne w prawodawstwach poszczególnych państw, podejmując decyzje o podjęciu ryzyka prowadzenia swojej działalności na terytorium tych państw. Dlatego uzasadnione jest ustanowienie zagrożeń karnych na bardzo wysokim pułapie, gdyż przy

takim założeniu prewencja generalna będzie oddziaływała skuteczniej niż w przypadku innego rodzaju przestępczości, gdzie przestępcy nie biorą pod uwagę wysokości zagrożenia karnego[23].

W Kodeksie karnym z 1969 r. przestępstwo szpiegostwa w typie podstawowym było zagrożone karą pozbawienia wolności na czas nie krótszy od lat 5 lub karą śmierci. W uchylonej właśnie regulacji art. 130 k.k. typ podstawowy przestępstwa szpiegostwa był zagrożony karą pozbawienia wolności od roku do lat 10. Zauważalne jest więc wyraźne obniżenie karalności za ten typ przestępstwa przez twórców Kodeksu karnego z 1997 r. Na podstawie analizy 13 wyroków sądów karnych w sprawach o szpiegostwo, które zapadły po wejściu w życie obowiązującego k.k., autor artykułu stwierdził, że faktycznie orzekane kary oscylują wokół dolnego pułapu granic przewidzianej kary pozbawienia wolności. Tylko w trzech sprawach zapadły wyroki skazujące na karę powyżej 3 lat pozbawienia wolności:

1) na karę 4 lat pozbawienia wolności Sąd Okręgowy w Warszawie skazał w marcu 2016 r. oskarżonego o to, że w okresie od bliżej nieustalonej daty do 17 lutego 2014 r. brał udział w działalności wywiadu Republiki Białoruś przeciwko Rzeczypospolitej Polskiej, tj. o przestępstwo z art. 130 § 2 k.k.[24];
2) na karę 6 lat pozbawienia wolności, pozbawienie praw publicznych na 5 lat, przepadek dowodu rzeczowego i korzyści majątkowej Wojskowy Sąd Okręgowy w Warszawie skazał w kwietniu 2016 r. oskarżonego o branie udziału w działalności obcego wywiadu przeciwko Rzeczypospolitej Polskiej, tj. o przestępstwo z art. 130 § 1 k.k.[25];
3) na karę 7 lat pozbawienia wolności Sąd Apelacyjny w Warszawie skazał w listopadzie 2017 r. oskarżonego o przestępstwo z art. 130 § 1 k.k.[26]

Jednocześnie w analizowanych sprawach czterokrotnie zapadały wyroki skazujące na karę 3 lat pozbawienia wolności[27]; wyrok skazujący na karę 2 lat i 2 miesięcy pozbawienia wolności[28]; wyrok skazujący na karę łączną 1 roku i 6 miesięcy

[23] Uzasadnienie do *Poselskiego projektu ustawy o zmianie ustawy*…, s. 13–14.

[24] Sygn. akt XVIII K 110/15.

[25] Sygn. akt So 1/16.

[26] Sygn. akt II AKa 269/17.

[27] Kolejno: wyrok Wojskowego Sądu Okręgowego w Warszawie z 11 IV 2001 r., sygn. akt So 24/00; wyrok Wojskowego Sądu Okręgowego w Warszawie z 3 XI 2005 r., sygn. akt So 37/05; wyrok Sądu Okręgowego w Warszawie z 22 XII 2010 r., sygn. akt VIII K 272/10; wyrok Sądu Okręgowego w Warszawie z 8 III 2019 r., sygn. akt XII K 176/18.

[28] Wyrok Sądu Apelacyjnego w Białymstoku z 28 XI 2016 r., sygn. akt II AKa 96/16.

pozbawienia wolności[29]; wyrok skazujący na karę łączną 1 roku i 4 miesięcy pozbawienia wolności; przepadek przedmiotu służącego do popełnienia przestępstwa oraz przepadek dowodów rzeczowych wyszczególnionych w wykazie dowodów[30]; wyrok skazujący na karę łączną 1 roku i 2 miesięcy pozbawienia wolności[31]; wyrok skazujący dwie osoby, pierwszą na karę 1 roku pozbawienia wolności z warunkowym zawieszeniem jej wykonania na okres próby w wymiarze 3 lat, drugą na karę 1 roku pozbawienia wolności[32]; wyrok skazujący na karę 6 miesięcy pozbawienia wolności, której wykonanie warunkowo zawieszono tytułem próby na okres 2 lat oraz grzywnę w kwocie 6300 zł[33].

Odwołując się do analogicznych analiz, ustawodawca zdecydował o znacznym podniesieniu wymiaru sankcji karnej za przestępstwo szpiegostwa w typie podstawowym. Ustalił ją jako karę pozbawienia wolności na czas nie krótszy od lat 5 (do lat 30).

Ponadto ustawodawca w nowelizacji utrzymał dwa dotychczasowe typy kwalifikowane:

– pierwszy, w którym surowsza odpowiedzialność jest związana z udzielaniem, podczas brania udziału w działalności obcego wywiadu lub działaniu na jego rzecz, obcemu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę RP (art. 130 § 2). Znacznie zwiększył jednak granice sankcji karnej, z dotychczasowej kary pozbawienia wolności na czas nie krótszy od lat 3 na rzecz kary pozbawienia wolności na czas nie krótszy od lat 8 (do lat 30) albo kary dożywotniego pozbawienia wolności;
– drugi, w którym kwalifikacja jest związana z organizowaniem działalności obcego wywiadu lub kierowaniem nią (art. 130 § 4). Analogicznie zostały zwiększone granice sankcji karnej, z dotychczasowej kary pozbawienia wolności na czas nie krótszy od lat 5 albo kary 25 lat pozbawienia wolności na rzecz kary pozbawienia wolności na czas nie krótszy od lat 10 (do lat 30) albo kary dożywotniego pozbawienia wolności.

Jednocześnie ustawodawca wprowadził trzy nowe typy kwalifikowane:

– pierwszy, związany z zaostrzeniem odpowiedzialności typu podstawowego w sytuacji sprawstwa przestępstwa szpiegostwa przez funkcjonariusza publicznego oraz osobę pełniącą dyspozycyjnie terytorialną służbę wojskową. Przewidział przy tym sankcję karną w postaci kary pozbawienia wolności

[29] Wyrok Sądu Okręgowego w Warszawie z 11 VIII 2022 r., sygn. akt XVIII K 78/22.

[30] Wyrok Sądu Okręgowego w Warszawie z 21 II 2022 r., sygn. akt XVIII K 58/20.

[31] Wyrok Sądu Okręgowego w Gdańsku z 17 V 2005 r., sygn. akt IV K 86/05.

[32] Wyrok Sądu Okręgowego w Katowicach z 19 X 2015 r., sygn. akt V K 141/15.

[33] Wyrok Wojskowego Sądu Okręgowego w Warszawie z 29 IV 2019 r., sygn. akt So 5/19.

na czas nie krótszy od lat 8 (do lat 30) albo kary dożywotniego pozbawienia wolności (art. 130 § 5);

– drugi, w którym okolicznością kwalifikującą jest dokonanie, podczas zachowania mieszczącego się w typie podstawowym, dywersji, sabotażu lub dopuszczenie się przestępstwa o charakterze terrorystycznym. Przewidział w tym przypadku sankcję karną w postaci kary pozbawienia wolności na czas nie krótszy od lat 10 (do lat 30) albo kary dożywotniego pozbawienia wolności (art. 130 § 7). Co istotne, w przypadku tego czynu zabronionego ustawodawca przewidział również karalność przygotowania do niego, zagrożonego karą pozbawienia wolności od 6 miesięcy do lat 8 (art. 130 § 8);
– trzeci, w którym okolicznością kwalifikującą jest prowadzenie, podczas zachowania mieszczącego się w typie podstawowym, dezinformacji, polegającej na rozpowszechnianiu nieprawdziwych lub wprowadzających w błąd informacji, w celu wywołania poważnych zakłóceń w ustroju lub gospodarce RP, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest RP, albo skłonienie organu władzy publicznej RP, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest RP, do podjęcia lub zaniechania określonych czynności, zagrożonego karą pozbawienia wolności na czas nie krótszy od lat 8 (do lat 30) (art. 130 § 9). Oczywiste jest – co zostało potwierdzone podczas debaty nad ustawą w Senacie RP[34] – że opisane w znamionach działanie dezinformacyjne nie stanowi przestępstwa odrębnego od szpiegostwa, lecz jest jego typem kwalifikowanym. Prowadzenie dezinformacji jest więc elementem działalności wywiadowczej mieszczącej się w znamieniu brania udziału w działalności obcego wywiadu lub działaniach na jego rzecz. Zwraca uwagę wprowadzenie tym przepisem, po raz pierwszy do polskiego systemu prawnego, pojęcia dezinformacji – które dotychczas było wykorzystywane głównie w naukach o bezpieczeństwie – z jednoczesną próbą zbudowania definicji działań mieszczących się w zakresie jej prowadzenia. Należy jednak wyraźnie podkreślić, że zakres tej definicji mieści się w potocznym rozumieniu tego pojęcia. Zgodnie z rozumieniem słownikowym dezinformacja to 'wprowadzenie w błąd przez podanie fałszywych informacji; nieprawdziwa, myląca informacja'[35]. Rozumienie to, w art. 130 § 9 k.k., zostało przez ustawodawcę zawężone przez znamię celu publicznego związanego z wywołaniem poważnych zakłóceń w ustroju lub gospodarce RP, państwa sojuszniczego

[34] Debata podczas 65. posiedzenia Senatu RP X kadencji 26 VII 2023 r., https://av8.senat.pl/10Sen651 [dostęp: 28 VIII 2023].

[35] *Słownik języka polskiego PWN*, t. 1, M. Szymczak (red.), Warszawa 1999, s. 365.

lub organizacji międzynarodowej albo też skłonienie organu władzy publicznej RP, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest RP, do podjęcia lub zaniechania określonych czynności. W tym kontekście należy dodać, że w Unii Europejskiej są widoczne dwa podejścia regulacyjne do problematyki dezinformacji: horyzontalne (np. Malta) – zakazujące rozpowszechniania dezinformacji w każdym kontekście, o ile występuje zagrożenie szkodą publiczną, oraz wertykalne (np. Węgry i Francja) – zwalczające dezinformację tylko w określonych obszarach, np. podczas procesu wyborczego. Stosowane są również dwa modele odpowiedzialności – karny (np. Malta) lub administracyjny (np. Francja). Rozwiązanie przyjęte w k.k. powiela więc model regulacji horyzontalnej (chociaż zawężonej – stanowiącej element działalności wywiadowczej) z przyjętym karnym rodzajem odpowiedzialności.

W ramach typów uprzywilejowanych ustawodawca utrzymał wcześniej występującą odmianę przestępstwa szpiegostwa, polegającą na gromadzeniu, przechowywaniu lub wchodzeniu do systemu informatycznego, aby uzyskać wiadomości w celu udzielenia ich obcemu wywiadowi, lub zgłaszaniu gotowości działania na rzecz obcego wywiadu przeciwko RP (art. 130 § 3).

Poza wskazanym powyżej typem uprzywilejowanym ustawodawca dodał nowy jego typ, polegający na braniu udziału w działalności obcego wywiadu nieskierowanej przeciwko RP, prowadzonej na jej terytorium bez zgody właściwego organu udzielonej na podstawie odrębnych przepisów, zagrożonej karą pozbawienia wolności od 6 miesięcy do lat 8. Jest to istotna zmiana regulacyjna w zakresie przestępstwa szpiegostwa, gdyż wcześniej Kodeks karny nie penalizował aktywności polegającej na braniu udziału w działalności obcego wywiadu, która byłaby nieskierowana przeciwko RP, a więc niezagrażającej lub nienaruszającej zewnętrznych lub wewnętrznych interesów państwa polskiego. Podczas debaty nad projektem jako przykład takich działań minister Stanisław Żaryn wskazał działania obcego wywiadu prowadzone na terytorium RP koncentrujące się na rozpoznaniu mniejszości narodowej pochodzącej z tego kraju[36]. Należy zauważyć, że prawodawca wprowadził do przedmiotowej regulacji swoisty kontratyp, wyłączający odpowiedzialność karną osób biorących udział w działalności obcego wywiadu, objętych tzw. zgodą pierwotną uprawnionego organu. Do tych organów ustawa zaliczyła Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego, a także Szefa Agencji

[36] Wypowiedź z 14 VI 2023 r. Sekretarza Stanu w Kancelarii Prezesa Rady Ministrów, Pełnomocnika Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP Stanisława Żaryna podczas posiedzenia Komisji Nadzwyczajnej do spraw zmian w kodyfikacjach rozpatrującej projekt ustawy, iTV Sejm – transmisje archiwalne, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?rok=2023&month=06&page=5#D535320871BCC086C12589CC00473889 [dostęp: 28 VIII 2023].

Wywiadu i Szefa Służby Wywiadu Wojskowego. Jak wskazano w uzasadnieniu do projektu ustawy (…) *warunkiem koniecznym przy wydawaniu takiej zgody będzie uzyskanie przez Szefa właściwej służby informacji o celach i przebiegu prowadzonej działalności oraz brak szkodliwości tych działań dla interesów RP*[37]. W odniesieniu do wydawania zgody pierwotnej należy zwrócić uwagę na kilka istotnych zagadnień. Po pierwsze, ustawodawca zawęził znamiona przestępstwa określonego w art. 130 § 6 k.k. wyłącznie do brania udziału w działalności obcego wywiadu nieskierowanej przeciwko RP prowadzonej na jej terytorium. Potwierdził to w warunkach wyrażania tej zgody, przewidując w art. 8a ust. 1 ustawy o ABW oraz AW i w art. 9a *Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (dalej: ustawa o SKW oraz SWW), że szefowie tych służb mogą wydać zgodę na udział w działalności obcego wywiadu prowadzonej na terytorium RP, w sytuacji gdy prowadzi ją organ lub służba innego państwa, kierując się przesłanką nienaruszenia, wskazanego w tych przepisach, interesu RP. Tak skonstruowane sformułowanie powoduje, że zarówno sam typ uprzywilejowany, jak i w konsekwencji zgoda pierwotna nie obejmują zachowania polegającego na działaniu na rzecz obcego wywiadu. Po drugie, użycie w opisie znamion zwrotu „branie udziału w działalności obcego wywiadu" powoduje wyraźne odróżnienie zgody pierwotnej od zgody następczej, o której mowa w dodanych ustawą art. 22b ust. 2a ustawy o ABW oraz AW i art. 27a ust. 2a ustawy o SKW oraz SWW. Przy dokonywaniu wykładni językowej tych regulacji wyraźnie zauważa się bowiem, że zgoda pierwotna może zostać udzielona wobec działalności obcego wywiadu prowadzonej na terenie RP, jeżeli nie narusza to interesu RP, zgoda następcza zaś może zostać udzielona wyłącznie w sytuacji prowadzenia takich działań przez wywiad państwa sojuszniczego (o czym szerzej w dalszej części artykułu). Oczywisty w tym zakresie wynik wykładni językowej stoi w sprzeczności z treścią uzasadnienia do projektu ustawy, w którym wskazano, że (…) *projekt dopuszcza również możliwość prowadzenia na terytorium RP przez służby sojusznicze działalności niewymierzonej w interesy Polski*[38]. Przyjęcie rozumowania zaprezentowanego w uzasadnieniu stałoby jednak w oczywistej sprzeczności z fundamentalną zasadą zakazu wykładni synonimicznej[39], w związku z czym jedynym dopuszczalnym rozumieniem normy jest zaprezentowany wynik wykładni językowej. W przypadku zgody pierwotnej szefowie służb uprawnionych do wyrażania zgody nie są więc ograniczeni podmiotowo wyłącznie do służb sojuszniczych, a jedyną przesłanką, którą muszą się kierować, jest potencjalny skutek

[37] Uzasadnienie do *Poselskiego projektu ustawy o zmianie ustawy*…, s. 14.

[38] Tamże.

[39] Zakaz przypisywania tego samego znaczenia w obrębie danego aktu lub gałęzi prawa różnym zwrotom i pojęciom.

nienaruszenia, przez taką działalność, interesu RP. Po trzecie, w kontekście brzmienia wyżej wymienionej przesłanki oczywista wydaje się również możliwość cofnięcia udzielonej zgody przez służbę, która ją wydała, w sytuacji stwierdzenia zaistnienia potencjalności naruszania interesu RP podczas prowadzenia działalności obcego wywiadu. Służba wydająca zgodę jest więc zmuszona do stałego monitorowania działalności wywiadowczej. Może to być jednak trudne, gdyż w przypadku tej zgody brakuje rozwiązań analogicznych do zgody następczej w postaci m.in. (…) *bieżącego informowania o zakresie prowadzonych przez wywiad czynnościach*. Jak się wydaje, to zróżnicowanie świadczy o pewnym niedopatrzeniu ustawodawcy. Cofnięcie zgody wiąże się również z ryzykiem poniesienia odpowiedzialności karnej przez osobę, która pomimo jej cofnięcia kontynuowała działalność wywiadowczą, ocenioną aktualnie jako ingerującą w interesy RP. Po czwarte, wystąpienie o zgodę pierwotną musi poprzedzać rozpoczęcie przez daną osobę udziału w działalności obcego wywiadu i musi być złożone nie przez tę osobę, lecz przez organ lub służbę innego państwa, w trybie kontaktów bilateralnych pomiędzy służbami. O cofnięciu zgody organ ten lub służba, w ramach tych samych kontaktów, powinny zostać poinformowane. Organ lub służba zwracające się o zgodę muszą być objęte zgodą na współdziałanie, o której mowa w art. 8 ustawy o ABW oraz AW i art. 9 ustawy o SKW oraz SWW[40]. Należy zwrócić uwagę, że z jednej strony art. 130 § 6 k.k. mówi o zgodzie na działalność obcego wywiadu, jednak z art. 8a ust. 1 ustawy o ABW oraz AW i art. 9a ust. 1 ustawy o SKW oraz SWW wynika, że szefowie służb wydają zgodę na udział w działalności obcego wywiadu. W związku z powyższym przepisy te należy czytać kompleksowo – w ten sposób, że organ lub służba innego państwa, zwracając się o zgodę na określoną działalność wywiadowczą, wskazują jednocześnie osoby biorące w niej udział. Wyrażona zgoda przyjmuje zatem charakter skonkretyzowany wobec danej działalności wywiadowczej oraz zindywidualizowany wobec osób biorących w nich udział. Brak charakteru zindywidualizowania zgody wykluczałby jej kontratypowe rozumienie w kontekście zasady indywidualizacji odpowiedzialności karnej wyrażonej w art. 21 k.k. O wydaniu zgody lub jej cofnięciu organ lub służba innego państwa powinny poinformować osobę, która ma brać lub bierze udział w ich działalności wywiadowczej.

Poza nadaniem nowego brzmienia art. 130 k.k. nowelizacja wprowadziła również inne zmiany do Kodeksu karnego. Po pierwsze, modyfikacji uległy zasady stosowania środka karnego w postaci pozbawienia praw publicznych, który zgodnie z dodanym art. 40 § 3, w razie skazania za przestępstwo szpiegostwa, określone w art. 130 § 1–5 lub 7–9, będzie orzekany przez sąd obligatoryjnie. Jest to istotne

[40] Wskazane przepisy na mocy ustawy zostały rozszerzone o możliwość współpracy z organizacjami międzynarodowymi.

novum regulacyjne w zakresie stosowania tego środka karnego, który wcześniej był orzekany wyłącznie na zasadzie fakultatywnego uznania sędziowskiego, po spełnieniu warunków określonych w art. 40 § 2 k.k. Po drugie, przez dodanie nowego art. 112a k.k. zostały rozszerzone dotychczasowe – określone w art. 112 k.k. – zasady bezwzględnego stosowania polskiej ustawy prawnokarnej. Zgodnie z jego brzmieniem polska ustawa znajdzie zastosowanie, niezależnie od przepisów obowiązujących w miejscu popełnienia czynu zabronionego, wobec obywatela polskiego oraz cudzoziemca w razie popełnienia przestępstwa przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, jeżeli ten czyn na terytorium RP wywołał lub mógł wywołać skutek naruszający interes państwa w zakresie ochrony niepodległości, integralności terytorialnej, bezpieczeństwa zewnętrznego i wewnętrznego, obronności, polityki zagranicznej, pozycji międzynarodowej lub potencjału naukowego lub gospodarczego. Nowelizacja wychodzi więc poza przestępstwo szpiegostwa, rozciągając się zakresem stosowania na wszystkie czyny ścigane w polskim porządku prawnym, popełnione w sposób w nim wskazany, tj. przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, jeżeli mógł on wywołać lub wywołał skutek naruszający jeden ze wskazanych w nim interesów państwa[41].

Ostatnia ze zmian wprowadzonych ustawą do k.k. nadaje nowe brzmienie art. 131 k.k. regulującemu instytucję czynnego żalu, wyłączając, w ściśle określonych sytuacjach, karalność sprawców niektórych przestępstw o przewidywalnej niższej szkodliwości. Jest to jednak zmiana wyłącznie wynikowa, związana z dodaniem nowych typów przestępstw w art. 130 k.k.

Zakres zmian wprowadzonych w innych ustawach

Jak wskazano na wstępie, poza nowelizacją przepisów karnych za pomocą ustawy dokonano systemowych zmian w ośmiu ustawach, zwłaszcza w ustawach kompetencyjnych wszystkich polskich służb specjalnych. Większość tych zmian jest bezpośrednim następstwem przedefiniowania brzmienia przestępstwa szpiegostwa i wiąże się głównie ze zwiększeniem uprawnień służb odpowiedzialnych za zwalczanie tych przestępstw.

Artykuł 130 § 6 k.k. wprowadził, jak już wspomniano, swoisty kontratyp, wyłączający odpowiedzialność karną osób biorących udział w działalności obcego wywiadu, objętych jednocześnie zgodą uprawnionego organu. Poprzez zmiany

[41] Sposób wprowadzenia art. 112a do k.k. spotkał się z krytyką rzecznika praw obywatelskich, wyrażoną podczas prac legislacyjnych w Senacie RP (pismo z 19 VII 2023 r. o nr II.510.565.2023.PZ).

polegające na dodaniu art. 8a w ustawie o ABW oraz AW i art. 9a w ustawie o SKW oraz SWW, Szef ABW, Szef AW oraz Szef SKW i Szef SWW zostali upoważnieni do wyrażania takiej zgody. W przypadku Szefa ABW oraz Szefa AW jedyną braną pod uwagę przesłanką warunkującą taką zgodę jest ewentualne naruszenie przez taką działalność interesu RP w zakresie określonym w art. 112a k.k., tj. w zakresie ochrony niepodległości, integralności terytorialnej, bezpieczeństwa zewnętrznego i wewnętrznego, obronności, polityki zagranicznej, pozycji międzynarodowej lub potencjału naukowego lub gospodarczego. W przypadku szefów SKW i SWW taką przesłanką jest brak ewentualnego stwierdzenia naruszenia obronności państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP lub jednostek organizacyjnych Ministerstwa Obrony Narodowej. Co więcej, każdy z szefów został zobowiązany do prowadzenia rejestru wydanych przez siebie zgód oraz udzielania pozostałym szefom informacji zgromadzonych w prowadzonym przez niego rejestrze, w celu realizacji ich zadań dotyczących wyrażania przedmiotowej zgody. W ten sposób rejestr ma pełnić funkcję koordynacyjną służb w procesie wydawania takiej zgody.

Analizowana ustawa wprowadziła również bardzo ważne modyfikacje w uprawnieniach ABW, przyznanych jej w 2016 r. ustawą AT. Na jej mocy ABW zyskała wiele uprawnień, nakierowanych na zapobieganie, przeciwdziałanie i zwalczanie zdarzeń o charakterze terrorystycznym. Te uprawnienia zostały określone przede wszystkim w rozdziale 2 ustawy AT (*Działania antyterrorystyczne zapobiegające zdarzeniom o charakterze terrorystycznym*), i dotyczą m.in. na mocy art. 9 tej ustawy tzw. niejawnego prowadzenia działań wobec cudzoziemców, oraz w przepisach dodanych wówczas do ustawy o ABW oraz AW, w tym art. 22b (dotyczącym tajnej współpracy z ABW sprawcy przestępstwa szpiegostwa lub podejrzanego o popełnienie przestępstwa o charakterze terrorystycznym), art. 32a (dotyczącym dokonywania przez ABW oceny bezpieczeństwa systemów teleinformatycznych), art. 32b (dotyczącym udzielania na żądanie Szefa ABW informacji o budowie, funkcjonowaniu oraz zasadach eksploatacji systemów teleinformatycznych) i art. 32c (dotyczącym blokady dostępności w systemie teleinformatycznym określonych danych informatycznych lub usług teleinformatycznych mających związek ze zdarzeniem o charakterze terrorystycznym). Analizowana ustawa antyszpiegowska rozszerzyła wszystkie wskazane uprawnienia, poza dotychczasowy wyłączny obszar przestępstw o charakterze terrorystycznym, również na przestępstwo szpiegostwa[42]. Jak wskazano w uzasadnieniu do projektu ustawy, (…) *przyjęcie* [tego] *rozwiązania prawnego jest konieczne z uwagi na potrzebę minimalizacji oddziaływania*

[42] Zakres omawianych zmian skłonił Biuro Legislacyjne Sejmu do złożenia propozycji zmiany tytułu ustawy AT przez rozszerzenie jej zakresu przedmiotowego o przestępstwo szpiegostwa. Posłowie nie zaakceptowali jednak tej zmiany.

niekorzystnych skutków w regulowanej materii powstałych w wyniku konfliktu zbrojnego na Ukrainie, w szczególności znacznie zwiększonej aktywności działań wywiadowczych skierowanych przeciwko Polsce ze strony służb Federacji Rosyjskiej i Białorusi[43].

Na skutek powyższych zmian zgodnie z art. 9 ust. 1 ustawy AT, w celu rozpoznawania, zapobiegania, zwalczania i wykrywania przestępstw o charakterze terrorystycznym lub przestępstwa szpiegostwa oraz ścigania ich sprawców Szef ABW może zarządzić wobec osoby niebędącej obywatelem RP, w stosunku do której istnieje obawa co do możliwości prowadzenia przez nią działalności terrorystycznej lub popełnienia przestępstwa szpiegostwa, na okres nie dłuższy niż 3 miesiące, niejawne prowadzenie czynności polegających na:

1) uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych;
2) uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne;
3) uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej;
4) uzyskiwaniu i utrwalaniu danych zawartych na informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;
5) uzyskiwaniu dostępu i kontroli zawartości przesyłek.

Analizując brzmienie przepisu art. 22b ustawy o ABW oraz AW, należy wskazać, że od 2 lipca 2016 r. przewidywał on możliwość odstąpienia przez Szefa ABW (na podstawie ustawy o SKW oraz SWW – Szefa SKW), w przypadku gdy jest to uzasadnione względami bezpieczeństwa państwa, od obowiązku zawiadomienia właściwego prokuratora o uzasadnionym podejrzeniu popełnienia przestępstwa oraz osobie, która według uzyskanych przez ABW (SKW) informacji lub materiałów może być jego sprawcą, jeżeli informacje lub materiały uzyskane przez ABW (SKW) podczas realizacji zadań, o których mowa w art. 5 ust. 1 ustawy o ABW oraz AW (w art. 5 ust. 1 ustawy o SKW oraz SWW), wskazują na popełnienie przestępstwa szpiegostwa albo uprawdopodobniają działalność zmierzającą do popełnienia przestępstwa o charakterze terrorystycznym. Na mocy znowelizowanej ustawy to uprawnienie zostało rozszerzone, przez ust. 2a dodany do art. 22b ustawy o ABW oraz AW, o możliwość tego odstąpienia, również w przypadku sprawcy przestępstwa, o którym mowa w art. 130 § 6 k.k. (tj. szpiegostwa nieskierowanego przeciwko RP), gdy wywiad państwa sojuszniczego, w którego działalności osoba brała udział – po pierwsze, ujawni okoliczności popełnionego czynu lub prowadzonej działalności;

[43] Uzasadnienie do *Poselskiego projektu ustawy o zmianie ustawy*…, s. 15.

po drugie, zobowiąże się do dalszego jej prowadzenia w ramach tajnej współpracy z ABW lub do bieżącego informowania o zakresie prowadzonych przez ten wywiad czynności – uzyskując zgodę następczą na zasadach określonych w art. 8a. Tożsame uprawnienie uzyskał również, na mocy ust. 2a dodanego do art. 27a ustawy o SKW oraz SWW, Szef SKW. Ustawodawca nie przewidział możliwości udzielania wskazanej zgody następczej przez szefów AW i SWW, chociaż udzielają oni zgody pierwotnej. Jak się wydaje, jest to świadomy zabieg, gdyż opisany normatywnie we wskazanych przepisach ciąg zdarzeń dotyczy de facto sytuacji rozpoznania przez polską służbę kontrwywiadowczą, tj. ABW lub SKW, osób biorących udział w działalności obcego wywiadu nieskierowanej przeciwko RP, ale prowadzonej na terenie RP, do działalności których, przed formalnym wszczęciem postępowania przygotowawczego, przyzna się wywiad państwa sojuszniczego stojący za tymi działaniami i ujawni okoliczności popełnionego czynu lub prowadzonej działalności, zobowiązując się do dalszego jej prowadzenia wspólnie z ABW (lub SKW) lub do bieżącego informowania o zakresie prowadzonych przez siebie czynności. Jak się wydaje – w uzasadnieniu projektu nie zawarto takiej informacji – celem tej regulacji, wprowadzającej swoisty „akt abolicyjny", jest zabezpieczenie współpracy sojuszniczej Polski przez danie służbom kontrwywiadowczym prawa „legalizowania" takich działań, aby realizować wspólne interesy strategiczne. To rozumowanie jest potwierdzone przez użycie przez ustawodawcę zwrotu „wywiad państwa sojuszniczego" a nie, jak w przypadku zgody pierwotnej, „obcego wywiadu". Należy również zwrócić uwagę, że ustawa nie definiuje pojęcia wywiadu państwa sojuszniczego (o czym szerzej wcześniej). W rozumieniu pojęcia państwa sojuszniczego należy się odwołać do rozważań doktrynalnych wypracowanych na gruncie tzw. zasady wzajemności określonej w art. 138 k.k. Jak wskazuje Kardas:

> (…) pojęcie państwa sojuszniczego ma charakter normatywny, związany z regulacjami zawartymi w aktach prawa międzynarodowego publicznego. Państwo sojusznicze to państwo, które na mocy umów lub traktatów międzynarodowych (multilateralnych lub bilateralnych) zostało uznane za politycznego i militarnego sojusznika Rzeczypospolitej Polskiej. Innymi słowy jest to państwo, z którym Rzeczpospolita Polska zawarła sojusz polityczny lub militarny. Państwami sojuszniczymi Rzeczypospolitej są m.in. wszystkie państwa pozostające w strukturze NATO od chwili przystąpienia do paktu Rzeczypospolitej Polskiej[44].

Tak więc zgoda pierwotna może zostać udzielona na udział w działalności obcego wywiadu prowadzonej na terenie RP, jeżeli nie narusza to interesu RP. Zgoda następcza zaś, przy zachowaniu tych samych warunków, może zostać udzielona

[44] P. Kardas, w: *Kodeks karny*…, art. 138.

wyłącznie w sytuacji prowadzenia działań przez wywiad państwa sojuszniczego. Zgoda ta, podobnie jak zgoda pierwotna, może zostać cofnięta przez ABW lub SKW w sytuacji braku realizacji warunków jej udzielenia. Jej cofnięcie może nastąpić: po pierwsze, w sytuacji, gdy prowadzona działalność zacznie naruszać interesy RP; po drugie, gdy zostaną pozyskane informacje wskazujące na wprowadzenie w błąd polskich służb w zakresie okoliczności popełnionego czynu lub prowadzonej działalności; po trzecie, gdy wywiad państwa sojuszniczego zaniecha dalszego prowadzenia działalności wspólnie z ABW (lub SKW) lub przestanie na bieżąco informować o zakresie prowadzonych przez siebie czynności.

Ponadto, zgodnie ze znowelizowanym brzmieniem art. 32a ustawy o ABW oraz AW, ABW uzyskała uprawnienie przeprowadzania oceny bezpieczeństwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, lub danych przetwarzanych w tych systemach. To uprawnienie przyznano nie tylko jak wcześniej w celu zapobiegania i przeciwdziałania zdarzeniom o charakterze terrorystycznym i ich zwalczania oraz w celu wykrywania przestępstw o charakterze terrorystycznym w tym obszarze i zapobiegania im, jak również ścigania ich sprawców, lecz także w celu zapobiegania i przeciwdziałania zdarzeniom uprawdopodabniającym popełnienie przestępstwa szpiegostwa i ich zwalczania oraz w celu rozpoznawania, wykrywania przestępstwa szpiegostwa i zapobiegania mu.

W tym samym zakresie Szef ABW uzyskał, na mocy znowelizowanego art. 32b ustawy o ABW oraz AW, uprawnienie żądania od wskazanych powyżej podmiotów przedstawienia informacji o budowie, funkcjonowaniu oraz zasadach eksploatacji posiadanych systemów teleinformatycznych, w tym informacji obejmujących hasła komputerowe, kody dostępu i inne dane umożliwiające dostęp do systemu oraz ich używanie, w celu reagowania na zdarzenia o charakterze terrorystycznym lub uprawdopodabniające popełnienie przestępstwa szpiegostwa i zapobiegania im, dotyczące tych systemów lub danych, a także rozpoznawania, zapobiegania i wykrywania przestępstw o charakterze terrorystycznym i przestępstwa szpiegostwa w tym obszarze oraz ścigania ich sprawców.

Analogicznie, o przestępstwo szpiegostwa rozszerzono możliwość wnioskowania przez Szefa ABW, na podstawie art. 32c ustawy o ABW oraz AW, o zastosowanie przez sąd, po uzyskaniu pisemnej zgody Prokuratora Generalnego tzw. blokady dostępności, czyli zablokowania przez usługodawcę świadczącego usługi drogą elektroniczną dostępności w systemie teleinformatycznym określonych danych

informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodabniającego popełnienie przestępstwa szpiegostwa. Uprawnienie to staje się szczególnie istotne w kontekście art. 130 § 9 k.k., w którym ustawodawca bezpośrednio włączył czynności prowadzenia dezinformacji jako element działalności wywiadowczej. Dotychczas jedynie art. 180 *Ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne* zobowiązywał przedsiębiorców telekomunikacyjnych do niezwłocznego blokowania połączeń telekomunikacyjnych lub przekazów informacji, na żądanie uprawnionych podmiotów (tj. Policji, Biura Nadzoru Wewnętrznego, Straży Granicznej, Inspektoratu Wewnętrznego Służby Więziennej, Służby Ochrony Państwa, Agencji Bezpieczeństwa Wewnętrznego, Służby Kontrwywiadu Wojskowego, Żandarmerii Wojskowej, Centralnego Biura Antykorupcyjnego i Krajowej Administracji Skarbowej), jeżeli te połączenia mogły zagrażać obronności, bezpieczeństwu państwa oraz bezpieczeństwu i porządkowi publicznemu, albo do umożliwienia dokonania przez nie takiej blokady. Nowelizowany przepis w ustawie o ABW oraz AW – wychodząc poza dotychczasowe zawężenie do przestępstw o charakterze terrorystycznym i obejmując zakresem również przestępstwo szpiegostwa – daje podstawę do blokowania przez usługodawcę świadczącego usługi drogą elektroniczną dostępności w systemie teleinformatycznym określonych danych informatycznych lub określonych usług teleinformatycznych, rozpowszechniających nieprawdziwe lub wprowadzające w błąd informacje, w celu wywołania poważnych zakłóceń w ustroju lub gospodarce RP, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest RP, albo skłonienie organu władzy publicznej RP, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest RP, do podjęcia lub zaniechania określonych czynności.

W kontekście opisanych powyżej zmian należy dodać, że ustawa dokonała również zmian w art. 32aa ustawy o ABW oraz AW, dodanym do niej w 2018 r. *Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*, zobowiązującym ABW do wdrażania, prowadzenia i koordynacji funkcjonowania systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet. Podobnie jak omówione wcześniej zmiany cel prowadzenia systemu został rozszerzony – poza zapobieganie i przeciwdziałanie zdarzeniom o charakterze terrorystycznym i ich zwalczanie oraz poza rozpoznawanie i wykrywanie przestępstw o charakterze terrorystycznym i zapobieganie im oraz ściganie ich sprawców – na zapobieganie i przeciwdziałanie zdarzeniom uprawdopodabniającym popełnienie przestępstwa szpiegostwa i zwalczanie ich oraz na rozpoznawanie i wykrywanie przestępstwa szpiegostwa i zapobieganie mu oraz ściganie jego sprawców.

Dodatkowo, (…) *w celu budowy spójnego katalogu sankcji, a także działań prewencyjnych*[45], poprzez zmiany w ustawie emerytalnej funkcjonariuszy służb mundurowych oraz żołnierzy zawodowych do katalogu przestępstw, których potwierdzone prawomocnym wyrokiem sądu popełnienie przez żołnierza, funkcjonariusza albo emeryta lub rencistę policyjnego skutkuje utratą praw emerytalnych, dodano popełnienie przestępstwa szpiegostwa.

Poza wskazanymi zmianami ustawa wprowadziła kilka dodatkowych zmian do ustaw kompetencyjnych służb specjalnych, niezwiązanych bezpośrednio ze zmianami w zakresie przestępstwa szpiegostwa, będących wynikiem doświadczeń płynących z funkcjonowania służb, jak np. rozszerzenie w przypadku ABW, AW, SKW i SWW uprawnienia do podejmowania współdziałania nie tylko z właściwymi organami i służbami innych państw, lecz także z organizacjami międzynarodowymi.

Jedna z tych zmian jest szczególnie istotna z perspektywy ogólnego bezpieczeństwa państwa. Ustawa dokonała bowiem nowelizacji ustawy o obronie Ojczyzny, ustanawiając w art. 616a zakaz – bez zezwolenia – fotografowania, filmowania lub utrwalania w inny sposób obrazu lub wizerunku obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa, obiektów resortu obrony narodowej nieuznanych za obiekty szczególnie ważne dla bezpieczeństwa lub obronności państwa, obiektów infrastruktury krytycznej, jeżeli zostały oznaczone znakiem graficznym wyrażającym ten zakaz, oraz osób lub ruchomości znajdujących się w tych obiektach. O oznaczeniu obiektu znakiem zakazu fotografowania ma decydować organ właściwy w zakresie ochrony tego obiektu, z uwzględnieniem zagrożeń jego bezpieczeństwa. Z tym zakazem jest sprzężone nowe wykroczenie, zakładające karę aresztu albo grzywny wobec osoby, która bez zezwolenia fotografuje, filmuje lub utrwala w inny sposób obraz obiektu oznaczonego znakiem zakazu fotografowania albo wizerunek osoby lub ruchomości znajdującej się w takim obiekcie.

Podsumowanie

Podsumowując powyższe rozważania, należy wskazać, że uchwalona 17 sierpnia 2023 r. przez Sejm Rzeczypospolitej Polskiej ustawa o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, która znacznie zmieniła sposób penalizacji przestępstwa szpiegostwa w Polsce, musi być oceniona pozytywnie. Po kilkuletnich pracach legislacyjnych, będących wynikiem postulatów zgłaszanych zarówno przez przedstawicieli doktryny prawniczej, jak i praktyków zajmujących się zwalczaniem tego czynu zabronionego, pojawiła się nowelizacja, z założenia dostosowująca

[45] Uzasadnienie do *Poselskiego projektu ustawy o zmianie ustawy*…, s. 14.

przepisy Kodeksu karnego w tym zakresie do aktualnej sytuacji geopolitycznej, kształtowanej głównie przez duże zagrożenie nowymi otwartymi konfliktami zbrojnymi oraz agresywnymi działaniami niemilitarnymi opisywanymi w doktrynach wojennych. Co więcej, ta nowelizacja koresponduje z zagrożeniami związanymi z postępem technologicznym oraz z opisywanymi sposobami działania potencjalnych sprawców przestępstwa szpiegostwa.

Oczywiste jest, że przyjęte zmiany, obejmujące m.in. użycie w znamionach czynów zabronionych nowych pojęć, niewystępujących dotychczas w systemie prawnym, w tym wielu pojęć szerokich znaczeniowo, podatnych na zróżnicowane interpretacje, będą musiały zostać zweryfikowane pod kątem ich skuteczności przez praktykę postępowań karnych. Przyniesie ona odpowiedź zwłaszcza na pytanie o to, czy praktyczne rozumienie nowych przepisów nie pozbawia w konsekwencji penalizacji określonego spektrum zachowań rozpoznawanych przez służby jako zagrożenia hybrydowe prowadzone przez obce służby specjalne.

W najbliższych latach powinny zostać podjęte analizy tej skuteczności, oparte na doświadczeniach z praktyki stosowania nowych regulacji. Jeśli przyjęte rozwiązania prawne okażą się nieskuteczne, to należy rozważyć ponowne rozpatrzenie propozycji, które padały podczas opisanego procesu legislacyjnego, w tym formułowanej wówczas definicji działalności wywiadowczej.

Bibliografia

Burczaniuk P., *Przestępstwo szpiegostwa – rys historyczny, aktualne regulacje na tle doświadczeń praktycznych i analizy prawno-porównawczej wybranych państw*, w: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, P. Burczaniuk (red.), Warszawa 2017, s. 86–107.

Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-211a (cz. 1), W. Wróbel, A. Zoll (red.), Warszawa 2017.

Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, wydanie specjalne: *Wojna hybrydowa*, s. 39–50.

Słownik Języka Polskiego PWN, t. 1, M. Szymczak (red.), Warszawa 1999.

Wojnowski M., *Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, wydanie specjalne: *Wojna hybrydowa*, s. 7–38.

Źródła internetowe

Głosowanie nr 46 na 78. posiedzeniu Sejmu dnia 07-07-2023 r. o godz. 19:21:18, https://www.sejm.gov.pl/sejm9.nsf/agent.xsp?symbol=glosowania&NrKadencji=9&NrPosiedzenia=78&NrGlosowania=46 [dostęp: 28 VIII 2023].

McKew M.K., *Doktryna Gierasimowa, czyli rosyjski sposób na wojnę: chaos, a nie bomby*, Onet, 6 IX 2017 r., https://wiadomosci.onet.pl/swiat/doktryna-gierasimowa-czyli-rosyjski-sposob-na-wojne-chaos-a-nie-bomby/svh4p0h [dostęp: 28 VIII 2023].

Mikowski M., *Wiceszef MS: zmiany ws. surowszych kar za szpiegostwo są już gotowe*, PAP, 23 X 2022 r., https://www.pap.pl/aktualnosci/news%2C1460354%2Cwiceszef-ms-zmiany-ws-surowszych-kar-za-szpiegostwo-sa-juz-gotowe.html [dostęp: 28 VIII 2023].

Rejestracja posiedzenia sejmowej Komisji Nadzwyczajnej do spraw zmian w kodyfikacjach – 14 VI 2023 r., iTV Sejm – transmisje archiwalne, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?rok=2023&month=06&page=5#D535320871BCC086C12589CC00473889 [dostęp: 28 VIII 2023].

Rejestracja 77. posiedzenia Sejmu – 13 VI 2023 r., iTV Sejm – transmisje archiwalne, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?page=9#1C429C6BE7B92E29C12588FB0033AB2F [dostęp: 28 VIII 2023].

Rejestracja 65. posiedzenia Senatu RP X kadencji – 26 VII 2023 r., https://av8.senat.pl/10Sen651 [dostęp: 28 VIII 2023].

Rozpatrywanie sprawozdania Komisji o poselskim projekcie ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (druki nr 3232, 3232-A i 3358), iTV Sejm – transmisje archiwalne, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?page=2#0CD6003114C05652C12588FB0033AD73 [dostęp: 28 VIII 2023].

Uzasadnienie do *Poselskiego projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw* (druk nr 3232), https://orka.sejm.gov.pl/Druki9ka.nsf/0/F53D07E65F8EC17AC12589B1003F2A96/%24File/3232.pdf [dostęp: 28 VIII 2023].

Zmiany w Kodeksie karnym związane z zagrożeniem bezpieczeństwa państwa, Ministerstwo Sprawiedliwości, 29 III 2022 r., https://www.gov.pl/web/sprawiedliwosc/zmiany-w-kodeksie-karnym-zwiazane-z-zagrozeniem-bezpieczenstwa-panstwa [dostęp: 28 VIII 2023].

Rosyjskie źródła internetowe

Герасимов В., *Ценность науки в предвидении*, „Военно-промышленный курьер", 27 II 2013 r., https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html [dostęp: 28 VIII 2023].

Фельгенгауэр П., *Добиться превосходства над остальным человечеством Начальник российского Генштаба формулирует программу подготовки к масштабной войне*, Новая газета, 9 III 2019 r., https://novayagazeta.ru/articles/2019/03/09/79808-dobitsya--prevoshodstva-nad-ostalnym-chelovechestvom [dostęp: 28 VIII 2023].

Akty prawne

Ustawa z dnia 17 sierpnia 2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (DzU z 2023 r. poz. 1834).

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (t.j. DzU z 2024 r. poz. 248).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2023 r. poz. 913, ze zm.).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. DzU z 2022 r. poz. 2632).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2023 r. poz. 122).

Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j. DzU z 2023 r. poz. 81, ze zm.).

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. DzU z 2022 r. poz. 1648, ze zm.).

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. DzU z 2023 r. poz. 1136, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (DzU z 2022 r. poz. 1138, ze zm.).

Orzecznictwo

Wyrok Sądu Apelacyjnego w Białymstoku z 28 XI 2016 r., sygn. akt II AKa 96/16.

Wyrok Sądu Apelacyjnego w Warszawie z 24 XI 2017 r., sygn. akt II AKa 269/17.

Wyrok Sądu Okręgowego w Gdańsku z 17 V 2005 r., sygn. akt IV K 86/05.

Wyrok Sądu Okręgowego w Katowicach z 19 X 2015 r., sygn. akt V K 141/15.

Wyrok Sądu Okręgowego w Warszawie z 11 VIII 2022 r., sygn. akt XVIII K 78/22.

Wyrok Sądu Okręgowego w Warszawie z 21 II 2022 r., sygn. akt XVIII K 58/20.

Wyrok Sądu Okręgowego w Warszawie z 8 III 2019 r., sygn. akt XII K 176/18.

Wyrok Sądu Okręgowego w Warszawie z 23 III 2016 r., sygn. akt XVIII K 110/15.

Wyrok Sądu Okręgowego w Warszawie z 22 XII 2010 r., sygn. akt VIII K 272/10.

Wyrok Wojskowego Sądu Okręgowego w Warszawie z 29 IV 2019 r., sygn. akt So 5/19.

Wyrok Wojskowego Sądu Okręgowego w Warszawie z 26 IV 2016 r., sygn. akt So 1/16.

Wyrok Wojskowego Sądu Okręgowego w Warszawie z 3 XI 2005 r., sygn. akt So 37/05.

Wyrok Wojskowego Sądu Okręgowego w Warszawie z 11 IV 2001 r., sygn. akt So 24/00.

Inne dokumenty

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [dostęp: 28 VIII 2023].

Dr Piotr Burczaniuk

Doktor nauk prawnych, adiunkt Instytutu Nauk Prawnych Uniwersytetu Kardynała Stefana Wyszyńskiego, radca prawny, legislator. Specjalizuje się w teorii prawa, prawie gospodarczym i prawie IT.

Kontakt: p.burczaniuk@uksw.edu.pl

Działania informacyjne Federacji Rosyjskiej w 2023 roku

Information activities of the Russian Federation in 2023

KAROLINA KUŚMIREK

Autorka niezależna

https://orcid.org/0000-0001-6679-2088

Przegląd Bezpieczeństwa Wewnętrznego, 2024, nr 30: 79–95

https://doi.org/10.4467/20801335PBW.24.003.19605

ARTYKUŁ

Abstrakt

Podjęcie tematyki działań informacyjnych prowadzonych przez Federację Rosyjską wynikało z dynamicznych zmian zachodzących w środowisku bezpieczeństwa. Przy omówieniu tego problemu wykorzystano metody badawcze typowe dla nauk społecznych: metodę porównawczą przy zestawieniu narracji oraz metodę analizy treści obejmującą badanie materiału źródłowego pozyskanego ze środowiska informacyjnego. We wprowadzeniu przedstawiono istotę działań informacyjnych jako element prowadzonych przedsięwzięć militarnych. W kolejnej części zaprezentowano rosyjskie działania informacyjne, które umożliwiły osiągnięcie celów politycznych zarówno w samej Federacji Rosyjskiej, jak i na arenie międzynarodowej. We wnioskach wskazano te działania, które różnicowały odbiorców. Efektem przeprowadzonych badań było zidentyfikowanie rodzajów aktywności informacyjnej podejmowanej przez władze Rosji, które przyczyniły się do narzucenia swoich racji rosyjskiemu społeczeństwu oraz w globalnej rywalizacji mocarstw.

Słowa kluczowe

bezpieczeństwo międzynarodowe, Federacja Rosyjska, działania informacyjne, NATO

Abstract

The subject of information activities carried out by the Russian Federation was taken up as a result of the dynamic changes taking place in the security environment. Research methods from the field of scientific research methodology typical for social sciences were used to implement the undertaken research problem. The comparative method was used to juxtapose narratives and content analysis method included the analysis of the source material obtained from the information environment. The introduction presents information on the essence of information activities as an element of military activities. The next section of the article presents information activities that enabled the achievement of political goals both in Russia itself and on the international arena. The conclusions indicate those activities that diversified the recipients. The result of the conducted research was the identification of those information activities that allowed the Russian Federation to impose its arguments on the Russian society and in the global competition of superpowers.

Keywords

international security, Russian Federation, information activities, NATO

Wprowadzenie

Dynamiczne zmiany w środowisku międzynarodowym, które nastąpiły we współczesnym świecie, spowodowały, że informacja stała się narzędziem walki równie skutecznym co broń konwencjonalna. Postępowanie Federacji Rosyjskiej (FR) zmieniło strukturę bezpieczeństwa w Europie i doprowadziło do narzucenia nowego ładu. Działania informacyjne[1] FR miały wpływać na przeciwnika w taki sposób, aby interpretował on sytuację zgodnie z intencją jej władz i aby jego zdolności do odpowiedzi były ograniczone[2].

Podjęty problem badawczy pozwala zaprezentować na przykładzie FR sposoby realizacji celów strategicznych i ugruntowania przez mocarstwo swojej pozycji na arenie międzynarodowej przy wykorzystaniu działań informacyjnych.

[1] *Operacje informacyjne DD-3.10(A)*, Centrum Doktryn i Szkolenia Sił Zbrojnych Rzeczypospolitej Polskiej, Bydgoszcz 2017, s. 15; *Operacje psychologiczne DD-3.10.1(B)*, Centrum Doktryn i Szkolenia Sił Zbrojnych Rzeczypospolitej Polskiej, Bydgoszcz 2017, s. 13.

[2] *Operacje informacyjne DD-3.10(A)*…, s. 15–17; Z. Modrzejewski, *Operacje informacyjne*, Warszawa 2015, w wielu miejscach; *Informacyjny wymiar wojny hybrydowej*, M. Wrzosek i in. (red. nauk.), Warszawa 2018, s. 183–200.

W artykule przeanalizowano poszczególne płaszczyzny oddziaływania oraz zaprezentowano wybrane przykłady realizacji działań informacyjnych FR, które wprowadziły chaos informacyjny, doprowadziły do podważenia legitymizacji władzy i obniżenia zaufania do administracji innych państw. Efektem badań jest wskazanie konkretnych poczynań FR, które wpłynęły na zmianę architektury bezpieczeństwa w Europie.

W publikacji zastosowano metody badawcze typowe dla nauk społecznych. Metoda porównawcza została wykorzystana przy skontrastowaniu narracji FR i państw Zachodu. Metoda analizy treści obejmowała badanie materiału źródłowego pozyskanego z międzynarodowego środowiska informacyjnego i krajowych dokumentów.

Szczególne znaczenie dla podejmowanej tematyki mają publikacje dotyczące działań informacyjnych (np. *Operacje informacyjne* Zbigniewa Modrzejewskiego) czy geopolityki (np. *Putin's War on Ukraine* Samuela Ramaniego).

Dotychczas pojawiło się niewiele opracowań naukowych, które koncentrowałyby się na działaniach informacyjnych, a nie propagandowych czy dezinformacyjnych będących jedynie ich częścią.

Działania informacyjne Federacji Rosyjskiej

Federacja Rosyjska prowadzi działania informacyjne w Europie Środkowej, w tym w stosunku do Rzeczpospolitej Polskiej (RP). Dąży do osiągnięcia celów strategicznych, które umożliwiłyby jej powrót do czasów świetności, dlatego koncentruje się na wyszukiwaniu luk w systemach bezpieczeństwa i testowaniu odporności obywateli na rosyjską propagandę.

Rosja wykorzystuje działania informacyjne, w tym propagandowe i dezinformacyjne, a także używa technik informacyjnych. Posługuje się np. kluczowymi liderami opinii do wzmocnienia własnego przekazu, rozpowszechnia tematy, które są wrażliwe i dobrze rezonują w środowisku informacyjnym, takie jak uchodźcy czy możliwość zastosowania broni nuklearnej[3].

[3] L. Phillips, D. Crouch, *Have Chemical Weapons been Used in Ukraine?*, RUSI, 20 VI 2023 r., https://rusi.org/explore-our-research/publications/commentary/have-chemical-weapons-been-used-ukraine [dostęp: 7 VII 2023]; W. Courtney, *Countering Russia's Nuclear Threat in Europe*, RAND, 20 IV 2023 r., https://www.rand.org/blog/2023/04/countering-russias-nuclear-threat-in-europe.html [dostęp: 7 VII 2023].

Działania skierowane przeciwko Rzeczpospolitej Polskiej

Federacja Rosyjska zaczęła intensywnie oddziaływać na percepcję zarówno społeczności międzynarodowej, w tym państw bałtyckich, jak i własnego społeczeństwa od 2014 r. Wtedy przedstawiała Polaków jako najemnych żołnierzy na usługach kijowskich faszystów. Potwierdza to opinia, jaką wyraził minister bezpieczeństwa państwowego Donieckiej Republiki Ludowej Leonid Baranow, że 105 polskich najemników brało udział w walkach na Donbasie[4]. Rosyjski aparat propagandowy odchodzi stopniowo od przedstawiania Polaków – najemników jako osób dopuszczających się nagannych czynów, np. gwałtów na miejscowych kobietach, na rzecz deprecjonowania udziału polskich obywateli w wojnie rosyjsko-ukraińskiej[5]. Taka narracja oddziałuje na percepcję odbiorców i maskuje brak postępów w „specjalnej operacji wojskowej"[6], a ponadto staje się źródłem animozji między Ukraińcami a Polakami.

Federacja Rosyjska prowadzi działania propagandowe przeciwko RP w międzynarodowym środowisku informacyjnym. Polska była ukazywana w nim jako państwo gotowe do realizacji swoich celów i aspiracji, np. zawłaszczenia zachodnich ziem Ukrainy, szczególnie Lwowa, bez zważania na stosunki międzynarodowe. Takie fake newsy pojawiały się w 2014 r., gdy próbowano przekonać społeczność międzynarodową, że Ukraina powinna zostać podzielona między europejskie państwa i taki plan był rzekomo przygotowywany przez Unię Europejską (UE). Z jednej strony przedstawiano roszczenia RP, z drugiej strony wskazywano na dysfunkcję UE. Celem takich działań było wzbudzenie emocji w społeczeństwie i przedstawienie Polski jako agresora, a nie jako państwa udzielającego pomocy.

Działania dezinformacyjne są prowadzone przez FR długofalowo. Rosja uwypukla wrażliwe tematy, które stają się narzędziem do podsycania niepokojów społecznych. Najpierw testuje pojedyncze komunikaty, które uderzają w poczucie bezpieczeństwa obywateli, po czym tworzy z nich kampanie informacyjne podważające wiarygodność instytucji państwowych i służb mundurowych. W ten sposób następuje dekompozycja państwa i filarów jego bezpieczeństwa[7].

---

[4] *ДНР заявляет о взятых в плен польских наемниках*, РИА Новости, 2 IX 2014 r., https://ria.ru/20140902/1022431781.html [dostęp: 7 VII 2023].

[5] *СМИ сообщили об изнасиловании несовершеннолетней наемниками из Польши*, Известия, 10 II 2023 r., https://iz.ru/1468024/2023-02-10/smi-soobshchili-ob-iznasilovanii-nesovershennoletnei-naemnikami-iz-polshi [dostęp: 7 VII 2023].

[6] Termin „specjalna operacja wojskowa" jest używany przez stronę rosyjską w odniesieniu do wojny w Ukrainie, którą Rosja zaczęła na Donbasie w 2014 r., a 24 II 2022 r. rozszerzyła na całą Ukrainę.

[7] Zob. K. Kuśmirek, *Działania informacyjne i propagandowe Federacji Rosyjskiej na wybranych przykładach*, w: *Zarządzanie informacją i wiedzą na potrzeby analiz strategicznych i operacyjnych Sił Zbrojnych RP*, J. Tarczyński, A. Lis (red.), Warszawa–Bydgoszcz 2022, s. 79–93; J. Fiszer, M. Fiszer, *Wojna w Ukrainie. Od napaści do kontrofensywy*, Warszawa 2023, w wielu miejscach.

Aby uzyskać zakładane efekty informacyjne, FR angażuje dodatkowo liderów opinii publicznej, w tym przedstawicieli władzy, naukowców, oraz tzw. pożytecznych idiotów. Przykładem jest wypowiedź rosyjskiego historyka Olega Nazarowa, który wskazywał, że Polska dąży do aneksji zachodniej części Ukrainy.

Grupą opiniotwórczą byli także przedstawiciele rosyjskiej administracji. W 2023 r. szef Służby Wywiadu Zagranicznego FR (Служба Внешней Разведки Российской Федерации) Siergiej Naryszkin powielił narrację o chęci przyłączenia przez RP zachodnich ziem Ukrainy i w tym kontekście przywołał stwierdzenie, że Polska to „hiena Europy"[8]. W przekazie skierowanym do własnego społeczeństwa Rosja jest przedstawiana jako państwo zmuszone do walki o swoją integralność i wartości, ponieważ Zachód próbuje je zniszczyć. W przypadku RP mówi się o jej rusofobicznych zachowaniach[9]. Takie zjawisko nosi nazwę syndromu oblężonej twierdzy.

W 2023 r. nastąpiło zaostrzenie rosyjskiej retoryki skierowanej przeciwko Polsce. Wynikało to z zaangażowania RP w lobbing na rzecz Ukrainy. Rosyjski polityk Dmitrij Miedwiediew rozpowszechniał szczególnie wrogą propagandę wobec m.in. polskiego prezydenta: *Polskie szumowiny o imieniu „duda" zaproponowały, że rozstrzelają Rosję jak wściekłą bestię. A ktoś inny ma nadzieję negocjować z takimi draniami? To nie ma sensu*[10]. Deprecjonując wizerunek Prezydenta RP, użył pejoratywnego określenia dranie, aby stworzyć alternatywną rzeczywistość. Prezydent Białorusi Alaksandr Łukaszenka w kwietniu 2023 r. oskarżał Polskę o szkolenie najemników do zbrojnego powstania przeciwko białoruskiemu reżimowi. W rezultacie przygotowywał społeczeństwo na konieczność starcia Białorusi z Zachodem. Polska jest utożsamiana w białoruskim środowisku informacyjnym z Organizacją Traktatu Północnoatlantyckiego, dlatego walka z nią jest walką z całym Sojuszem.

Bunt Prigożyna w rosyjskim środowisku informacyjnym

Jewgienij Prigożyn, szef Grupy Wagnera[11], rozpoczął marsz na Kreml 24 czerwca 2023 r. Celem była zmiana na najważniejszych stanowiskach w Siłach Zbrojnych FR

---

[8] M. Sławiński, *Szef rosyjskiego wywiadu poszedł z tym do Łukaszenki: Polska czeka na odpowiedni moment*, Wprost, 4 IV 2023 r., https://www.wprost.pl/swiat/11165518/szef-rosyjskiego-wywiadu-poszedl-z-tym-do-lukaszenki-polska-czeka-na-odpowiedni-moment.html [dostęp: 6 VII 2023].

[9] *Польские бизнесмены ответят за русофобию Варшавы*, ВЗГЛЯД, 14 VII 2023 r., https://vz.ru/politics/2023/7/14/1221118.html [dostęp: 31 VII 2023].

[10] *Медведев считает, что заявления Польши подтверждают бессмысленность каких-либо переговоров*, Tacc, 23 VI 2023 r., https://tass.ru/politika/18100221 [dostęp: 6 VII 2023]. Tłumaczenia w artykule pochodzą od autorki (dop. red.).

[11] Grupa Wagnera została utworzona w 2014 r. jako prywatna firma wojskowa. Nazwa pochodzi od pseudonimu jej założyciela Dmitrija Utikina ps. „Wagner". Zob. A.M. Dyner, W. Lorenz, F. Bryjka,

oraz „przywrócenie sprawiedliwości”[12]. Było to wynikiem przymuszenia wagnerowców do podpisania kontraktów i wcielenia ich do rosyjskiego wojska[13]. Dodatkowym czynnikiem był konflikt między Prigożynem a rosyjskimi wojskowymi dotyczący wojny w Ukrainie i sposobu wykorzystania Grupy Wagnera. W ciągu kilku godzin odstąpiono od buntu, a Ministerstwo Obrony FR zagwarantowało bezpieczeństwo najemnikom, którzy skontaktują się z departamentem lub organami ścigania.

Prezydent FR Władimir Putin w swoim wystąpieniu wyemitowanym dzień po buncie nazwał wagnerowców zdrajcami i zaproponował przemieszczenie Grupy Wagnera na Białoruś[14]. Należy jednak rozważyć, czy działanie Prigożyna było elementem rosyjskiej maskirowki w celu przerzucenia sił na Białoruś i prowadzenia dalszych działań hybrydowych wobec NATO. Potwierdzają to słowa Łukaszenki, który stwierdził, że wagnerowcy chcą (…) *jechać na wycieczkę do Warszawy i Rzeszowa*[15].

Wiadomość, że Prigożyn wraz ze swoimi najemnikami opuścił FR i udał się na Białoruś, opublikowano w rosyjskim środowisku informacyjnym dopiero kilkanaście godzin po tym wydarzeniu. Wprowadzono chaos informacyjny, ponieważ nie podano powodów zmiany planów Prigożyna. Ponadto propagowano narrację, że najemnicy nie mieli dostatecznego wsparcia do kontynuowania buntu. Autorytet

---

Grupa Wagnera na Białorusi – konsekwencje dla NATO i UE, PISM, 7 IX 2023 r., https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-konsekwencje-dla-nato-i-ue [dostęp: 18 I 2024].

[12] *Ekspert: śmierć Prigożyna to dobra wiadomość, zaostrza się walka o władzę w otoczeniu osłabionego Putina*, PAP, 24 VIII 2023 r., https://www.pap.pl/aktualnosci/ekspert-smierc-prigozyna-dobra-wiadomosc-zaostrza-sie-walka-o-wladze-w-otoczeniu [dostęp: 18 I 2024].

[13] M. Murphy, *Ukraine war: Russia moves to take direct control of Wagner Group*, BBC, 11 VI 2023 r., https://www.bbc.com/news/world-europe-65871232 [dostęp: 25 VII 2023]. Doradca prezydenta Ukrainy Wołodymyra Zełenskiego Mychajło Podolak skomentował ten pucz jako przykład braku przyzwolenia na przemoc. Inną opinię zaprezentował dziennikarz Władisław Davidzon, który stwierdził, że była to forma upokorzenia prezydenta Rosji i pokazanie skali wewnętrznych podziałów w kierowanym przez niego systemie. Podobne zdanie wyrazili eksperci z The Atlantic Council, którzy wskazali, że Kreml utraci zaufanie oligarchów, a wojna w Ukrainie przestanie być dla nich priorytetem.

[14] *Putin wygłosił przemówienie do Rosjan. Mówił o „zdradzie organizatorów buntu”*, Rzeczpospolita, 26 VI 2023 r., https://www.rp.pl/swiat/art38660701-putin-wyglosil-przemowienie-do-rosjan-mowil-o-zdradzie-organizatorow-buntu [dostęp: 30 I 2024].

[15] *Łukaszenko w rozmowie z Putinem: Wagnerowcy chcą jechać na wycieczkę do Warszawy i Rzeszowa*, Rzeczpospolita, 23 VII 2023 r., https://www.rp.pl/polityka/art38770821-lukaszenko-w-rozmowie-z-putinem-wagnerowcy-chca-jechac-na-wycieczke-do-warszawy-i-rzeszowa [dostęp: 18 I 2024]. Zob. także: M. Duningan, *Where Will All the Wagner Group Mercenaries Go Now That Russia Has Exiled Their Leader?*, RAND, 3 VII 2023 r., https://www.rand.org/blog/2023/07/where-will-all-the-wagner-group-mercenaries-go-now.html [dostęp: 25 VII 2023]; М. Сакавик, *Зачем Путин и Лукашенко угрожают Польше „вагнеровцами”?*, DW, 24 VII 2023 r., https://www.dw.com/ru/spektakl-putina-i-lukasenko-zacem-polse-ugrozaut-vagnerovcami/a-66332295 [dostęp: 26 VII 2023]; G. Kuczyński, *Wagnerowcy. Psy wojny Putina*, Warszawa 2022, w wielu miejscach.

i wizerunek Putina jako silnego lidera niewątpliwie został osłabiony. Rosyjskiemu społeczeństwu ograniczono dostęp do informacji przez wprowadzenie cenzury. Działania psychologiczne FR wobec własnego społeczeństwa koncentrowały się na wywołaniu zmiany oceny sytuacji oraz zastraszeniu ludności. Natomiast na arenie międzynarodowej Putin przestał być postrzegany jako sprawny przywódca[16]. W związku z tym w przyszłości należy spodziewać się działań w skali globalnej, które odbudują jego reputację jako władcy imperium.

Federacja Rosyjska w celu uwiarygodnienia przekazu wykorzystała zaangażowanie kluczowych liderów, w tym polityków. Putinowi udzielili wsparcia ambasador FR w Mińsku Borys Gryzłow, a także żołnierze 155 Brygady Piechoty Morskiej Floty Pacyfiku, którzy nagrali wiadomość wideo z poparciem dla prezydenta[17]. Przedstawiciele mediów również zajęli stanowisko w tej sprawie, m.in. przewodniczący Związku Dziennikarzy Rosji Władimir Sołowjow zaapelował do rosyjskich dziennikarzy, aby nie ulegali prowokacjom i kontynuowali pracę dla dobra społeczeństwa[18]. Uruchomiono ponadto aparat propagandowy, w tym instytucje kulturalne i tzw. pożytecznych idiotów. Przedstawiciele rosyjskiego Towarzystwa Wojskowo-Historycznego szczególnie potępili próbę buntu i wezwali obywateli do niepopierania najemników. Takie gesty akceptacji wzmacniały pozytywny wizerunek prezydenta i stanowiły dowód wierności wobec władzy.

Federacja Rosyjska wykorzystała do przekonania opinii publicznej o jedności państwa związkowego także mniejszości etniczne. Podczas aneksji Krymu przywiązywano dużą wagę do kwestii Tatarów krymskich. Należy wskazać, że docenienie znaczenia mniejszości narodowych stanowi istotny element tożsamości rosyjskiego społeczeństwa. W sytuacji kryzysowej za naczelnym wodzem stanęli ataman Wszechrosyjskiego Towarzystwa Kozackiego Nikołaj Dołuda oraz przedstawiciel Centrum Koordynacyjnego Muzułmanów Północnego Kaukazu Ismail Berdiew, którzy uznali bunt za zdradę państwa i doprowadzanie do anarchii. W celu zastraszenia rosyjskiego społeczeństwa wskazywano, że najemnicy próbowali wywołać bratobójczą wojnę domową oraz mieli dostęp do arsenału nuklearnego.

Do ustabilizowania sytuacji zewnętrznej po buncie Prigożyna FR użyła korpusu dyplomatycznego, ale prowadziła też intensywną politykę zagraniczną w międzynarodowym środowisku informacyjnym.

---

[16] Prigożyn zginął w katastrofie lotniczej 23 VIII 2023 r. Jego śmierć może być ostrzeżeniem, że nie wolno przeciwstawiać się prezydentowi Rosji.

[17] *Глава Приморья опубликовал обращение 155-й бригады морской пехоты в поддержку Путина*, Tacc, 25 VI 2023 r., https://tass.ru/armiya-i-opk/18109961 [dostęp: 26 VII 2023].

[18] *Глава СЖР призвал журналистов не поддаваться на провокации*, РИА Новости, 24 VI 2023 r., https://ria.ru/20230624/zhurnalisty-1880217102.html [dostęp: 26 VII 2023].

Wsparcie dla prezydenta FR okazały: Wenezuela, Indie, Iran oraz Arabia Saudyjska. Część z tych państw została wymieniona w Strategii Bezpieczeństwa Federacji Rosyjskiej (2021 r.), w której wskazano relacje bilateralne z nimi[19].

Dyslokację Grupy Wagnera po puczu Prigożyna należy rozpatrywać jako przemieszczenie sił rosyjskich na Białoruś i wzmocnienie tego kierunku[20]. Przedsięwzięcie miało zdezorientować opinię publiczną (zastosowano technikę nagromadzenia informacji) oraz zamaskować realne posunięcia. Aktywność Grupy Wagnera trzeba zaliczyć do działań hybrydowych, które w tamtym momencie można było skuteczniej zneutralizować przez podjęcie działań niekinetycznych niż wyłącznie kinetycznych.

Grupa Wagnera kontynuuje swoją działalność jako firma i dokumentuje ją na profilu Orkiestra Wagnera na portalu Telegram. Przedstawia tam postępy na polu walki, np. pod Bachmutem, gdzie zniszczono polską armatohaubicę Krab. Prowadzi także działania psychologiczne ukierunkowane na budowanie pozytywnego wizerunku, np. zrelacjonowała spotkanie z dziećmi z klubu patriotycznego Ryś. To zmieniało obraz wagnerowców w oczach Białorusinów. Te same działania prowadzono podczas aneksji Krymu. Ich celem było przekonanie społeczeństwa o pokojowych zamiarach Grupy Wagnera i stworzenie wrażenia, że jej członkowie są częścią społeczności[21].

Działania informacyjne polegają na wzmacnianiu przychylnych wobec FR postaw przedstawicieli innych państw, którzy legitymizują jej działania i potwierdzają jej pozycję w światowym systemie bezpieczeństwa.

Szczyt NATO w Wilnie

Podczas szczytu NATO w Wilnie (11–12 lipca 2023 r.) FR zastosowała technikę kontrastowania: zły Zachód przeciwko dobrej Rosji. Jednocześnie demonstrowała, że tylko ona jest w stanie zapewnić światowe bezpieczeństwo (zastosowano technikę wyolbrzymienia), NATO zaś jest archaiczną strukturą, która nie spełnia obietnic i nadaje priorytet interesom partykularnym. Przyjazd na ten szczyt prezydenta Stanów Zjednoczonych Ameryki Joe Bidena nasilił rywalizację między mocarstwami.

---

[19] *Указ Президента Российской Федерации от 02.07.2021 г. № 400*, Kremlin.ru, http://www.kremlin.ru/acts/bank/47046 [dostęp: 27 VI 2023].

[20] *Лукашенко подтвердил приезд главы ЧВК „Вагнер" Пригожина в Беларусь*, БЕЛТА, 27 VI 2023 r., https://www.belta.by/president/view/lukashenko-podtverdil-priezd-glavy-chvk-vagner-prigozhina-v-belarus-574036-2023/ [dostęp: 10 VII 2023].

[21] *Wagnerowcy odwiedzili „patriotyczne" białoruskie dzieci*, Belsat, 27 VII 2023 r., https://belsat.eu/pl/news/27-07-2023-wagnerowcy-odwiedzili-patriotyczne-bialoruskie-dzieci [dostęp: 28 VII 2023]. Zob. szerzej: Оркестр Вагнера, wpis na kanale Telegram, https://t.me/s/orchestra_w [dostęp: 28 VII 2023].

Przedstawiciele ukraińskiej administracji oraz mediów, m.in. redaktor portalu Europejska Pravda Serhij Sydorenko, wyrazili opinię, że nieprzedstawienie Ukrainie podczas tego szczytu konkretnego planu przystąpienia do Sojuszu Północnoatlantyckiego będzie dla niej ciosem[22]. Zełenski budował w świadomości społeczności międzynarodowej, m.in. przez działania dyplomatyczne, potrzebę akcesji Ukrainy do NATO. Przykładem tego był apel do Bidena o zaproszenie Ukrainy do Sojuszu, nawet jeśli miałaby ona zostać członkiem tej organizacji po zakończeniu wojny. Szczyt w Wilnie miał być dla Ukrainy kamieniem milowym w drodze do akcesji do Sojuszu i mocnym sygnałem ostrzegawczym dla FR. Podniosłoby to morale oraz dodało ukraińskim żołnierzom i ludności sił do dalszej walki. Należy jednak podkreślić, że wstąpienie do NATO jest uwarunkowane prawnie, czego przykładem może być Szwecja, która jeszcze nie została włączona w strukturę Sojuszu[23]. Szczyt w Wilnie był jedynie wstępem do spotkania, które odbędzie się w Waszyngtonie w 2024 r. Decydujące zobowiązania zostaną podjęte dopiero po wyborach prezydenckich w USA (jesień 2024 r.) i objęciu władzy przez kolejną amerykańską administrację oraz po zmianie na stanowisku sekretarza generalnego NATO, która nastąpi podczas szczytu w Waszyngtonie.

W rosyjskim środowisku informacyjnym szczyt w Wilnie był przedstawiany jako wydarzenie, podczas którego państwa NATO dążyły do rozmieszczenia 300 000 swoich żołnierzy wzdłuż granicy z FR. Jednocześnie ukazywano Rosję jako ofiarę działań Sojuszu i powtarzano, że dąży ona jedynie do zapewnienia bezpieczeństwa swoim obywatelom[24]. Przekaz został uwiarygodniony przez prezydenta Putina, który stwierdził: *Jeśli chodzi o członkostwo Ukrainy w NATO, wielokrotnie mówiliśmy, że stanowi to oczywiście zagrożenie dla bezpieczeństwa Rosji. I tak naprawdę jednym z powodów specjalnej operacji wojskowej jest groźba wstąpienia Ukrainy do NATO*[25].

Oprócz tego FR negatywnie odniosła się do deklaracji Sojuszu o przekazaniu stronie ukraińskiej amunicji kasetowej. Rosja uznała, że Siły Zbrojne Ukrainy użyją

---

[22] *Ukraina w NATO? Publicysta: Brak konkretnego planu na szczycie w Wilnie będzie dla nas ciosem*, TVP Info, 21 VI 2023 r., https://www.tvp.info/70705131/ukrainski-publicysta-przedstawienie-na-szczycie-w-wilnie-niekonkretnego-planu-czlonkostwa-ukrainy-w-nato-bedzie-dla-nas-ciosem [dostęp: 7 VII 2023].

[23] Artykuł został ukończony 30 IX 2023 r. W tym czasie Szwecja miała status państwa zaproszonego do NATO. Z dniem 7 III 2024 r. stała się członkiem Sojuszu.

[24] *Политолог назвала главное событие предстоящего саммита НАТО в Вильнюсе*, Известия, 10 VII 2023 r., https://iz.ru/1542191/2023-07-10/politolog-nazvala-glavnoe-sobytie-predstoiashchego-sammita-nato-v-vilniuse [dostęp: 18 VII 2023].

[25] *Путин назвал последствия принятия Украины в НАТО*, РИА Новости, 13 VII 2023 r., https://crimea.ria.ru/20230713/putin-nazval-posledstviya-prinyatiya-ukrainy-v-nato-1130043821.html [dostęp: 18 VII 2023].

tej broni do uderzeń na cele cywilne, dlatego będzie walczyć z tymi siłami[26]. Działania informacyjne prowadzone wobec rosyjskiego społeczeństwa miały na celu zmianę percepcji, a także wzmocnienie negatywnych emocji wobec państw Zachodu, które przedstawiano jako zagrożenie suwerenności Rosji.

W zachodnich środkach masowego przekazu koncentrowano się głównie na pokazaniu jedności Sojuszu, ale wskazywano jednocześnie na dualizm oczekiwań strony ukraińskiej i państw członkowskich. Ukraińcy byli zdania, że po 500 dniach wojny udowodnili swoją gotowość do akcesji, NATO natomiast zajęło stanowisko, że rozszerzenie Paktu Północnoatlantyckiego o Ukrainę nie jest możliwe do momentu zakończenia wojny. Członkostwo Ukrainy mogłoby bowiem zachęcić FR do eskalacji działań na inne państwa Europy[27]. Taka sytuacja przyczynia się do budowania wewnętrznych podziałów w NATO oraz stworzenia przestrzeni dla rosyjskiej propagandy deprecjonującej Ukrainę na Zachodzie.

Inny obraz bieżącej sytuacji geopolitycznej był kształtowany w amerykańskim środowisku informacyjnym. W USA szczyt w Wilnie wykorzystano jako wstęp do kampanii prezydenckiej, w której wątek ukraiński będzie podejmowany przez pryzmat wydatkowania pieniędzy i udzielonego wsparcia. Tezę tę potwierdził Lorne Cook w artykule w „The Washington Post", w którym podsumował szczyt. Wskazał on, że ukraińska administracja jest wdzięczna za obietnice większej ilości broni i amunicji, lecz jednocześnie rozczarowana, że nie wyznaczono konkretnej daty wstąpienia Ukrainy do NATO. Publicysta zwrócił uwagę na kwestię finansowania i niewywiązywania się sojuszników z zobowiązania do zwiększenia procentu PKB przeznaczanego na obronność[28]. Działania informacyjne FR i USA będą ewoluować w zależności od rozwoju sytuacji w międzynarodowym środowisku bezpieczeństwa.

---

[26] Г. Мишутин, Н. Гасымов, *Чем для Украины закончился саммит НАТО в Вильнюсе*, Ведомости, 13 VI 2023 r., https://www.vedomosti.ru/politics/articles/2023/07/13/985067-mezhdunarodnie-novosti [dostęp: 18 VII 2023].

[27] M. Gebauer, R. Naukirch, Ch. Schult, *Gehört die Ukraine in die NATO?*, Spiegel, 10 VII 2023 r., https://www.spiegel.de/politik/nato-gipfel-in-vilnius-gehoert-die-ukraine-in-das-buendnis-a-e79ca421-d4d9-4663-9fac-1530b01b3b43 [dostęp: 17 VII 2023]; N. Barotte, *Garanties de sécurité, processus d'adhésion de l'Ukraine… Les grands enjeux du sommet de l'OTAN à Vilnius*, Le Figaro, 10 VII 2023 r., https://www.lefigaro.fr/international/otan-quelles-garanties-de-securite-pour-l-ukraine-le-dilemme-allie-20230710 [dostęp: 17 VII 2023]; *NATO summit: Ukraine's future membership to be discussed by leaders in Vilnius*, BBC, 11 VI 2023 r., https://www.bbc.com/news/world-europe-66157625 [dostęp: 18 VII 2023].

[28] L. Cook, *NATO summit results in brief: Mixed news for Ukraine, hope for Sweden and a response to Russia*, The Washington Post, 12 VI 2023 r., https://www.washingtonpost.com/world/2023/07/12/nato-summit-vilnius-lithuania-ukraine/980690b6-20c8-11ee-8994-4b2d0b694a34_story.html [dostęp: 17 VII 2023]. Por. *Despite Successes at NATO Summit, Divisions Remain*, The New York Times, 12 VII 2023 r., https://www.nytimes.com/2023/07/12/world/europe/nato-summit-ukraine-biden.html [dostęp: 17 VII 2023]. Zob. także: S. Ramani, *Putin's War on Ukraine*, London 2023, w wielu miejscach.

Perspektywy

Działania informacyjne Rosji w Europie Środkowej będą koncentrowały się na tworzeniu nowego ładu, jak również na wzbudzaniu emocji w społeczeństwie. Wynika to z chęci odbudowy imperialnych wpływów oraz z potrzeby zapewnienia bezpieczeństwa obywatelom rosyjskojęzycznym w różnych państwach.

Należy zwrócić uwagę, że FR oddziałuje na międzynarodową społeczność przez wzbudzanie strachu i przekraczanie granic respektowanych przez państwa demokratyczne. Działania niekinetyczne, w tym działania informacyjne, będą takie same jak wcześniej. Zmienią się tylko czas i narzędzia, techniki informacyjne natomiast pozostaną niezmienne. Część rosyjskiej narracji jest powielana od aneksji Krymu w 2014 r. i wciąż aktualna. Propagowane treści dotyczą m.in.:

1) silnej i nierozerwalnej więzi historycznej Donbasu z Rosją,
2) intensyfikacji działań NATO przy granicy z FR, które są interpretowane jako atak na rosyjską suwerenność,
3) rusofobii Zachodu, a szczególnie USA[29].

Ich celem jest wpływanie na relacje dwustronne Rosji i Zachodu oraz podważanie pozycji legalnie wybranej władzy w Ukrainie. Prezydent FR wzywał ukraińskie siły zbrojne do obalenia rządu w Kijowie i siłowego przejęcia kontroli nad państwem. Taka postawa FR stała się przedmiotem wystąpienia Johna Kelleya, amerykańskiego ministra ds. politycznych, który powiedział m.in.: *Słyszeliśmy, jak Rosja twierdzi, że nie jest agresorem, że próbuje powstrzymać „ludobójstwo" we wschodniej Ukrainie, że musi „zdenazyfikować" ukraiński rząd i walczyć z narkomanami oraz satanistami. Bez względu na to, jaka jest dzisiejsza wymówka, nie może ona ukryć faktu, że Rosja nie jest ofiarą, za którą się podaje*[30].

Rosja wpływała na polskie środowisko informacyjne zarówno podczas rosyjsko-białoruskich ćwiczeń wojskowych Zapad-21, jak i w trakcie ćwiczeń realizowanych przez RP (m.in. ćwiczenia Anakonda)[31]. Dążyła przez lata do wyeksponowania tematów, które zdyskredytują polską administrację rządową i służby mundurowe.

---

[29] *В ДНР рассказали, что стало точкой невозврата в Донбассе*, РИА Новости, 13 IV 2021 r., https://ria.ru/20210413/operatsiya-1728010412.html [dostęp: 10 VII 2023].

[30] J. Kelley, *Remarks at a UN Security Council Briefing Called by Russia on Russophobia*, United States Mission to the United Nations, 14 III 2023 r., https://usun.usmission.gov/remarks-at-a-un-security-council-briefing-called-by-russia-on-russophobia/ [dostęp: 10 VII 2023]. Przeciwdziałaniem dezinformacji propagowanej przez Rosję jest rzetelne informowanie opinii publicznej. Zob. *EU response to Russia's invasion of Ukraine*, European Council, https://www.consilium.europa.eu/en/policies/eu-response-ukraine-invasion/ [dostęp: 10 VII 2023].

[31] Ćwiczenia Zapad-21 skoncentrowały się m.in. na działaniach psychologicznych destabilizujących wewnętrzny system bezpieczeństwa RP. Dodatkowo były one *show of force* Sił Zbrojnych FR i sposobem na odwrócenie uwagi społeczeństwa od bieżących wyzwań na arenie międzynarodowej.

Deprecjonowano m.in. wysokich rangą oficerów przez preparowanie wywiadów (np. rozmowa z gen. dyw. Maciejem Jabłońskim w 2018 r.)[32], dezinformowano na temat wypełnienia sojuszniczych zobowiązań oraz zakupu uzbrojenia.

Operacje w cyberprzestrzeni są innym sposobem destabilizowania środowiska informacyjnego. Jednym z wykorzystywanych w nich narzędzi jest *deepfake* służący do fałszowania obrazu. Rosja rozwija je, aby zdobyć zaufanie społeczeństwa lub zdyskredytować decydentów.

Wspólnym mianownikiem niekinetycznych działań podejmowanych przez FR jest chęć utrzymania pozycji hegemona w Europie Środkowej. Z uwagi na wojskowe zakupy poczynione przez Polskę należy spodziewać się rosyjskiej aktywności, której celem będzie umniejszenie potencjału Sił Zbrojnych RP.

Działania przeciwnika przy granicy z RP generują wiele zagrożeń, np. eskalację kryzysu migracyjnego, sabotaż, atak na infrastrukturę krytyczną[33]. Odpowiedź polskiej strony może stać się pretekstem dla FR do całkowitego zaanektowania Białorusi i w ten sposób udzielenia jej pomocy. Należy zaznaczyć, że w obliczu zagrożenia zapewnienie bezpieczeństwa polskim obywatelom jest priorytetem.

W związku z tym, że sytuacja geopolityczna na Bliskim Wschodzie oraz Indo-Pacyfiku jest coraz bardziej napięta, FR będzie realizowała działania informacyjne (w tym działania psychologiczne, takie jak demonstracja siły i presja psychologiczna), które ustabilizują jej pozycję w rejonie Morza Bałtyckiego oraz wymuszą ustępstwa Zachodu i zamrożą na pewien czas działania w Europie (wojna z Ukrainą)[34].

Wnioski

Federacja Rosyjska prowadzi działania informacyjne przez dostosowanie się do realiów funkcjonowania poszczególnych państw (uwarunkowania polityczne, społeczne, ekonomiczne itp.). Uwzględnienie tych realiów pozwoliło FR na zastosowanie

[32] Fake news dotyczący ćwiczeń Anakonda-18 wraz z wypowiedzią gen. dyw. Macieja Jabłońskiego został opublikowany na prorosyjskim, dezinformującym portalu Niezależny Dziennik Polityczny. Zob. *Gen. Jabłoński OSTRO: Dowódca Operacyjny zhańbił moją dywizję bojową! O co chodzi?*, Niezależny Dziennik Polityczny, 13 XI 2018 r., https://dziennik-polityczny.com/2018/11/13/gen-jablonski-ostro-dowodc%D0%B0-operacyjny-zhanbil-moja-dywizje-bojowa-o-co-chodzi/ [dostęp: 7 VII 2023].

[33] A.M. Dyner, *Grupa Wagnera na Białorusi – potencjalne zagrożenia dla Polski*, PISM, 27 VII 2023 r., https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-potencjalne-zagrozenia-dla-polski [dostęp: 28 VII 2023].

[34] Zob. M. Priebe, *Alternative Futures Following a Great Power War: Miranda Priebe and Bryan Frederick in Conversation*, RAND, 9 V 2023 r., https://www.rand.org/blog/2023/05/alternative-futures-following-a-great-power-war-miranda.html [dostęp: 7 VII 2023].

takich narzędzi, jak np. metody oddziaływania psychologicznego, za pomocą których wywiera się nacisk na wolę decydentów i kształtuje się rozumienie sytuacji przez społeczeństwo. Rosja po raz kolejny próbuje wpłynąć na architekturę bezpieczeństwa.

Główne wnioski, jakie się nasuwają, to:

1. Działania informacyjne FR są prowadzone długofalowo i ukierunkowane na utrzymanie roli hegemona oraz chęć powrotu do czasów świetności rosyjskiego imperium.
2. Działania informacyjne są elementem rozgrywki mocarstw na poziomie globalnym. Intensyfikacja potencjalnego konfliktu na Indo-Pacyfiku zmieni układ sił na świecie.
3. Szczyt NATO w Wilnie w 2023 r. był wstępem do dyskusji na temat bieżącej sytuacji geopolitycznej, w tym istniejących na arenie międzynarodowej konfliktów i ich skutków. Ostateczne decyzje dotyczące działań Sojuszu zapadną podczas spotkania w Waszyngtonie w 2024 r. Duży wpływ na nie będzie miała nowa amerykańska administracja, która nada swój ton w globalnych relacjach.
4. Federacja Rosyjska permanentnie prowadzi wrogie działania informacyjne w państwach regionu Morza Bałtyckiego w celu zminimalizowania w nich dominacji NATO. Rozpowszechnia narracje i stosuje narzędzia, które sprawdziły się w poprzednich konfliktach.
5. Rosja eskaluje napięcie przez straszenie użyciem taktycznych ładunków jądrowych. Może to być wstęp do stworzenia warunków, w których zastosuje ona broń masowego rażenia.
6. Wojna rosyjsko-ukraińska doprowadziła do sytuacji, w której Ukraina stała się najbardziej zmilitaryzowanym państwem Europy. Zweryfikowało to w rezultacie możliwości technologiczne Zachodu i samej FR.

Wiele działań informacyjnych realizowanych przez Rosję w ramach polityki wewnętrznej oraz zagranicznej umożliwiło osiągnięcie części jej celów strategicznych i informacyjnych. Rosja pozostaje podmiotem stosunków międzynarodowych i jest nadal aktywnym uczestnikiem globalnej rywalizacji. Działania informacyjne FR w Europie są prowadzone wobec podmiotów stosunków międzynarodowych w celu ugruntowania rosyjskiej pozycji w regionie i osiągnięcia założonych efektów informacyjnych. Zmiana percepcji odbiorców oraz tworzenie alternatywnej rzeczywistości jest istotnym czynnikiem destabilizacji państw Zachodu. Działania informacyjne FR silnie oddziałują na społeczeństwa RP i państw bałtyckich. Poczucie strachu wśród obywateli wpływa na ich decyzje polityczne i jest czynnikiem determinującym postawy społeczne. Władze Rosji oddziałują także na własne społeczeństwo, aby uzyskać poparcie dla „wojskowej operacji specjalnej" i ugruntować pragnienie powrotu do czasów świetności imperium. Typowa dla rosyjskiego społeczeństwa wyższość

zachowań kolektywnych nad jednostkowymi, nieprzychylne nastawienie do zmiany realiów oraz myślenie o Wielkiej Rosji przez pryzmat mniejszości etnicznych stanowią fundament działań informacyjnych FR.

Należy uznać, że problematyka przedstawiona w artykule jest zagadnieniem istotnym zarówno dla przedstawicieli środowiska naukowego, jak i militarnego. Wnioski z prezentowanych badań mogą stanowić punkt wyjścia do przygotowania raportu dla decydentów. Jednocześnie artykuł nie wyczerpuje tematu i nie podejmuje wielu jego aspektów, co daje asumpt do dalszych badań.

Bibliografia

Fiszer J., Fiszer M., *Wojna w Ukrainie. Od napaści do kontrofensywy*, Warszawa 2023.

Informacyjny wymiar wojny hybrydowej, M. Wrzosek i in. (red. nauk.), Warszawa 2018.

Kuczyński G., *Wagnerowcy. Psy wojny Putina*, Warszawa 2022.

Lis A., Tarczyński J., *Zarządzanie informacją i wiedzą na potrzeby analiz strategicznych i operacyjnych Sił Zbrojnych RP*, Warszawa–Bydgoszcz 2022.

Modrzejewski Z., *Operacje informacyjne*, Warszawa 2015.

Operacje informacyjne DD-3.10(A), Centrum Doktryn i Szkolenia Sił Zbrojnych Rzeczypospolitej Polskiej, Bydgoszcz 2017.

Operacje psychologiczne DD-3.10.1(B), Centrum Doktryn i Szkolenia Sił Zbrojnych Rzeczypospolitej Polskiej, Bydgoszcz 2017.

Ramani S., *Putin's War on Ukraine*, London 2023.

Źródła internetowe

Barotte N., *Garanties de sécurité, processus d'adhésion de l'Ukraine… Les grands enjeux du sommet de l'OTAN à Vilnius*, Le Figaro, 10 VII 2023 r., https://www.lefigaro.fr/international/otan-quelles-garanties-de-securite-pour-l-ukraine-le-dilemme-allie-20230710 [dostęp: 17 VII 2023].

Cook L., *NATO summit results in brief: Mixed news for Ukraine, hope for Sweden and a response to Russia,* The Washington Post, 12 VI 2023 r., https://www.washingtonpost.com/world/2023/07/12/nato-summit-vilnius-lithuania-ukraine/980690b6-20c8-11ee-8994-4b2d0b694a34_story.html [dostęp: 17 VII 2023].

Courtney W., *Countering Russia's Nuclear Threat in Europe*, RAND, 20 IV 2023 r., https://www.rand.org/blog/2023/04/countering-russias-nuclear-threat-in-europe.html [dostęp: 7 VII 2023].

Despite Successes at NATO Summit, Divisions Remain, The New York Times, 12 VII 2023 r., https://www.nytimes.com/2023/07/12/world/europe/nato-summit-ukraine-biden.html [dostęp: 17 VII 2023].

Duningan M., *Where Will All the Wagner Group Mercenaries Go Now That Russia Has Exiled Their Leader?*, RAND, 3 VII 2023 r., https://www.rand.org/blog/2023/07/where-will-all-the-wagner-group-mercenaries-go-now.html [dostęp: 25 VII 2023].

Dyner A.M., *Grupa Wagnera na Białorusi – potencjalne zagrożenia dla Polski*, PISM, 27 VII 2023 r., https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-potencjalne-zagrozenia-dla-polski [dostęp: 28 VII 2023].

Dyner A.M., Lorenz W., Bryjka F., *Grupa Wagnera na Białorusi – konsekwencje dla NATO i UE*, PISM, 7 IX 2023 r., https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-konsekwencje-dla-nato-i-ue [dostęp: 18 I 2024].

Ekspert: śmierć Prigożyna to dobra wiadomość, zaostrza się walka o władzę w otoczeniu osłabionego Putina, PAP, 24 VIII 2023 r., https://www.pap.pl/aktualnosci/ekspert-smierc-prigozyna-dobra-wiadomosc-zaostrza-sie-walka-o-wladze-w-otoczeniu [dostęp: 18 I 2024].

EU response to Russia's invasion of Ukraine, European Council, https://www.consilium.europa.eu/en/policies/eu-response-ukraine-invasion/ [dostęp: 10 VII 2023].

Gebauer M., Naukirch R., Schult Ch., *Gehört die Ukraine in die Nato?*, Spiegel, 10 VII 2023 r., https://www.spiegel.de/politik/nato-gipfel-in-vilnius-gehoert-die-ukraine-in-das-buendnis-a-e79ca421-d4d9-4663-9fac-1530b01b3b43 [dostęp: 17 VII 2023].

Gen. Jabłoński OSTRO: Dowódca Operacyjny zhańbił moją dywizję bojową! O co chodzi?, Niezależny Dziennik Polityczny, 13 XI 2018 r., https://dziennik-polityczny.com/2018/11/13/gen-jablonski-ostro-dowodc%D0%B0-operacyjny-zhanbil-moja-dywizje-bojowa-o-co-chodzi/ [dostęp: 7 VII 2023].

Kelley J., *Remarks at a UN Security Council Briefing Called by Russia on Russophobia*, United States Mission to the United Nations, 14 III 2023 r., https://usun.usmission.gov/remarks-at-a-un-security-council-briefing-called-by-russia-on-russophobia/ [dostęp: 10 VII 2023].

Łukaszenko w rozmowie z Putinem: Wagnerowcy chcą jechać na wycieczkę do Warszawy i Rzeszowa, Rzeczpospolita, 23 VII 2023 r., https://www.rp.pl/polityka/art38770821-lukaszenko-w-rozmowie-z-putinem-wagnerowcy-chca-jechac-na-wycieczke-do-warszawy-i-rzeszowa [dostęp: 18 I 2024].

Murphy M., *Ukraine war: Russia moves to take direct control of Wagner Group*, BBC, 11 VI 2023 r., https://www.bbc.com/news/world-europe-65871232 [dostęp: 25 VII 2023].

NATO summit: Ukraine's future membership to be discussed by leaders in Vilnius, BBC, 11 VI 2023 r., https://www.bbc.com/news/world-europe-66157625 [dostęp: 18 VII 2023].

Phillips L., Crouch D., *Have Chemical Weapons been Used in Ukraine?*, RUSI, 20 VI 2023 r., https://rusi.org/explore-our-research/publications/commentary/have-chemical-weapons-been-used-ukraine [dostęp: 7 VII 2023].

Priebe M., *Alternative Futures Following a Great Power War: Miranda Priebe and Bryan Frederick in Conversation*, RAND, 9 V 2023 r., https://www.rand.org/blog/2023/05/alternative-futures-following-a-great-power-war-miranda.html [dostęp: 7 VII 2023].

Putin wygłosił przemówienie do Rosjan. Mówił o „zdradzie organizatorów buntu", Rzeczpospolita, 26 VI 2023 r., https://www.rp.pl/swiat/art38660701-putin-wyglosil-przemowienie-do-rosjan-mowil-o-zdradzie-organizatorow-buntu [dostęp: 30 I 2024].

Sławiński M., *Szef rosyjskiego wywiadu poszedł z tym do Łukaszenki: Polska czeka na odpowiedni moment*, Wprost, 4 IV 2023 r., https://www.wprost.pl/swiat/11165518/szef-rosyjskiego-wywiadu-poszedl-z-tym-do-lukaszenki-polska-czeka-na-odpowiedni-moment.html [dostęp: 6 VII 2023].

Ukraina w NATO? Publicysta: Brak konkretnego planu na szczycie w Wilnie będzie dla nas ciosem, TVP Info, 21 VI 2023 r., https://www.tvp.info/70705131/ukrainski-publicysta-przedstawienie-na-szczycie-w-wilnie-niekonkretnego-planu-czlonkostwa-ukrainy-w-nato-bedzie-dla-nas-ciosem [dostęp: 7 VII 2023].

Wagnerowcy odwiedzili „patriotyczne" białoruskie dzieci, Belsat, 27 VII 2023 r., https://belsat.eu/pl/news/27-07-2023-wagnerowcy-odwiedzili-patriotyczne-bialoruskie-dzieci [dostęp: 28 VII 2023].

Rosyjskie źródła internetowe

В ДНР рассказали, что стало точкой невозврата в Донбассе, РИА Новости, 13 IV 2021 r., https://ria.ru/20210413/operatsiya-1728010412.html [dostęp: 10 VII 2023].

Глава Приморья опубликовал обращение 155-й бригады морской пехоты в поддержку Путина, Тасс, 25 VI 2023 r., https://tass.ru/armiya-i-opk/18109961 [dostęp: 26 VII 2023].

Глава СЖР призвал журналистов не поддаваться на провокации, РИА Новости, 24 VI 2023 r., https://ria.ru/20230624/zhurnalisty-1880217102.html [dostęp: 26 VII 2023].

ДНР заявляет о взятых в плен польских наемниках, РИА Новости, 2 IX 2014 r., https://ria.ru/20140902/1022431781.html [dostęp: 7 VII 2023].

Лукашенко подтвердил приезд главы ЧВК „Вагнер" Пригожина в Беларусь, БЕЛТА, 27 VI 2023 r., https://www.belta.by/president/view/lukashenko-podtverdil-priezd-glavy-chvk-vagner-prigozhina-v-belarus-574036-2023/ [dostęp: 10 VII 2023].

Медведев считает, что заявления Польши подтверждают бессмысленность каких-либо переговоров, Tacc, 23 VI 2023 r., https://tass.ru/politika/18100221 [dostęp: 6 VII 2023].

Мишутин Г., Гасымов Н., *Чем для Украины закончился саммит НАТО в Вильнюсе*, Ведомости, 13 VI 2023 r., https://www.vedomosti.ru/politics/articles/2023/07/13/985067-mezhdunarodnie-novosti [dostęp: 18 VII 2023].

Оркестр Вагнера, wpis na kanale Telegram, https://t.me/s/orchestra_w [dostęp: 28 VII 2023].

Политолог назвала главное событие предстоящего саммита НАТО в Вильнюсе, Известия, 10 VII 2023 r., https://iz.ru/1542191/2023-07-10/politolog-nazvala-glavnoe--sobytie-predstoiashchego-sammita-nato-v-vilniuse [dostęp: 18 VII 2023].

Польские бизнесмены ответят за русофобию Варшавы, ВЗГЛЯД, 14 VII 2023 r., https://vz.ru/politics/2023/7/14/1221118.html [dostęp: 31 VII 2023].

Путин назвал последствия принятия Украины в НАТО, РИА Новости, 13 VII 2023 r., https://crimea.ria.ru/20230713/putin-nazval-posledstviya-prinyatiya-ukrainy-v-nato-1130043821.html [dostęp: 18 VII 2023].

Сакавик М., *Зачем Путин и Лукашенко угрожают Польше „вагнеровцами"?*, DW, 24 VII 2023 r., https://www.dw.com/ru/spektakl-putina-i-lukasenko-zacem-polse-ugrozaut-vagnerovcami/a-66332295 [dostęp: 26 VII 2023].

СМИ сообщили об изнасиловании несовершеннолетней наемниками из Польши, Известия, 10 II 2023 r., https://iz.ru/1468024/2023-02-10/smi-soobshchili-ob-iznasilovanii-nesovershennoletnei-naemnikami-iz-polshi [dostęp: 7 VII 2023].

Указ Президента Российской Федерации от 02.07.2021 г. № 400, Kremlin.ru, http://www.kremlin.ru/acts/bank/47046 [dostęp: 27 VI 2023].

Dr Karolina Kuśmirek

Doktor nauk o polityce, analityk. W badaniach naukowych koncentruje się na walce informacyjnej oraz działaniach służb specjalnych na świecie.

Kontakt: karolinakusmirek@gmail.com

Analiza krytyczna efektywności unijnych sankcji finansowych zastosowanych wobec Federacji Rosyjskiej

Critical analysis of the effectiveness of EU financial sanctions against the Russian Federation

ANGELA PACHOLCZAK

Autorka niezależna

https://orcid.org/0009-0000-4670-2364

Przegląd Bezpieczeństwa Wewnętrznego, 2024, nr 30: 97–129

https://doi.org/10.4467/20801335PBW.24.004.19606

ARTYKUŁ

Abstrakt

Artykuł jest poświęcony problematyce międzynarodowych sankcji finansowych w kontekście wyzwań, jakie stawia dla ich skuteczności rynek kryptowalutowy. Punktem odniesienia dla tej analizy są sankcje nałożone przez Radę Unii Europejskiej (wspierane zastosowaniem komplementarnych sankcji przez część społeczności międzynarodowej) na Federację Rosyjską w związku z jej agresją na Ukrainę. Celem artykułu jest ukazanie różnych płaszczyzn oceny skuteczności sankcji, a zwłaszcza wskazanie przyczyn, dla których w większości wypadków, pomimo osłabiania potencjału gospodarczego sankcjonowanego kraju, nie realizują one pierwotnego celu ich nałożenia, czyli powstrzymania działań militarnych. W tym przedmiocie osią zainteresowania jest aktualny oraz prospektywny wpływ rozwiązań finansowych opartych na technologii blockchain na tworzenie istotnej luki w systemie sankcyjnym, która pozwala eliminować lub marginalizować skutki międzynarodowych sankcji finansowych. To zagadnienie jest oceniane także przez pryzmat aktualnie wdrażanych unijnych regulacji rynku kryptowalut, w tym zastosowania do transakcji kryptowalutowych tzw. *travel rule*.

Słowa kluczowe

Federacja Rosyjska, finansowe sankcje międzynarodowe, kryptoaktywa, zdecentralizowane finanse, DeFi, cyfrowy pieniądz banku centralnego, CBDC, rozporządzenie MiCA

Abstract

The article focuses on the issue of international sanctions of a financial nature in the context of, in particular, the challenges to their effectiveness generated by the cryptocurrency market. An essential point of reference for this analysis is the current case of sanctions imposed by the Council of the European Union (supported by the application of complementary sanctions by part of the international community) on the Russian Federation in relation to that country's military aggression against Ukraine. The aim of this article is to show different perspectives on the assessment of the effectiveness of sanctions and, in particular, to identify the sources why, in a key number of cases, while weakening the economic potential of the sanctioned state, they nevertheless fail to achieve the original objective of their imposition, i.e. the deterrence of military action. In this subject, the axis of interest is the current and prospective impact of blockchain-based financial solutions on the creation of an important loophole in the sanctions regime to eliminate or marginalise the effects of international financial sanctions. The issue is also assessed through the prism of the crypto-asset market regulation entering into force in the European Union in the near future and the implementation of the so-called travel rule for cryptocurrency transactions.

Keywords

Russian Federation, financial international sanctions, crypto-assets, decentralised finance, DeFi, central bank digital currency, CBDC, MiCA regulation

Wojna jest tylko kontynuacją polityki innymi środkami.
Carl von Clausewitz, *O naturze wojny* (1832)

Zaangażowanie się w działania militarne przez społeczność międzynarodową w odpowiedzi na naruszenie prawa międzynarodowego przez jedno z państw trudno uznać za dobre rozwiązanie, gdy celem nadrzędnym jest uniknięcie eskalacji konfliktu zbrojnego. W związku z tym lepszym, a czasem jedynym wyborem dla społeczności międzynarodowej staje się zastosowanie sankcji, które są postrzegane jako liberalna alternatywa wobec wojny. Jednak w kontekście osiągnięcia głównego celu zastosowania sankcji, czyli powstrzymania agresji militarnej, bardziej stanowią one

sygnał[1], niż mają realny wpływ na stronę nimi objętą, zwłaszcza jej decydentów politycznych oraz środowiska powiązane z ośrodkami władzy.

Pojęcie sankcji wiąże się przede wszystkim z zastosowaniem narzędzi ekonomicznych bezpośrednio odnoszących się do sfery gospodarczej, które polega na zaprzestaniu lub groźbie zaprzestania istniejących relacji handlowych lub finansowych. Sankcje to coś więcej niż jedynie dyplomatyczna deklaracja, a ich rzeczywista skuteczność jest warunkowana wywołaniem drastycznego wpływu na gospodarkę sankcjonowanego kraju.

Należy podzielić pogląd, że skuteczna egzekucja sankcji finansowych jest zdecydowanie łatwiejsza niż egzekucja sankcji handlowych[2], co wynika z tego, że instytucje finansowe i państwa są istotnymi dostawcami lub gwarantami przepływów finansowych. Ponadto zdecydowanie większy nadzór istnieje nad rynkiem finansowym niż nad rynkiem handlu. Działalność finansowa zatem, przynajmniej w założeniu, powinna być łatwiejsza do monitorowania i ewentualnego identyfikowania naruszeń sankcji. Poza tym w badaniach potwierdzono większą skuteczność sankcji finansowych w porównaniu z sankcjami handlowymi[3]. Nie można bowiem pominąć, że w uwarunkowaniach gospodarczych działalność handlowa wymaga dostępu do zasobów finansowych. Tym samym sankcje finansowe mają komplementarny wpływ na przepływy handlowe, gdyż pozwalają na uniknięcie problemu egzekwowania sankcji w nie wymierzonych[4]. Jednak wbrew pozorom, podobnie jak innego rodzaju sankcje, również te finansowe mogą mieć niehumanitarny charakter i wyrządzać nieodwracalne szkody dla ludności cywilnej sankcjonowanego kraju, ale niekoniecznie muszą mieć bezpośredni wpływ na sytuację jego decydentów politycznych.

---

[1] Wynika to ze sposobu rozumienia podstaw normatywnych, zgodnie z którym przyjmuje się, że przez karanie i zawstydzanie jest możliwe kreowanie motywacji moralnych. Wiąże się to z pojmowaniem sankcji międzynarodowych jako negatywnej reakcji społeczności międzynarodowej wobec państwa, które narusza jej normy. Zob. R. Bierzanek, J. Symonides, *Prawo międzynarodowe publiczne*, Warszawa 2003, s. 24.

[2] G.C. Hufbauer i in., *Economic Sanctions Reconsidered: Supplemental case histories*, Washington 2007, s. 97–98.

[3] W badaniach Gary'ego C. Hufbauera, Jeffreya J. Schotta i Kimberly A. Elliott przeprowadzonych w 1985 r. (zaktualizowanych w 1990 r. i 2007 r.), w odniesieniu do kazusów zastosowania sankcji finansowych za sukces uznano 19 przypadków z 53 związanych ze stosowaniem wyłącznie tych sankcji (36%), w 32 przypadkach na 101 spraw obejmujących zastosowanie sankcji finansowo-handlowych (32%) oraz w 8 na 21 w sytuacji zamrożenia aktywów (38%). Dla odmiany w sytuacji zastosowania wyłącznie sankcji handlowych pozytywny rezultat odnotowano w 10 przypadkach na 40 weryfikowanych (25%). Zob. G.C. Hufbauer i in., *Economic Sanctions Reconsidered*…, s. 98.

[4] Tamże, s. 47–48, 97.

Pojawia się przy tym istotna wątpliwość dotycząca wpływu przemian na rynkach finansowych, w skali globalnej obserwowanych od ponad dekady (w tym innowacyjnych alternatyw dla tradycyjnych systemów bankowych oddziałujących w coraz większym stopniu na państwowe systemy monetarne i walutowe), na osłabienie skuteczności sankcji międzynarodowych. Można bowiem postawić pytanie nie tylko o obowiązywanie odpowiednich przepisów prawa, lecz także o możliwość wyrażenia w nich norm w pełni regulujących nowe rozwiązania stosowane na rynkach finansowych, co pośrednio zapewniałoby skuteczność egzekucji ustanawianych sankcji. Celem artykułu jest ukazanie złożoności tej problematyki w kontekście dostępu do nowych instrumentów finansowych i ich wykorzystania przez aparaty państwowe. Nie ograniczono się wyłącznie do badań metodą dogmatyczną nad tą problematyką, lecz z uwagi na postrzeganie prawa jako wielopłaszczyznowego zjawiska kulturowego[5], odniesiono się do wyników ekonomicznych i politologicznych badań naukowych nad skutecznością sankcji międzynarodowych, z uwzględnieniem przeglądu innowacyjnych instrumentów finansowych istotnych z punktu widzenia unijnych sankcji nałożonych na Federację Rosyjską (FR) w związku z jej agresją zbrojną na Ukrainę.

Nieskuteczność sankcji ekonomicznych

Z sankcjami wiąże się błędne przekonanie, że wymuszenie oczekiwanej normy zachowania zostanie wywołane przez samą obawę o wyniki gospodarcze ze strony objętego nimi państwa. Wbrew temu założeniu badania ekonomiczne przeprowadzone w 1990 r. przez Gary'ego C. Hufbauera, Jeffreya J. Schotta i Kimberly A. Elliott wykazały, że skuteczność sankcji gospodarczych była stosunkowo niska i wynosiła ok. 34%[6]. W wyniku analizy krytycznej tych badań w ujęciu politologicznym Robert A. Pape uznał, że ze wskazanych w nich 40 przypadków tylko pięć można byłoby uznać za rzeczywisty sukces zastosowania sankcji[7].

[5] Zob. K. Opałek, J. Wróblewski, *Zagadnienia teorii prawa*, Warszawa 1969; ciż sami, *Prawo. Metodologia, filozofia, teoria prawa*, Warszawa 1991.

[6] Badania z 1990 r. objęły 116 przypadków zastosowania sankcji. W 40 sprawach uznano, że ich zastosowanie przyniosło pozytywny efekt.

[7] Pape skorygował liczbę zbadanych przypadków – było ich 115, a nie 116. Uznał, że 5 spraw stanowi powtórzenie, podobnie wśród 40 przypadków zakwalifikowanych jako sukces zidentyfikował 1 powtórzenie, w 18 przypadkach rozstrzygnięcie w rzeczywistości wynikało z bezpośredniego lub pośredniego użycia siły, w 8 przypadkach sankcje nie przyniosły żadnego efektu, gdyż państwa nimi objęte nie poczyniły żadnych ustępstw, a 6 przypadków dotyczyło sporów handlowych, a nie stricte sankcji gospodarczych dla celów politycznych. W 3 przypadkach ewaluacja pod kątem

Na nieefektywność sankcji wpływa wiele czynników, przede wszystkim są to nieadekwatność i niewystarczalność zastosowanych środków. Ułatwia to uniknięcie sankcji lub przynajmniej zminimalizowanie ich negatywnych implikacji. W tym kontekście podstawowym warunkiem skuteczności jest jednomyślność społeczności międzynarodowej w sprawie nałożenia sankcji na dane państwo. Brak tej solidarności otwiera drogę do możliwości ograniczenia i neutralizacji skutków sankcji. Dla przykładu w zakresie wymiany handlowej otwiera to nowe kierunki importowe oraz zmianę rynków zbytu dla eksportu. Jednocześnie za pośrednictwem nowych destynacji handlowych staje się możliwy „przemyt" towarów objętych sankcjami do krajów formalnie je stosujących[8]. W odniesieniu natomiast do systemu finansowego jest możliwe jego zabezpieczenie przez tzw. zaszczepienie gospodarki (ang. *vaccinate the economy*) polegające na jej izolowaniu od wpływu sankcji przez zabezpieczenie remedium na te sankcje albo uzyskanie łatwego dostępu do alternatywnych rozwiązań[9].

Z sankcjami wiąże się także zjawisko nasilenia się postaw nacjonalistycznych w państwie, wobec którego są one stosowane. Zwraca na to uwagę Pape, który jednoznacznie wskazuje na nieskuteczność sankcji w sytuacji, gdy nie tylko aparat państwowy, lecz także obywatele są skłonni znosić dotkliwe ograniczenia w imię interesów narodowych. Takie tendencje charakteryzują zwłaszcza systemy autokratyczne, w których władza może zaakceptować wysokie koszty społeczne, jeżeli to umożliwia jej osiągnięcie własnych celów[10]. Tym samym ten fenomen zaprzecza twierdzeniom, że uderzenie w interesy ekonomiczne obywateli danego kraju musi wiązać się z opowiedzeniem się przez nich za zmianami politycznymi.

Aktualnie nieskuteczność sankcji finansowych wiąże się także ze wzrostem znaczenia w skali globalnej kryptoaktywów. Mogą one odgrywać istotną rolę w minimalizowaniu sankcji zarówno indywidualnych, jak i obejmujących system finansowy danego państwa.

---

skuteczności sankcji jest niemożliwa. Zob. R.A. Pape, *Why Economic Sanctions Do Not Work*, „International Security" 1997, t. 22, nr 2, s. 93, 99.

[8] Oczywiście wiąże się to mimo wszystko z negatywnymi konsekwencjami dla państwa objętego sankcjami w związku ze spadkiem cen eksportowanych surowców i towarów.

[9] A. Demarais, *Backfire: How Sanctions Reshape the World Against U.S. Interests*, New York 2022, s. 35–50.

[10] R.A. Pape, *Why Economic Sanctions*…, s. 106.

Kazus rosyjski

Z uwagi na działania wojenne przeciwko Ukrainie oraz nielegalne aneksje obwodów: donieckiego, ługańskiego, zaporoskiego i chersońskiego (2022 r.), a także z uwzględnieniem środków ograniczających nałożonych na FR w związku z aneksją Krymu (2014 r.), m.in. Unia Europejska (UE)[11] podjęła decyzję o objęciu tego kraju kolejnymi sankcjami. Były to środki ograniczające w postaci sankcji zarówno indywidualnych, jak i gospodarczych oraz wizowych. Według stanu na 5 marca 2024 r. Rada UE przyjęła 13 pakietów sankcji.

Koncentrując się wyłącznie na zagadnieniu bezpośredniego oddziaływania na rosyjski system finansowy, należy wskazać następujące sankcje unijne:

- zakaz finansowania rządu rosyjskiego i Centralnego Banku Federacji Rosyjskiej, CBFR (ros. Центральный банк Российской Федерации lub Банк России; ang. The Central Bank of Russian Federation lub Bank of Russia) oraz wszelkich transakcji związanych z zarządzaniem jego rezerwami i aktywami (zamrożenie rezerw walutowych), a także organami, podmiotami lub osobami działającymi w imieniu lub pod jego kierownictwem [np. Fundusz Dobrobytu Narodowego (Фонд национального благосостояния)];
- zakaz eksportu banknotów oraz sprzedaży zbywalnych papierów wartościowych[12] do Rosji denominowanych w euro oraz w pozostałych walutach urzędowych UE[13];
- zakaz inwestowania w projekty współfinansowane przez rosyjski Fundusz Inwestycji Bezpośrednich (Российский фонд прямых инвестиций), a także uczestniczenia w projektach lub dokonywania innego wkładu w te projekty[14];

[11] Poza sankcjami UE (oraz jej krajów członkowskich, które zachowały możliwość nakładania odrębnych, dodatkowych sankcji) na Rosję środki nałożyły także: USA, Wielka Brytania, Kanada, Szwajcaria, Japonia, Singapur, Korea Południowa, Australia, Nowa Zelandia oraz Tajwan. Zakres tych sankcji nie jest w wielu przypadkach jednorodny. Singapur np. zdecydował się wyłącznie na nałożenie ograniczonych sankcji finansowych oraz kontrolę eksportu w zakresie broni i przedmiotów służących ofensywnym operacjom cybernetycznym. Zob. *Sanctions and Restrictions Against Russia in Response to its Invasion of Ukraine*, Ministry of Foreign Affairs Singapore, 5 III 2022 r., https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/03/20220305-sanctions [dostęp: 5 III 2024].

[12] Z tym zakazem łączy się zakaz prowadzenia rachunków rosyjskich klientów przez unijne centralne depozyty papierów wartościowych.

[13] Wyjątki obejmują środki niezbędne do osobistego użytku podróżujących do Rosji lub oficjalnych celów misji dyplomatycznych, konsularnych, organizacji międzynarodowych.

[14] W tym zakresie przewidziano ściśle określone odstępstwa dotyczące umów zawartych przed 2 marca 2022 r.

– zakaz przeprowadzania wszelkich transakcji z niektórymi rosyjskimi przedsiębiorstwami państwowymi z różnych sektorów, tworzących militarno-przemysłowy kompleks Kremla[15], a także zakaz zajmowania stanowisk w organach zarządzających tych przedsiębiorstw;
– zakaz dopuszczenia do obrotu giełdowego akcji rosyjskich podmiotów państwowych w unijnych systemach obrotu i świadczenia związanych z nimi usług;
– zakaz bezpośredniego lub pośredniego kupna, sprzedaży lub świadczenia usług inwestycyjnych lub pomocy w emisji i innych czynności w odniesieniu do zbywalnych papierów wartościowych i instrumentów rynku pieniężnego w odniesieniu do m.in. rządu Rosji i CBFR, osób prawnych, podmiotów oraz organów działających w ich imieniu, a także podmiotów wskazanych w załącznikach V i VI *Rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie* (dalej: rozporządzenie 833/2014);
– zakaz świadczenia bezpośrednio lub pośrednio usług dla biznesu, takich jak usługi w zakresie: rachunkowości, audytu, badania ustawowego, prowadzenia ksiąg rachunkowych i doradztwa podatkowego, doradztwa informatycznego, doradztwa prawnego, architektury i inżynierii, doradztwa w zakresie zarządzania, public relations, badań rynku i opinii publicznej, badań i analiz technicznych, reklamy i usług ratingowych;
– zakaz świadczenia na rzecz kluczowych rosyjskich banków specjalistycznych usług w zakresie komunikatów finansowych, wykorzystywanych do wymiany danych finansowych w ramach Society for Worldwide Interbank Financial Telecommunication (SWIFT)[16];
– zakaz udzielania finansowania publicznego lub pomocy finansowej na rzecz handlu ze stroną rosyjską lub inwestycji na terenie FR[17];

---

[15] Kompletna lista wyżej wymienionych podmiotów została określona w wykazie z załącznika XIX *Rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie*.

[16] Sankcje w ramach trzeciego pakietu z 2 marca 2022 r. objęły siedem rosyjskich banków, tj. Банк Открытие (Bank Otkrytije), Новикомбанк (Nowikombank), Промсвязьбанк (Promswiaz'bank), Банк „Россия" (Bank „Rossiya"), Совкомбанк (Sowkombank), Vnesheconombank (VEB, VEB.RF) i Банк ВТБ (WTB Bank), a także wszystkie osoby prawne, podmioty lub organy z siedzibą w Rosji, w których ponad 50% praw własności należy bezpośrednio lub pośrednio do ww. instytucji. Następnie w ramach szóstego pakietu z 3 czerwca 2022 r. wyłączenie ze SWIFT rozszerzono na Сбербанк России (Sbierbank Rossii), Московский кредитный банк (Moskowskij krieditnyj bank) i Российский сельскохозяйственный банк (Россельхозбанк) – (Rossijskij sielskochoziajstwiennyj bank, Rossielchozbank).

[17] Wyjątkami są: zastrzeżenie możliwości sfinalizowania kontraktów zawartych przed 26 lutego 2022 r. oraz szczególne przypadki dotyczące handlu produktami spożywczymi, środkami do celów

- zakaz udziału rosyjskich wykonawców w zamówieniach publicznych i koncesjach udzielanych w państwach członkowskich UE;
- zakaz prowadzenia rachunków rosyjskich klientów przez unijne centralne depozyty papierów wartościowych oraz sprzedaży im papierów wartościowych denominowanych w euro;
- zakaz przyjmowania depozytów od obywateli lub rosyjskich rezydentów, osób prawnych, podmiotów lub organów mających siedzibę na terenie Rosji lub osób prawnych, podmiotów lub organów mających siedzibę poza UE, w przypadku których ponad 50% praw własności należy bezpośrednio lub pośrednio do obywateli rosyjskich lub osób fizycznych zamieszkałych na terenie Rosji, jeżeli łączna wartość ich depozytów na instytucję kredytową przekracza kwotę 100 000 euro;
- zakaz świadczenia usług doradztwa w zakresie planowania finansowego i trustów oraz przyjmowania dużych depozytów przez banki z UE;
- zakaz świadczenia usług kryptograficznych pierwotnie o wysokiej wartości (tj. 10 000 euro), a następnie niezależnie od wartości.

Jednocześnie po wprowadzeniu trzynastego pakietu sankcji skierowanych przeciwko Rosji łącznie wobec 2177 osób i podmiotów[18] przyjęto sankcje indywidualne polegające m.in. na zamrożeniu aktywów oraz wprowadzeniu zakazu udostępniania funduszy lub zasobów gospodarczych. Ustanowiono także nowe sankcje wobec Białorusi (z uwagi na działania podważające integralność terytorialną, suwerenność i niezależność Ukrainy) oraz Iranu (w związku z udzielonym wsparciem wojskowym w postaci dostaw bezzałogowych statków powietrznych). W przypadku sankcji indywidualnych nałożonych na Białoruś zostały one zastosowane wobec 271 osób i podmiotów[19], na Iran – wobec 280 osób i podmiotów[20].

rolniczych, medycznych lub humanitarnych, a także dotyczące programów unijnych dla małych i średnich przedsiębiorstw – do określonej kwoty.

[18] Zgodnie z załącznikiem I *Rozporządzenia Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających* – przy czym według stanu na 5 marca 2024 r. 36 osób i podmiotów zostało skreślonych z listy, zatem 2141 osób i podmiotów pozostaje objętych sankcjami.

[19] Zgodnie z załącznikiem I *Rozporządzenia Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy*, przy czym według stanu na 5 marca 2024 r. 1 podmiot został skreślony z listy, zatem 270 osób i podmiotów pozostaje objętych sankcjami.

[20] Zgodnie z załącznikiem I *Rozporządzenia Rady (UE) nr 359/2011 z dnia 12 kwietnia 2011 r. dotyczącego środków ograniczających skierowanych przeciwko niektórym osobom, podmiotom i organom w związku z sytuacją w Iranie* – przy czym według stanu na 5 marca 2024 r. 8 osób zostało skreślonych z listy, zatem 272 osoby i podmioty pozostają objęte sankcjami.

Egzekucja sankcji nakładanych przez Radę UE ciąży na państwach członkowskich, które są odpowiedzialne za ich wdrożenie. W tym zakresie wsparcia udziela im Komisja Europejska (KE), odpowiadająca za jednolitość tych działań i ich koordynację międzynarodową[21].

Sankcje unijne wymierzone w Rosję i Białoruś są uzupełniane w Polsce przez sankcje krajowe. W tym zakresie najważniejszy akt prawny to *Ustawa z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego*, statuująca m.in. ustanowienie dodatkowej krajowej listy sankcyjnej prowadzonej przez ministra właściwego do spraw wewnętrznych[22].

Zgodnie z przepisami tej ustawy karze pieniężnej, nakładanej przez Szefa Krajowej Administracji Skarbowej w drodze decyzji administracyjnej, w wysokości do 20 mln zł[23] podlegają osoba lub podmiot, które w stosunku do osoby lub podmiotu wpisanego na listę nie dopełniają: obowiązku zamrożenia środków finansowych, funduszy lub zasobów gospodarczych lub zakazu udostępniania środków finansowych, funduszy lub zasobów gospodarczych, określonego w art. 2 ust. 1 lub 2 *Rozporządzenia Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy* (dalej: rozporządzenie 765/2006) lub art. 2 *Rozporządzenia Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających* (dalej: rozporządzenie 269/2014), albo obowiązku niezwłocznego przekazywania informacji, wymaganych na podstawie art. 4 ust. 2 lub art. 5 rozporządzenia 765/2006 lub na podstawie art. 7 ust. 1 lub art. 8 rozporządzenia 269/2014; bądź nie stosują się do zakazu świadomego i celowego udziału w działaniach, których celem lub skutkiem jest ominięcie stosowania środków określonych w art. 2 ust. 1 lub 2 rozporządzenia 765/2006 lub art. 2 rozporządzenia 269/2014.

---

[21] W tym celu KE powołała grupę zadaniową Freeze and Seize, której zadaniem jest koordynowanie na szczeblu UE wdrożenia indywidualnych sankcji wobec osób fizycznych. Grupa ta odpowiada również za współpracę w ramach grupy zadaniowej REPO (Russian Elites, Proxies, and Oligarchs), zarządzającej współpracą UE z krajami G7 (Group of Seven) oraz Australią.

[22] Lista jest niezależna od wykazów osób i podmiotów określonych w rozporządzeniach 765/2006 i 269/2014, gdyż zakres środków stosowanych wobec osób i podmiotów wpisanych na nią nie może powielać zakresu środków określonych względem nich w tych rozporządzeniach (art. 2 ust. 2 ustawy). Według stanu aktualizacji listy na dzień 29 lutego 2024 r. przez MSWiA obejmowała ona 427 osób fizycznych oraz 82 podmioty. Jednocześnie z listy w latach 2022–2023 wykreślono 1 osobę fizyczną i 8 podmiotów. W efekcie wskazanego dnia sankcjami pozostawało objętych 426 osób fizycznych i 74 podmioty.

[23] Artykuł 6 *Ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego*.

Należy zgodzić się z Pape'em, że pomimo kompleksowości sankcji ich nałożenie na FR okazało się niepowodzeniem. Bez wątpienia są one dotkliwe dla gospodarki[24], jednak w rzeczywistości nie zmuszają Rosji do zaprzestania prowadzonej „operacji wojskowej"[25]. Przykład tego kraju pokazuje pełen zakres ograniczeń co do skuteczności systemu sankcji międzynarodowych.

Głównym czynnikiem determinującym niewielką skuteczność zastosowanych sankcji był – jak wspomniano wyżej – brak jednomyślności społeczności międzynarodowej w tym przedmiocie, a zwłaszcza postawa Chin, Indii, Iranu oraz państw dawnych republik radzieckich Azji Środkowej i Kaukazu czy Turcji, które negatywnie odniosły się do wprowadzenia sankcji. Przewidzenie przez Rosję braku jednomyślności społeczności międzynarodowej pozwoliło na zaszczepienie jej gospodarki oraz znalezienie alternatyw pozwalających na zmniejszenie dotkliwości sankcji, czego przykładem może być odnotowywany w latach poprzedzających agresję na Ukrainę wzrost wysokości utrzymywanych rezerw walutowych i w złocie[26]. Pomimo zamrożenia w wyniku zastosowania sankcji części rosyjskich rezerw walutowych ich kluczowe zasoby zostały zachowane wskutek utrzymywania przez CBFR największego poziomu rezerw w złocie (tzw. złoto monetarne) zdeponowanym w skarbcach na terytorium FR (21,7%), a także ulokowania ok. 13,8% wszystkich rezerw w Chinach. Ważne jest również to, że rezerwy walutowe nie obejmowały wyłącznie euro i dolara, lecz były sukcesywnie lokowane przede wszystkim w renminbi (yuan), a także np. w jenach i rupiach[27]. Polityka CBFR pozwoliła w nowych uwarunkowaniach na zachowanie środków niezbędnych dla podejmowania interwencji na rynku walutowym i dłużnym. Również utrata dostępu do SWIFT nie okazała się, jak przewidywano, „finansową bronią nuklearną"[28]. Pomimo zastosowania tej drastycznej sankcji banki

[24] Potwierdzeniem tego jest m.in. odnotowany spadek rosyjskiego produktu krajowego brutto (PKB). Zgodnie z analizami Banku Światowego, Międzynarodowego Funduszu Walutowego i Organizacji Współpracy Gospodarczej i Rozwoju w 2022 r. rosyjski PKB obniżył się o 2,1%, przy wzroście na poziomie 3% prognozowanym przed inwazją przez Federalną Służbę Statystyki Państwowej, Rosstat (Федеральная служба государственной статистики, Росстат). Zob. *Wpływ sankcji na rosyjską gospodarkę*, Rada UE, https://www.consilium.europa.eu/pl/infographics/impact-sanctions-russian-economy/ [dostęp: 5 III 2024].

[25] R.A. Pape, wpis na portalu LinkedIn, https://www.linkedin.com/posts/robert-pape_someone-asked-my-view-on-how-sanctions-are-activity-6970475273985171456-6ora [dostęp: 5 III 2024].

[26] *Annual value of international reserves of Russia from 2012 to 2022, by type*, Statista, https://www.statista.com/statistics/1049298/russia-international-reserves-value-by-type/ [dostęp: 5 III 2024].

[27] *Bank of Russia foreign exchange and gold asset management report*, Bank of Russia, Moscow 2022, https://www.cbr.ru/Collection/Collection/File/39685/2022-01_res_en.pdf [dostęp: 5 III 2024].

[28] Francuski minister finansów Bruno Le Maire po spotkaniu ministrów finansów UE w dniu 25 lutego 2022 r. wyraził opinię, że wyłączenie FR z międzynarodowego systemu płatności SWIFT

rosyjskie nadal mogą funkcjonować i pozyskiwać zasoby gotówkowe umożliwiające prowadzenie działalności i interakcje z rynkami zewnętrznymi. Wynika to z dostępności różnych alternatywnych rozwiązań, które pozwalają ominąć sankcje. Wskutek obaw o wykluczenie ze SWIFT rosyjskiego sektora bankowego CBFR już podczas aneksji Krymu w 2014 r. rozpoczął testowanie systemu transmisji komunikatów finansowych – SPFS (Система передачи финансовых сообщений). Według oświadczenia CBFR już w lipcu 2023 r. system ten przetwarzał 70% krajowych transakcji finansowych[29]. Nie jest on jednak przeznaczony wyłącznie do rozliczeń krajowych. Według informacji ze stycznia 2024 r. korzysta z niego 557 podmiotów, w tym 157 podmiotów zagranicznych z 20 państw[30]. Opcją obejścia sankcji jest również posłużenie się transgranicznym międzybankowym systemem płatniczym – CIPS (Chinese Cross-Border Interbank Payment System), a także jego ewentualna integracja z SPFS, zwłaszcza w odniesieniu do chińsko-rosyjskich rozliczeń transgranicznych.

Pomimo negatywnego wpływu na gospodarkę i uwarunkowania społeczne sankcje również nie wywołały istotnych przemian politycznych, a wręcz przeciwnie – uwolniły duży potencjał adaptacyjny, który ułatwił ustabilizowanie się sytuacji gospodarczej. Prognozuje się, że w perspektywie czasu, wskutek zwiększania kontroli gospodarki i ugruntowania modelu kapitalizmu państwowego, może to również przyczynić się do dalszego wzmocnienia pozycji władz[31].

powinno być traktowane jako rozwiązanie ostateczne. Stwierdził, że „SWIFT jest finansową bronią nuklearną. (…) Faktem pozostaje, że mając w rękach broń nuklearną, myśli się, zanim jej użyje. Niektóre kraje członkowskie wyraziły zastrzeżenia, bierzemy je pod uwagę". Tłumaczenia w tekście pochodzą od autorki (dop. red.). Zob. G. Leali, *France not opposed in principle to cutting Russia from SWIFT: Bruno Le Maire*, Politico, 25 II 2022 r., https://www.politico.eu/article/Frances-le-maire-not-againstcutting-russia-out-of-swift/ [dostęp: 5 III 2024]. Należy podkreślić, że tę sankcję uważano za najbardziej drastyczną, co w czasie rosyjskiej inwazji na Krym w 2014 r. skutkowało odrzuceniem apeli o wykluczenie już wówczas FR ze SWIFT, gdyż uznano ten krok za nadmierną eskalację konfliktu.

[29] *В ЦБ сообщили о 70% внутрироссийского трафика у национального аналога SWIFT*, Известия, 3 VII 2023 r., https://iz.ru/1538263/2023-07-03/v-tcb-soobshchili-o-70-vnutrirossiiskogo-trafika-u-natcional nogoanaloga-swift [dostęp: 5 III 2024].

[30] *Российский аналог SWIFT распространяется на Восток*, News.Ru, 27 I 2024 r., https://news.ru/economics/rossijskij-analog-swift-rasshiryaet-svoe-vliyanie [dostęp: 5 III 2024].

[31] I. Wiśniewska, *Rosyjska gospodarka w roku 2022. Adaptacja i rosnący deficyt budżetu*, OSW, 16 II 2023 r., https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2023-02-16/rosyjska-gospodarka-w-roku-2022-adaptacja-i-rosnacy-deficyt [dostęp: 5 III 2024].

Kryptoaktywa jako przedmiot sankcji nałożonych na Federację Rosyjską

W lutym 2022 r. Bloomberg, powołując się na szacunki rosyjskiego rządu[32], podał, że obywatele rosyjscy posiadają aktywa kryptograficzne o wartości 16,5 bln rubli (214 mld dolarów), co stanowiło 12% całkowitej wartości tych aktywów na świecie. Szacowano, że tego rodzaju aktywa posiadało ponad 17 mln Rosjan[33]. Według ocen Cambridge Centre for Alternative Finance (CCAF) z przełomu 2021 i 2022 r. Rosja była także jednym z pięciu największych ośrodków wydobywczych bitcoina – zapewniała 4,66% jego światowej produkcji[34]. Potwierdzeniem obaw, że kryptoaktywa mogą być istotną luką w systemie sankcji finansowych wymierzonych w Rosję i sposobem na ograniczenie ich skutków, były odnotowane wzrosty wolumenu obrotów między rublem a najważniejszymi kryptowalutami[35]. W odpowiedzi na to zagrożenie w tzw. *Compliance package* z 9 marca 2022 r. odnoszącym się do Białorusi doprecyzowano, że w rozporządzeniu 269/2014 niewyczerpująca definicja funduszy obejmuje także kryptowaluty, a definicja zasobów gospodarczych może dotyczyć również niektórych kryptoaktywów. W związku z tym kryptoaktywa miały podlegać przepisom dotyczącym zamrożenia aktywów oraz zakazowi udostępniania funduszy lub zasobów gospodarczych osobom umieszczonym na listach sankcyjnych. Uznano także, że w rozumieniu rozporządzenia 833/2014 zbywalne papiery wartościowe obejmują kryptoaktywa z wyjątkiem instrumentów płatniczych. Ponadto podkreślono, że kryptoaktywów nie należy wykorzystywać do obchodzenia jakichkolwiek sankcji unijnych[36].

Najważniejsze ograniczenia w tym obszarze wprowadzono jednak dopiero w ramach piątego pakietu sankcji z 8 kwietnia 2022 r. Podjęto wówczas decyzję

---

[32] Oszacowanie zostało przeprowadzone na podstawie m.in. analizy adresów IP największych użytkowników giełd kryptowalutowych.

[33] E. Pismennaya, *Russia Values Local Crypto at $200 Billion as Rules Near*, Bloomberg, 1 II 2022 r., https://www.bloomberg.com/news/articles/2022-02-01/russia-values-local-crypto-market-at-200-billion-as-rules-near#xj4y7vzkg [dostęp: 5 III 2024].

[34] *Bitcoin Mining Map*, CCAF, https://ccaf.io/cbnsi/cbeci/mining_map [dostęp: 5 III 2024].

[35] Po wprowadzeniu sankcji w lutym 2022 r. wzrost obrotów zaobserwowano zwłaszcza na transakcjach zakupu tethera i bitcoina, co było uwarunkowane przede wszystkim początkowym drastycznym spadkiem wartości rubla. Zob. T. Wilson, *Rouble-crypto trading soars as sanctions hit Russian currency*, Reuters, 28 II 2022 r., https://www.reuters.com/markets/europe/rouble-crypto-trading-soars-sanctions-hit-russian-currency-2022-02-28/ [dostęp: 5 III 2024].

[36] Komunikat prasowy Komisji Europejskiej: *Ukraine: EU agrees to extend the scope of sanctions on Russia and Belarus*, 9 III 2022 r., https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1649 [dostęp: 5 III 2024]; *Crypto-assets. Relevant provision: Article 5b(2) of Council Regulation (EU) No 833/2014. Frequently asked question*s, UE, 21 III 2023 r., https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [dostęp: 5 III 2024].

o zakazie świadczenia usług, których przedmiotem jest udostępnianie portfeli służących do przechowywania kryptoaktywów, prowadzenia rachunków lub przechowywania kryptoaktywów, na rzecz obywateli rosyjskich lub osób fizycznych zamieszkałych na terenie Rosji lub osób prawnych, podmiotów lub organów z siedzibą w tym kraju, jeżeli całkowita wartość kryptoaktywów osoby fizycznej lub prawnej, podmiotu lub organu na dostawcę portfela lub rachunku lub na podmiot przechowujący kryptoaktywa przekracza 10 000 euro[37]. Ta sankcja została zaostrzona w ósmym pakiecie z 5 października 2022 r. przez przyjęcie całkowitego zakazu świadczenia tego rodzaju usług na rzecz ww. osób i podmiotów, niezależnie od wartości kwoty portfela[38].

Kryptoaktywa jako źródło luki w systemie międzynarodowych sankcji finansowych

Część komentatorów[39] nie przypisywała dużego znaczenia możliwości wytworzenia się luki w systemie sankcji finansowych. Wskazywano przede wszystkim na ograniczenie płynności rynku kryptowalut, który nie mógłby zaspokoić skali rosyjskich potrzeb. Stąd uznawano, że FR nie byłaby w stanie w takim samym wymiarze powielić strategii Iranu, który w obliczu sankcji zalegalizował płatności kryptowalutowe w imporcie. Należy jednak zauważyć, że w sytuacji zaostrzania zachodnich sankcji strona rosyjska rozważała sformalizowanie możliwości użycia kryptowalut w rozliczeniach transgranicznych[40].

---

[37] Artykuł 1 pkt 18 *Rozporządzenia Rady (UE) 2022/576 z dnia 8 kwietnia 2022 r. w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie*.

[38] Artykuł 1 pkt 10 *Rozporządzenia Rady (UE) 2022/1904 z dnia 6 października 2022 r. w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie*.

[39] Zob. *Cryptocurrencies: a way to evade sanctions?*, BAFFI – Centre on Economics, Finance and Regulation, https://baffi.unibocconi.eu/research-units/mints-alternative-monies/newsletter/issue-0/cryptocurrencies-way-evade-sanctions [dostęp: 5 III 2024].

[40] Głównym przeciwnikiem wdrożenia takiego rozwiązania jest CBFR, który podchodzi sceptycznie do rynku kryptowalut. Instytucja ta miała również największy wpływ na treść ustawy federalnej nr 331-FZ „W sprawie zmiany niektórych aktów ustawodawczych Federacji Rosyjskiej oraz w sprawie zawieszenia niektórych przepisów art. 5 ust. 1 ustawy federalnej «O bankach i działalności bankowej»", nowelizującej ustawę federalną nr 259-FZ „W sprawie cyfrowych aktywów finansowych, waluty cyfrowej oraz zmian w niektórych aktach prawnych Federacji Rosyjskiej", przez dodanie w jej art. 4 ust. 10 o treści: „Zabrania się przyjmowania cyfrowych aktywów finansowych jako środka płatniczego lub innego wynagrodzenia za przekazane dobra, wykonaną pracę, świadczone usługi, a także w jakikolwiek inny sposób umożliwiający zapłatę za towary (pracę, usługę) cyfrowym aktywem finansowym,

Podkreślano także błąd postrzegania decentralizacji jako gwarancji zachowania pełnej anonimowości użytkowników[41]. Technologia blockchain jest publiczną księgą aktywności, umożliwiającą monitorowanie przepływów środków pomiędzy portfelami. Ten argument był odrzucany wobec wskazania, że identyfikacja na blockchainie następuje na podstawie adresów kluczy publicznych, a nie rzeczywistej tożsamości, co potencjalnie może umożliwić uniknięcie sankcji w sytuacji posłużenia się nieprawdziwą tożsamością. Sceptycy uznawali takie zagrożenie za marginalne wobec faktu, że większość obrotów kryptowalutowych odbywa się z udziałem pośredników, takich jak kantory i giełdy kryptowalutowe czy dostawcy portfeli kryptowalutowych. Z uwagi na te czynniki w większości jurysdykcji ten obrót podlega regulacjom przeciwdziałającym praniu pieniędzy oraz finansowaniu terroryzmu. Duża część giełd kryptowalutowych wdraża także zasady Know Your Customer, KYC (pol. poznaj swojego klienta)[42].

Dla przykładu w polskiej *Ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu*, w związku z wprowadzeniem do niej definicji legalnej pojęcia waluty wirtualnej (art. 2 ust. 2 pkt 26), rozszerzono katalog instytucji obowiązanych o podmioty, które prowadzą działalność gospodarczą polegającą na świadczeniu usług w zakresie: wymiany między walutami wirtualnymi i środkami płatniczymi, wymiany między samymi walutami wirtualnymi, pośrednictwa w ich wymianie, a także prowadzenia ich rachunków (tzw. portfeli)[43].

---

z wyjątkiem przypadków przewidzianych w ustawach federalnych". Jednak wobec artykułowania przez rosyjskie Ministerstwo Finansów oczekiwania co do możliwości wykorzystania kryptowalut jako środka rozliczeń transgranicznych, CBFR promuje w tym zakresie wykorzystanie cyfrowego rubla. Zob. *ЦБ предложил дать зарубежным банкам доступ к цифровому рублю с 2025 года*, RBC.ru, 10 X 2023 r., https://www.rbc.ru/finances/10/10/2023/6523e87b9a7947b24f71b430 [dostęp: 5 III 2024].

41 Zob. C.S. Wright, *Bitcoin Is Anything BUT Anonymous*, Bitcoin & Blockchain Tech, 1 IX 2019 r., https://craigwright.net/blog/bitcoin-blockchain-tech/bitcoin-is-anything-but-anonymous/ [dostęp: 5 III 2024]. Należy odróżnić koncepcję anonimowości od prywatności i poufności. Całkowita anonimowość może być elementem niepotrzebnym i w większości przypadków niepożądanym, jest natomiast możliwe zachowanie prywatności i poufności przy akceptacji wymogu udowodnienia swojej tożsamości. Tym samym prywatność ukrywa szczegóły transakcji przed szeroko rozumianą opinią publiczną, ale nie przed osobami, które brały udział w wymianie, a także nie przed tymi, których prawo upoważnia do monitorowania wymian.

42 KYC to obowiązkowy proces identyfikacji i weryfikacji przez instytucje finansowe tożsamości klienta przy otwieraniu przez niego rachunku, a następnie cykliczne poddawanie tego klienta ponownej ewaluacji.

43 W art. 2 ust. 1 pkt 12 ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu uznano ww. podmioty za instytucje obowiązane, które m.in. są zobligowane do stosowania środków bezpieczeństwa w przypadku transakcji okazjonalnej z wykorzystaniem waluty wirtualnej o równowartości 1000 euro lub większej (art. 35 ust. 1 pkt 2 lit. c ww. ustawy). Jednocześnie sama działalność w zakresie

W efekcie podmioty świadczące tego rodzaju usługi pozostają zobowiązane do realizacji zadań AML/CFT[44].

Niemniej kryptoaktywa, jak wspomniano, mogą zapewnić rozwiązania pozwalające na uniknięcie sankcji finansowych, zwłaszcza indywidualnych. Są to np.:

- *chain-hopping* (pol. przeskakiwanie łańcuchów) – polegające na szybkiej zmianie zasobów kryptograficznych w celu dokonania zmiany blockchaina utrudniającej śledzenie przepływu środków[45],
- *mixers*, *tumblers*, *foggers* – usługi polegające na mieszaniu potencjalnie identyfikowalnych lub skażonych funduszy kryptowalutowych z innymi, w celu uniemożliwienia ustalenia ich rzeczywistego źródła pochodzenia,
- portfele niehostowane – umożliwiające przenoszenie środków bez podlegania monitoringowi giełd kryptowalutowych, w przeciwieństwie do udostępnianych przez nie portfeli hostowanych; wymagają one jednak ujawnienia w przypadku chęci wymiany kryptowaluty na walutę fiducjarną. Niemniej jest możliwe wówczas skorzystanie z giełd w jurysdykcjach o niskich wymogach AML/CFT lub KYC,
- kryptowaluty nastawione na prywatność, tzw. monety prywatności (ang. *privacy token* lub *private coin*) – ich zastosowanie jest bliskie realizacji idei anonimowych transakcji, pomimo bowiem uwidocznienia samej transakcji w księdze publicznej (blockchain) adresy portfeli stron transakcji pozostają niewidoczne. Przykładem może być kryptowaluta monero, wykorzystująca w transakcjach ukryte adresy w celu ochrony prywatności odbiorcy[46], dla ochrony nadawcy natomiast stosująca tzw. podpisy pierścieniowe, które polegają na łączeniu klucza konta użytkownika z kluczami publicznymi z blockchaina,

walut wirtualnych jest działalnością regulowaną w rozumieniu przepisów *Ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców* i może być wykonywana po uzyskaniu wpisu do rejestru działalności w zakresie walut wirtualnych dokonywanego przez ministra do spraw finansów publicznych. Jednocześnie jest konieczne spełnienie wymogów niekaralności i posiadania odpowiedniej wiedzy lub doświadczenia przy wykonywaniu tego rodzaju działalności (art. 129m–129w ustawy).

[44] AML/CFT (ang. *Anti Money Laundering/Counter Financing of Terrorism*) – zbiorcze określenie przepisów i zasad, których stosowanie jest wymagane od podmiotów świadczących usługi finansowe w celu zapobiegania praniu pieniędzy i finansowaniu terroryzmu.

[45] Tę technikę skutecznie wykorzystywała m.in. północnokoreańska grupa Lazarus w celu ukrycia ścieżki transferów środków skradzionych giełdom kryptowalutowym.

[46] W celu uniknięcia zapisu adresu portfela odbiorcy na blockchainie jest używany system Stealth Address, w którym każdą transakcję wysyła się do unikalnego, jednorazowego adresu. Odbiorca ma dostęp do środków przesłanych na ukryty adres, bez ujawniania połączeń do prawdziwego publicznego portfela i historii transakcji.

– zdecentralizowane finanse (ang. *decentralized finance*, DeFi) – oparte na wymianie *peer-to-peer* (P2P)[47].

Pomimo istotnego znaczenia jednostek analityki finansowej (Financial Intelligence Units)[48] w odniesieniu do kryptowalut kluczowa rola egzekucji sankcji finansowych przypada komercyjnym instytucjom finansowym. Te, podlegając ścisłym regulacjom nadzorczym ze strony państw, są zmuszone śledzić źródła przepływu pieniędzy i weryfikować, czy strony transakcji nie figurują na listach sankcyjnych. W sytuacji objęcia danego podmiotu sankcjami finansowymi staje się konieczne poszukiwanie przez niego alternatywnych rozwiązań w celu zachowania możliwości przepływu kapitału. Właśnie w tym obszarze tkwi potencjał kryptoaktywów jako instrumentu obchodzenia sankcji. Istnienie zasobów cyfrowych w przestrzeni wirtualnej ma tę zasadniczą zaletę, że transakcje finansowe mogą następować z pominięciem monitorowanych rynków, globalnych sieci płatniczych czy ściśle regulowanych systemów finansowych.

W momencie wprowadzania sankcji unijnych rynek tokenów płatniczych (bitcoin, altcoin i stablecoin) oraz tokenów inwestycyjnych i użytkowych pozostawał w praktyce poza regulacjami oraz nadzorem UE i jej krajów członkowskich.

Zgodnie z polskimi regulacjami rynek kryptoaktywów nie jest identyfikowany jako segment rynku finansowego w rozumieniu przepisów *Ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym*. Tym samym Komisja Nadzoru Finansowego sprawuje nadzór wyłącznie nad działalnością giełd i kantorów wymiany walut wirtualnych związany ze świadczeniem przez te podmioty usług płatniczych na podstawie przepisów *Ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych*.

Wymiana kryptowalut odbywa się przez szyfrowane przelewy pomiędzy portfelami za pomocą dwukluczowego mechanizmu: przelewy wymagają klucza publicznego, czyli adresu portfela, oraz klucza prywatnego, który pełni funkcję hasła. Oba klucze to kody alfanumeryczne. Jak wcześniej wspomniano, portfele mogą mieć charakter kustodialny (powierniczy, hostowany), co wiąże się z powierzeniem przez inwestora stronie trzeciej zarządzania i ochrony swoimi kluczami do portfela. To skutkuje przejęciem przez powiernika odpowiedzialności za własność inwestora. Na przeciwległym biegunie są tzw. portfele niekustodialne (niepowiernicze, niehostowane). Między tymi rodzajami portfeli istnieją istotne różnice. Przede wszystkim właściciele portfeli depozytowych powierzają swoje klucze prywatne dostawcom usług w zakresie

[47] Na taki katalog ewentualnych rozwiązań wskazano m.in. w dokumencie K.E. Busch, P. Tierno, *Russian Sanctions and Cryptocurrency*, Congressional Research Service, 4 V 2022 r., https://crsreports.congress.gov/product/pdf/IN/IN11920 [dostęp: 5 III 2024].

[48] W Polsce głównym elementem systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu jest Generalny Inspektor Informacji Finansowej, który realizuje swoje zadania przez Departament Informacji Finansowej wyodrębniony w strukturze Ministerstwa Finansów.

kryptoaktywów (ang. *crypto-asset service providers*, CASPs), podczas gdy zarówno klucze prywatne, jak i publiczne portfeli niepowierniczych pozostają w wyłącznej dyspozycji ich właścicieli, którzy dokonują transferów za pośrednictwem transakcji P2P. Dostawcy usług, będący platformą pośredniczącą, w celu dokonania identyfikacji klienta będą wymagać ujawnienia informacji co najmniej w zakresie danych dotyczących rachunku bankowego lub karty kredytowej. Portfele niepowiernicze natomiast nie wymagają zaufanego pośrednika w postaci zewnętrznej instytucji, która gwarantowałaby bezpieczeństwo transakcji. Drugą istotną różnicą jest to, że transakcji pomiędzy portfelami depozytowymi nie przechowuje się na blockchainie do czasu wycofania środków od CASP, podczas gdy transakcje P2P są natychmiast rejestrowane.

CASPs w porównaniu z sektorem bankowym mają zdecydowanie mniejsze instrumenty egzekwowania prawa w zakresie identyfikacji klientów, mimo że formalnie obowiązują je takie same wymogi AML/CFT, jakie dotyczą instytucji finansowych. Wiąże się to z trudnościami w przypadku portfeli niepowierniczych, ponieważ jedynie niektóre dane na temat transakcji na blockchainie są rejestrowane przez transfery P2P. W efekcie ustalenie własności takich portfeli wymagałoby połączenia szczegółów transakcji z adresami IP jej stron[49].

Tę sytuację zmieni, przynajmniej częściowo, wejście w życie przepisów *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937* (tzw. rozporządzenie MiCA). Ustanowiono w nim ramy prawne dla dostawców usług zarówno w zakresie kryptoaktywów, jak i ochrony konsumentów. Regulacje te mają wzmocnić ochronę nabywców i posiadaczy kryptoaktywów, a w konsekwencji wpłynąć nie tylko na bezpieczeństwo obrotu, lecz przede wszystkim na jego przejrzystość. W rozporządzeniu wyróżnia się trzy rodzaje kryptoaktywów, tj. tokeny powiązane z aktywami (ART),

[49] Osobnym problemem jest to, że nielegalne transfery pieniężne ułatwia także podatność blockchaina i CASPs na cyberataki, co wiąże się z wtórnymi lukami. Przykładem jest przejęcie kontroli nad 51% mocy obliczeniowej blockchaina (ang. *hush rate*), a w efekcie uzyskanie możliwości modyfikacji lub zmiany szczegółów transakcji, które nie zostały jeszcze zatwierdzone. Podobnie istnieje możliwość wykorzystywania tzw. mostów międzyłańcuchowych (ang. *cross-chain bridges*), które są zdecentralizowanymi platformami zapewniającymi transfer tokenów pomiędzy odrębnymi sieciami i gwarantują interoperacyjność ekosystemów kryptowalutowych. Jednocześnie ataki umożliwiają zachowanie anonimowości w transakcjach P2P. W normalnych warunkach takie transfery są szyfrowane, ale nie anonimowe. Pozwala to na identyfikację płatników dzięki szczegółom i zaszyfrowanym aliasom przechowywanym na blockchainie przez łączenie transakcji z komputerami osobistymi za pośrednictwem adresów IP. W związku z maskowaniem lub zmianą tych informacji na łańcuchu bloków przed zatwierdzeniem cyberataki pozwalają na dokonanie nielegalnych transakcji bez ryzyka identyfikacji. W przypadku CASPs zastosowanie wobec nich procederów przestępczych jest o tyle łatwiejsze, że te instytucje są powiernikami dla wielu portfeli.

tokeny będące pieniądzem elektronicznym (EMT) i tokeny użytkowe. Świadczenie usługi w zakresie kryptoaktywów będzie dopuszczalne wyłącznie przez osoby prawne mające siedzibę statutową w państwie członkowskim UE, które uzyskały zezwolenie na prowadzenie działalności w charakterze dostawcy takich usług[50]. Przy czym rozporządzenie MiCA ułatwia ich świadczenie podmiotom takim, jak: instytucje kredytowe, domy maklerskie, depozyty papierów wartościowych czy instytucje pieniądza elektronicznego, ponieważ nie wymaga od nich uzyskania zezwolenia na świadczenie usług w zakresie kryptoaktywów. Ustanawia się jedynie wymóg powiadomienia o tym właściwego organu nadzoru[51].

W rozporządzeniu MiCA szczególną uwagę w odniesieniu do sankcji zwraca się na kwestie dotyczące prania pieniędzy i finansowania terroryzmu. Poza tym, że CASPs będą zaliczeni do katalogu instytucji obowiązanych na gruncie AML, to jednocześnie wątki związane z AML i prywatnością (anonimowością) odnoszą się m.in do zakazu dopuszczania do obrotu kryptoaktywów, które mają wbudowaną funkcję anonimizacji[52]. CASP prowadzący platformę obrotu kryptoaktywami będzie musiał dysponować procedurami zapobiegającymi wykorzystywaniu jego infrastruktury do celów prania pieniędzy lub finansowania terroryzmu, a samo narażenie działalności przez organ zarządzający CASP na ryzyko prania pieniędzy jest obligatoryjną przesłanką odmowy udzielenia zezwolenia. Brak skutecznych procedur wewnętrznych w zakresie AML będzie natomiast obligatoryjną przesłanką cofnięcia zezwolenia. Ponadto obecny obowiązek stosowania procedur KYC od 1000 euro w przypadku niewystępowania żadnych podejrzeń w stosunku do klienta przeprowadzającego transakcję w przyszłości zostanie obniżony do 1 euro. To spowoduje obowiązek weryfikacji każdej operacji i tym samym korzystania ze środków bezpieczeństwa

[50] Wniosek o uzyskanie zezwolenia na prowadzenie działalności w charakterze dostawcy usług w zakresie kryptoaktywów będzie musiał zawierać przede wszystkim: opis procedury i systemu wykrywania nadużyć na rynku, opis zasad funkcjonowania platformy obrotu kryptoaktywami, opis systemów informatycznych i rozwiązań stosowanych przez dostawcę w zakresie bezpieczeństwa. Rejestr dostawców usług w zakresie kryptoaktywów będzie prowadzić Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (European Securities and Markets Authority, ESMA).

[51] Jednocześnie w rozporządzeniu MiCA jest wskazane wprost, że pewne usługi mogą być świadczone tylko przez określone podmioty. Dotyczy to m.in. dokonania oferty publicznej lub ubiegania się o dopuszczenie do obrotu EMT, co może zostać dokonane wyłącznie przez instytucję kredytową lub instytucję pieniądza elektronicznego, która jednocześnie jest emitentem takiego tokena (art. 48 ust. 1 rozporządzenia MiCA). Podobnie instytucje kredytowe nie będą zobowiązane do uzyskania zezwolenia na ofertę publiczną lub ubieganie się o dopuszczenie się do obrotu ART. Tak jak w przypadku licencji CASP, w tym zakresie instytucja kredytowa jest zobowiązana do sporządzenia dokumentu informacyjnego, odpowiedniej dokumentacji oraz do notyfikowania organowi nadzoru [pkt (44) preambuły i art. 17 rozporządzenia MiCA].

[52] Poza wyjątkiem, gdy CASP prowadzący platformę obrotu będzie w stanie zidentyfikować posiadaczy kryptoaktywów i historię transakcji.

finansowego. W znacznym stopniu wpłynie to na anonimowość, szczególnie pod kątem wymiany kryptowalut na waluty fiat. Podmioty spoza UE co do zasady utracą możliwość oferowania usług z zakresu kryptowalut na terenie Unii. Na ten moment w rozporządzeniu MiCA nie ma natomiast odniesień do sytuacji podmiotów z Europejskiego Stowarzyszenia Wolnego Handlu (European Free Trade Association, EFTA) i Europejskiego Obszaru Gospodarczego (European Economic Area, EEA). Terytorialny zakres rozporządzenia MiCA jest jednak ograniczony w związku z dopuszczeniem wykonywania działalności objętej jego zakresem przez firmy z państw trzecich w modelu *reverse solicitation*, czyli z wyłącznej inicjatywy klienta[53].

Przepisy MiCA w obszarze, w którym wprowadzają transparentne regulacje przepływu kryptoaktywów, są postrzegane jako źródło podniesienia skuteczności sankcji. Należy jednak uwzględnić, że unijne rozporządzenie formalnie zacznie obowiązywać dopiero od 30 grudnia 2024 r., przy czym nawet do 1 lipca 2026 r. może trwać okres przejściowy, w którym CASPs będą mogli kontynuować świadczenie usług w sposób nieregulowany. Istotne jest, że rozporządzenie MiCA nie objęło wielu newralgicznych zagadnień[54], w tym związanych z sankcjami międzynarodowymi, co dotyczy w szczególności zdecentralizowanych finansów[55] oraz cyfrowego pieniądza banku centralnego (ang. Central Bank Digital Currency, CBDC)[56].

---

[53] Na podstawie utrwalonych interpretacji na gruncie m.in. regulacji *Dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE* (tzw. Markets in Financial Instruments Directive, MiFID II) model świadczenia usługi z wyłącznej inicjatywy klienta nie powinien jednak znaleźć zastosowania w sytuacjach: podejmowania akcji promocyjnych ukierunkowanych na dany rynek, stworzenia stałego modelu biznesowego opierającego się na *reverse solicitation*, aktywnego pozyskiwania usługobiorców z innego państwa, posiadania przez usługodawcę strony internetowej z daną domeną krajową, a także inicjowania publikacji notek prasowych w portalach lub magazynach przeznaczonych dla danego rynku.

[54] MiCA nie odnosi się np. do tzw. tokenów zabezpieczających (ang. *security token*), które można uznać za zbywalne papiery wartościowe oraz do innych kryptoaktywów stanowiących instrumenty finansowe w rozumieniu MiFID II, jak również depozytów, pozycji sekurytyzacyjnych oraz produktów ubezpieczeniowych i emerytalnych. Podobnie rozporządzenie MiCA w najważniejszym zakresie nie obejmuje problematyki tokenów unikatowych (niewymiennych) – (ang. *non-fungible token*, NFT), chyba że replikują one instrument finansowy lub w przypadku których emitent tworzy „zbiór" aktywów do zakupu.

[55] Punkt (22) preambuły rozporządzenia MiCA statuuje wyłączenie stosowania przepisów rozporządzenia do usług w zakresie kryptoaktywów świadczonych w sposób w pełni zdecentralizowany bez pośredników. Niemniej rozporządzenie MiCA zawiera klauzule przeglądowe wynikające z art. 140 ust. 2 lit. t i art. 142 ust. 2 lit. a – w zakresie odnoszącym się do zdecentralizowanych finansów, które nakazują dokonywanie sprawozdawczości z oceny rozwoju DeFi na rynkach kryptoaktywów i odpowiedniego traktowania regulacyjnego zdecentralizowanych systemów kryptoaktywów, w tym ocenę konieczności i wykonalności regulacji zdecentralizowanego finansowania.

[56] Punkt (13) preambuły rozporządzenia MiCA precyzuje, że nie ma ono zastosowania do aktywów cyfrowych emitowanych przez banki centralne działające w charakterze organu kształtującego

Wraz z wejściem w życie rozporządzenia MiCA zacznie obowiązywać komplementarne z nim *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849* (dalej: rozporządzenie TFR). Wdraża ono zalecenia Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy (Financial Action Task Force, FATF) dotyczące tzw. *travel rule*. W tym zakresie nastąpi rozszerzenie obowiązków monitorowania przez unijnych dostawców usług płatniczych (w tym CASPs) transferów zarówno środków pieniężnych, jak i kryptoaktywów, co będzie polegało na obowiązku podawania szczegółowych informacji na temat płatnika (inicjatora) i odbiorcy transakcji (beneficjenta). *Travel rule*, tak jak w przypadku MiCA, nie znajdzie jednak zastosowania w sytuacji, gdy inicjujący transakcję i beneficjent są dostawcami usług płatniczych lub CASPs działającymi we własnym imieniu, a także w transferach między osobami przeprowadzanymi bez udziału CASP (art. 2 ust. 4 rozporządzenia TFR)[57].

Luka sankcyjna zdecentralizowanych finansów

Jak zasygnalizowano wcześniej, pkt (22) preambuły rozporządzenia MiCA precyzuje, że w zakres regulacji nie wchodzą określone w rozporządzeniu usługi związane z kryptowalutami, gdy są świadczone w sposób w pełni zdecentralizowany, bez pośredników. Pomimo to kwestia DeFi budzi na gruncie rozporządzenia MiCA sporo wątpliwości. Pojawia się np. problem dotyczący świadczenia usług wymiany kryptowalut lub obsługi platform handlu nimi w ramach zdecentralizowanych giełd (tzw. DEX). Trudność sprawia bowiem rozstrzygnięcie, czym jest pełna decentralizacja w rozumieniu tego rozporządzenia. Dotyczy to specyfiki budowy sieci blockchain, która powoduje, że DeFi wykorzystuje hierarchiczną architekturę warstwową o różnych celach[58]. Na gruncie rozporządzenia MiCA pozostaje

politykę pieniężną, co obejmuje także CBDC. Podobnie ramom unijnym nie podlegają powiązane usługi świadczone przez te banki centralne działające w charakterze władz monetarnych.

[57] Pierwszy wyjątek wynika bezpośrednio z faktu, że rozporządzenie TFR nie ma zastosowania do transferu środków pieniężnych, dla których płatnik i odbiorca są dostawcami usług płatniczych działającymi na własny rachunek (art. 2 ust. 4 lit. c rozporządzenia TFR). Drugi wyjątek wynika natomiast z zakresu określonego w art. 2 ust. 1 rozporządzenia TFR, tj. zastosowania wyłącznie do dostawców usług płatniczych, dostawców usług w zakresie kryptoaktywów lub pośredniczących dostawców usług płatniczych mających siedzibę w UE.

[58] Rozróżnia się trzy zasadnicze warstwy, tj. rozliczenia, protokołu oraz interfejsów. Warstwa rozliczenia (warstwa pierwsza) składa się z technologii rozproszonej księgi rachunkowej (DLT) i jej natywnego zasobu, zawierającego podstawowe zasady funkcjonowania ekosystemu. Warstwa protokołu (warstwa druga) obejmuje kompilator, zapewniając możliwość tworzenia interfejsów programowania

nierozstrzygnięte o jaki aspekt decentralizacji chodzi, ponieważ można mówić o niej w odniesieniu zarówno do warstwy rozliczenia (ang. *settlement layer*)[59], sposobu przechowywania kryptowalut, jak i do zarządzania organizacją i własnością protokołu. W związku z niedoprecyzowaniem tego zagadnienia w rozporządzeniu MiCA ocenę stopnia zdecentralizowania pozostawia się wyłącznemu uznaniu dostawcy usług kryptograficznych, który przez ten pryzmat ma dookreślić swój model biznesowy.

W obecnych uwarunkowaniach rozwoju technologicznego trudno sobie wyobrazić ustanowienie nad zdecentralizowanymi finansami ram regulacyjnych, które dawałyby realną możliwość ich egzekwowania. Przemawia za tym problem określenia właściwego porządku prawnego regulującego zasady dostępu do rynku i nadzoru, wynikający z dużego rozproszenia geograficznego użytkowników oraz z braku centralnych podmiotów odpowiedzialnych za świadczenie usług. Z uwagi na to rzeczywistą lukę w systemie sankcji międzynarodowych będą w przyszłości stanowić zdecentralizowane finanse, jako nowy model organizacji transferów finansowych bez żadnych pośredników, z automatyczną realizacją transakcji zawieranych za pomocą inteligentnych kontraktów (ang. *smart contracts*), będących protokołami, które działają w sieci blockchain.

DeFi, jako swoisty ekosystem zdecentralizowanych aplikacji finansowych opartych na tej technologii, oferuje możliwość zawierania szerokiego spektrum umów. System ten w istocie powiela istniejące modele usług finansowych z pominięciem ich scentralizowanych pośredników[60]. W efekcie w ramach DeFi użytkownicy zachowują pełną kontrolę nad swoimi aktywami w drodze synergii z ekosystemem przez zdecentralizowane aplikacje typu P2P. Aplikacje te nie potrzebują również podmiotów rozstrzygających ewentualne spory[61], gdyż wstępnie określony

aplikacji. Interfejs programowania aplikacji (ang. *application programming interface*, API) to zbiór definicji i protokołów do budowania i integrowania oprogramowania aplikacyjnego. W warstwie interfejsów (warstwa trzecia) są tworzone aplikacje zorientowane na użytkownika, umożliwiające interakcję z aplikacją za pośrednictwem strony internetowej. Zob. G. Maia, J. Vieira dos Santos, *MiCA and DeFi („Proposal for a Regulation on Market in Cryptoassets" and „Decentralised Finance")*, „Revista Electrónica de Direito" 2022, t. 28, nr 2, s. 63–65.

[59] W tej warstwie sieć węzłów niepolegająca na centralnym serwerze lub centralnej organizacji składa się z niewymagającego uprawnień blockchaina przez połączenia P2P pomiędzy niepowiązanymi i niezależnymi agentami.

[60] E. Avgouleas, A. Seretakis, *How Should Crypto Lending Be Regulated Under EU Law?*, „European Business Organization Law Review" 2023, t. 24, z. 3, s. 423–424. https://doi.org/10.1007/s40804-023-00293-3.

[61] Poprzez podejście probabilistyczne blockchain rozwiązał kwestię uzgadniania rozważaną w teorii gier, kryptografii oraz teorii systemów rozproszonych, określoną w 1980 r. przez Marshalla Pease'a, Leslie Lamporta i Roberta Shostaka jako problem generałów bizantyjskich. Zob. M. Pease, L. Lamport, R. Shostak, *The Byzantine Generals Problem*, „ACM Transactions on Programming Languages and Systems" 1982, t. 4, z. 3, s. 382–401. https://doi.org/10.1145/357172.357176.

kod dokona tego samodzielnie w przewidywalnych sytuacjach, jako tzw. *Lex Cryptographia*[62], a więc zgodnie z zasadami regulowanymi przez samowykonujące się inteligentne kontrakty i zdecentralizowane (autonomiczne) organizacje[63]. Z akceptacją idei „kod jest prawem" (ang. *code is law*) wiąże się jednak skutek w postaci wypierania przez technologię państwowych systemów prawnych[64].

Przy analizie problematyki inteligentnego kontraktu należy odnieść się do pierwotnej definicji tego pojęcia zaproponowanej przez Nicka Szabo, który określił go jako skomputeryzowany protokół transakcyjny, automatycznie realizujący warunki umowy. Celami projektowania są: spełnienie typowych warunków umownych, zminimalizowanie występowania wyjątków (zarówno złośliwych, jak i przypadkowych) oraz eliminacja jakichkolwiek zaufanych pośredników[65]. Idea ta opiera się bowiem na wykluczeniu potrzeby istnienia zaufania między stronami w związku ze zwiększeniem pewności wykonania umowy, zgodnie z tym, jak została ona zaprojektowana, wskutek gwarancji niezmienialności kontraktu (kodu). W efekcie z ekonomicznego punktu widzenia redukuje się mentalne i obliczeniowe koszty dodatkowe, obniżając straty związane z potencjalnymi oszustwami, kosztami arbitrażu i egzekucji oraz kosztami transakcyjnymi.

Aktualnie termin „inteligentny kontrakt" definiuje się jako kod wdrożeniowy działający w środowisku blockchain[66]. W tym sensie jest to kod algorytmiczny w programie komputerowym, wpisany oraz opierający się na danych w blockchainie[67].

---

[62] Blockchain w istotny sposób zmienia sposób rozumienia prawa przez oderwanie go od potrzeby istnienia jakiegokolwiek oparcia kulturowego czy legitymizacji autorytetem państwa. Według Katrin Becker blockchain oddziela pojęcie prawa od trzech kluczowych wymiarów, jakim są terytorium, język (i związana z tym interpretacja) oraz materia. Zob. K. Becker, *Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*, „Law and Critique" 2022, t. 33, s. 113–130. https://doi.org/10.1007/s10978-021-09317-8.

[63] A. Wright, P. De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, preprint, SSRN, 12 III 2015 r., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, s. 4 [dostęp: 5 III 2024]. http://dx.doi.org/10.2139/ssrn.2580664.

[64] D.A. Zetzsche, D.W. Arner, R.P. Buckley, *Decentralized Finance*, „Journal of Financial Regulation" 2020, t. 6, z. 2, s. 184. https://doi.org/10.1093/jfr/fjaa010.

[65] N. Szabo, *Smart Contracts*, 1994 r., https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html [dostęp: 5 III 2024]; tenże, *Smart Contracts: Building Blocks for Digital Markets*, 1996 r., https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html [dostęp: 5 III 2024].

[66] V. Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2014 r., https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [dostęp: 5 III 2024].

[67] R. Wilkens, R. Falk, *Smart Contracts. Grundlagen, Anwendungsfelder und rechtliche Aspekte*, Wiesbaden 2019, s. 3–4.

Wszelkie zobowiązania w inteligentnych kontraktach pozostają zgodne z klasyczną logiką Boole'a[68], stanowiącą podstawę całego przetwarzania cyfrowego, tj. „jeżeli-to" (ang. *if this then that*, IFTTT).

W kontekście sankcji międzynarodowych istotnym zagrożeniem dla ich realnej skuteczności jest możliwość dokonania agregacji wielu kontraktów przez stworzenie aplikacji o zaawansowanych funkcjonalnościach. Przykładami mogą być platformy pożyczkowe[69], pule płynności[70], platformy mediów społecznych czy rozproszone systemy zarządzania aktywami (tzw. *decentralised autonomous organisations*). Należy podkreślić, że inteligentne kontrakty wymykają się regulacjom prawnym rozporządzenia MiCA, nie są także definiowane w polskim ustawodawstwie oraz w innych reżimach prawnych. Oczywiście można przyjąć, że konstrukcja tych kontraktów przypomina specyficzny rodzaj zautomatyzowanego depozytu (ang. *escrow*) lub elektronicznego weksla. W sensie prawnym inteligentny kontrakt mógłby być traktowany jako szczególna forma umowy, ale wyłącznie przy założeniu, że jego zawarcie oparto by na świadomym oświadczeniu woli stron, że chcą one między sobą zawrzeć umowę o określonej treści[71]. Tą treścią mógłby być co do zasady kod zamieszczony na blockchainie. Wywołanie funkcji kodu na łańcuchu bloków stanowiłoby złożenie

---

[68] George Boole w 1854 r. stworzył tzw. algebrę Boole'a – strukturę matematyczną złożoną z trzech działań binarnych: ∨ (lub, or, alternatywa) – działanie podobne jak dodawanie; ∧ (i, and, koniunkcja) – odpowiednik mnożenia; ~ (nie, not, zaprzeczenie logiczne) oraz wyróżnionych elementów 0 (fałsz), 1 (prawda). Zob. S. Givant, P. Halmos, *Introduction to Boolean Algebras (Undergraduate Texts in Mathematics)*, New York 2009, s. 8–9.

[69] Środki pożyczane na platformach pożyczkowych są zapewniane przez samych użytkowników, w konsekwencji dostarczanie środków tego rodzaju usługom to *staking* w obrębie tej samej platformy. Przykładem jest projekt MakerDAO umożliwiający posiadaczom Ethereum (ETH) pożyczanie między członkami społeczności pieniędzy w postaci stablecoina DAI (starającego się utrzymać wartość 1:1 do dolara amerykańskiego). System polega na blokowaniu pewnej ilości ETH w inteligentnych kontraktach, co pozwala inwestorom wybijać nowe DAI i tym samym ustanawiać zabezpieczenie pożyczek. Po spłacie zadłużenia wraz z odsetkami następuje odblokowanie ETH. W sytuacji jednak, gdy wartość ETH spadnie poniżej kwoty pożyczonej w DAI, następuje likwidacja pożyczki poprzez sprzedaż ETH w celu spłaty pożyczonego DAI. Sama groźba likwidacji odstrasza od zaciągania nadmiernych pożyczek. W przypadku bowiem, gdy cena ETH gwałtownie spada, likwiduje się pożyczki w DAI, a wówczas posiadacze tokenów Maker (MKR) są pożyczkodawcami ostatniej szansy. MKR jest tworzony i sprzedawany w celu spłaty pożyczek, są w nich również uiszczane wszystkie opłaty w ramach MakerDAO. Kary likwidacyjne natomiast wykorzystuje się na odkup MKR, które następnie ulegają spalaniu.

[70] Pule płynności (ang. *liquidity pools*) to zbiór środków zablokowanych na inteligentnym kontrakcie, będących podstawą zdecentralizowanych giełd (DEX), takich jak Uniswap, które wykorzystują inteligentne kontrakty dla ułatwienia transakcji.

[71] Artykuł 60 *Ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny*.

dyspozycji generującej realizację umowy. Uznanie jednak inteligentnego kontraktu za umowę w rozumieniu prawa cywilnego oznaczałoby przyjęcie, że rzeczywiście doszło do w pełni świadomego złożenia oświadczenia woli. Spełnienie tego warunku wymagałoby samodzielnego tworzenia kodu przez strony inteligentnego kontraktu albo przynajmniej posiadania przez nie zdolności jego odczytania, czyli znajomości języka programowania, w którym ten inteligentny kontrakt został zakodowany[72]. Powstaje wątpliwość, czy w przypadku złożenia oświadczenia w formie kodu jest w ogóle możliwe przypisanie waloru świadomego oświadczenia woli co do treści umowy. Hipotetycznie taki problem mógłby zostać pominięty w sytuacji, gdyby inteligentny kontrakt był przedmiotem wcześniejszych negocjacji, których ustalenia zostałyby spisane w języku naturalnym, a dopiero następczo zakodowane w inteligentnym kontrakcie. Wówczas kod można byłoby potraktować wyłącznie w kategoriach narzędzia realizującego zobowiązania umowne, a nie podstawy powstania tych zobowiązań. Nie istnieje jednak żaden wymóg sporządzania inteligentnego kontraktu w języku naturalnym. Ponadto zdefiniowanie wszystkich elementów w samym kodzie automatycznie stanowi gwarancję zachowania pełnej anonimowości stron inteligentnego kontraktu.

Cyfrowy rubel – scentralizowana kryptowaluta

Kolejnym czynnikiem związanym z kryptowalutami i technologią blockchain, który może wpływać na osłabienie systemu sankcji finansowych, jest rozwój cyfrowego pieniądza banku centralnego (ang. Central Bank Digital Currency, CBDC). Bank Rozrachunków Międzynarodowych definiuje CBDC jako (…) *cyfrowy instrument płatniczy denominowany w krajowej jednostce rozliczeniowej, stanowiący bezpośrednie zobowiązanie banku centralnego*[73].

Z dniem 1 sierpnia 2023 r. weszły w życie przepisy ustawy federalnej nr 339-FZ „Zmieniającej w art. 128 i 140 części pierwszej, części drugiej oraz art. 1128 i 1174 części trzeciej Kodeksu cywilnego Federacji Rosyjskiej" oraz ustawy federalnej nr 340-FZ „Zmieniającej niektóre akty prawne Federacji Rosyjskiej". Regulacje te ukonstytuowały rubla cyfrowego opartego na blockchainie jako nową walutę narodową FR. Przepisy te określiły zasady wprowadzenia go do obiegu oraz warunki zastosowania w rozliczeniach. Dookreślono również uprawnienia CBFR jako operatora

[72] Obecnie najbardziej znaczącą platformą dla wdrażania inteligentnych kontraktów jest Ethereum, który implementuje kompletny język programowania Turinga pod nazwą Solidity.

[73] *Central bank digital currencies: foundational principles and core features*, Bank for International Settlements, 2020 r., https://www.bis.org/publ/othp33.pdf, s. 3 [dostęp: 5 III 2024].

jego platformy, a także rolę instytucji kredytowych przy przeprowadzaniu transakcji przez klientów oraz podstawy organizacyjne wykorzystania rubla cyfrowego przez osoby fizyczne i prawne jako nowej metody płatności, w tym w operacjach dokonywanych na rzecz cudzoziemców.

Do 31 grudnia 2024 r. Rada Dyrektorów CBFR wraz z Federalną Służbą Monitoringu Finansowego Federacji Rosyjskiej (Федеральная служба по финансовому мониторингу, Rosfinmonitoring) muszą określić zakres użytkowników platformy cyfrowego rubla, którzy będą uprawnieni do przeprowadzania transakcji rublami cyfrowymi na platformie, a także listę dopuszczalnych rodzajów transakcji oraz wartości progowe kwot dla takich operacji. Zgodnie z pierwotnymi założeniami możliwość dostępu do platformy cyfrowego rubla stwarza konieczność otworzenia cyfrowego konta rubla, będącego nowym rodzajem rachunku bankowego. Stronami umowy rachunku cyfrowego w rublu będą użytkownik i CBFR, a instytucja finansowa, w której użytkownik posiada klasyczny rachunek bankowy, będzie pośrednikiem reprezentującym CBFR w jego relacjach z użytkownikiem w celu korzystania z platformy cyfrowego rubla. Rosja powiela więc w tym zakresie pozytywne doświadczenia chińskie związane z wdrażaniem cyfrowego yuana (e-CNY).

Różnica między kryptowalutami a cyfrowymi walutami narodowymi jest fundamentalna. CBDC może przypominać tzw. stablecoin – cyfrową walutę (tokena płatniczego), której wartość jest powiązana ze stabilnym aktywem rezerwowym pozostającym w obrocie (np. walutą fiat lub złotem). CBDC, podobnie jak stablecoin, a w odróżnieniu od altcoina, podlega (przynajmniej teoretycznie) marginalnym wahaniom wartości. Najważniejsza różnica polega na tym, że CBDC jest, w przeciwieństwie do kryptowalut, prawnym środkiem płatniczym w kraju emisji, wspieranym przez rząd[74]. Scentralizowane cyfrowe waluty narodowe, zarządzane przez narodowe banki centralne, nie mogą jednak zapewnić użytkownikom pełnej anonimowości. O ile bowiem obie strony transakcji zachowają anonimowość w relacji zewnętrznej, o tyle nie będą już anonimowe z punktu widzenia banku centralnego, co da władzom możliwość pełnego monitoringu przepływów finansowych w czasie rzeczywistym[75].

[74] Z uwagi na swoją specyfikę stablecoiny, co do zasady, mogłyby spełnić wymogi definicji pieniądza elektronicznego ustanowione w ustawie o usługach płatniczych.

[75] Taki wariant dotyczy modelu opartego na rachunku, w którym zatwierdzenie transakcji przez zleceniodawcę i beneficjenta następuje na podstawie weryfikacji tożsamości użytkowników, gdyż ich transakcje są przypisywane do rachunków opartych na tożsamości. Inne rozwiązanie to CBDC bazujący na tokenach, gdzie transakcja zostaje zatwierdzona przez zleceniodawcę i beneficjenta na podstawie pary kluczy publiczno-prywatnych oraz podpisów cyfrowych. Taki system nie wymaga dostępu do tożsamości użytkownika, co zapewnia mu wysoki poziom prywatności. Zob. *Central Bank Digital Currencies. Building Block of the Future of Value Transfer*, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/financial-services/in-fs-cbdc-noexp.pdf [dostęp: 5 III 2024].

Z perspektywy państwa CBDC dostarcza nowych narzędzi polityki monetarnej i może być skutecznym instrumentem wpływu m.in. na dynamikę podaży pieniądza w gospodarce. Najważniejszym celem wdrażania tego instrumentu w kontekście obsługi wymiany transgranicznej jest oczekiwanie przełamania dominacji dolara w rozliczeniach handlowych. Należy zauważyć, że pełne wdrożenie cyfrowego rubla obejmuje plany uruchomienia platformy rozliczeń transgranicznych w ramach przestrzeni postradzieckiej Euroazjatyckiej Unii Gospodarczej i Wspólnoty Niepodległych Państw, a także w odniesieniu do krajów BRICS[76]. W konsekwencji rozwój CBDCs z perspektywy tych państw może znacząco przyczynić się do marginalizacji znaczenia zachodnich sankcji międzynarodowych w związku z uzyskaniem przez te państwa zdolności do dokonywania płatności bez udziału zagranicznych banków komercyjnych i infrastruktury finansowej takiej jak SWIFT[77]. To właśnie banki komercyjne są kluczowym ogniwem egzekwowania zachodnich sankcji, nie tylko z powodu uprawnień tych banków, lecz także ze względu na ponoszenie przez nie odpowiedzialności za blokowanie transakcji z udziałem podmiotów objętych sankcjami. Z uwagi przede wszystkim na amerykańskie sankcje nawet instytucje w krajach formalnie ich niestosujących, w przypadku wystąpienia elementu dolarowego lub innego łącznika amerykańskiego, muszą podchodzić z dużą ostrożnością do transakcji ze stroną rosyjską w związku z obawą nałożenia na te instytucje wtórnych sankcji.

W tym kontekście cyfrowy rubel w przyszłości mógłby umożliwić płatności transgraniczne bez konieczności korzystania z systemu bankowego innych krajów, dzięki obsłudze transakcji odbywającej się wyłącznie za pośrednictwem platformy cyfrowego rubla CBFR.

[76] BRICS jest formą współpracy państw o charakterze polityczno-gospodarczym. Pierwotnie grupa obejmowała Brazylię, Rosję, Indie i Chiny, a od 2011 r. także Republikę Południowej Afryki. Od stycznia 2024 r. miała ona poszerzyć swój skład o kolejne państwa, tj. Argentynę, Egipt, Etiopię, Arabię Saudyjską, Iran oraz Zjednoczone Emiraty Arabskie. Według oficjalnego przekazu ostatecznie Argentyna odstąpiła od planu przystąpienia do grupy, w przypadku Arabii Saudyjskiej natomiast nadal oficjalnie nie potwierdzono jej członkostwa. Główny cel tej grupy to stworzenie nowego systemu walutowego. Zob. BRICS Information Portal, http://infobrics.org/ [dostęp: 5 III 2024]; K. Karwowski, *Jeden statek – różni kapitanowie. Grupa BRICS po rozszerzeniu*, Instytut Nowej Europy, 20 III 2024 r., https://ine.org.pl/jeden-statek-rozni-kapitanowie-grupa-brics-po-rozszerzeniu/ [dostęp: 26 III 2024].

[77] K. Izenman, *The Other Side of the Digital Coin: Central Bank Digital Currencies and Sanctions*, RUSI, 26 V 2021 r., https://rusi.org/explore-our-research/publications/commentary/other-side-digital-coin-central-bank-digital-currencies-and-sanctions [dostęp: 5 III 2024].

Wnioski

Kazus rosyjski dobrze obrazuje problem oceny skuteczności sankcji gospodarczych. Przy założeniu, że ich celem jest dyscyplinowanie i ukaranie krajów[78], na które są one nakładane, należałoby uznać, że sankcje zastosowane wobec FR spełniają swoją funkcję. Bezsprzecznie wpływają negatywnie na rosyjską gospodarkę i jej system finansowy, ograniczają władzom dostępne wybory gospodarcze i polityczne, co powoduje większą centralizację gospodarki i uzależnienie od dostępnych partnerów handlowych. Z perspektywy pierwotnego i podstawowego celu, jakim było doprowadzenie do zaniechania przez FR ofensywy wojskowej w Ukrainie, zastosowane sankcje nie przyniosły jednak oczekiwanego rezultatu. Pojawia się także zasadniczy problem, że narastającym skutkom sankcji gospodarczych, negatywnie odbijającym się na wzroście gospodarczym i zdolnościach inwestycyjnych tego kraju, towarzyszy naturalna tendencja tworzenia się odporności na nie, ponieważ kształtują się możliwości ich skutecznego obchodzenia.

Przedstawiona analiza potwierdza wskazaną na wstępie wątpliwość dotyczącą realnej skuteczności sankcji w perspektywie rozwoju innowacyjnych instrumentów finansowych. W tym kontekście niewłaściwe byłoby niedostrzeganie rosnącego potencjału zasobów cyfrowych, w szczególności w wariancie DeFi oraz ich specyficznej odmiany w postaci walut cyfrowych banków centralnych. Te instrumenty w bliskiej przyszłości mogą pozwolić na stworzenie nowych, alternatywnych kanałów przepływów finansowych, niezależnych od obecnie istniejących zachodnich systemów płatności. Ich dalszy rozwój może wykreować bezsankcyjną przestrzeń transakcji finansowych i spowodować, że skutki ewentualnie nakładanych sankcji, zarówno w wymiarze finansowym, jak i handlowym, będą nieść za sobą wyłącznie lub w przeważającym zakresie negatywne skutki dla państw je stosujących. To, co teraz stanowi niszę i w marginalnym stopniu pozwala na uchylanie się przed egzekucją sankcji międzynarodowych, w nieodległym czasie może stać się potężnym narzędziem kształtującym nowy porządek międzynarodowy. Stanie się to wyzwaniem nie tylko dla systemów nadzoru rynków finansowych, lecz także dla podmiotów odpowiedzialnych za przeciwdziałanie zjawiskom prania pieniędzy i finansowania terroryzmu.

Niestety nie można jednoznacznie odpowiedzieć na pytanie, jakie środki prawne w pełni wyeliminowałyby istnienie luk w systemie finansowych sankcji międzynarodowych, w szczególności w odniesieniu do kazusu dużych światowych gospodarek, a także w perspektywie dalszego rozwoju możliwości wykorzystania

[78] J. Field, *Sanctions, Russia and 'crypto crime'*, CoinGeek, 7 IV 2023 r., https://coingeek.com/sanctions-russia-and-crypto-crime/ [dostęp: 5 III 2024].

technologii blockchain. Utopijne jest również oczekiwanie uzyskania międzynarodowej jednomyślności decyzyjnej zarówno w sprawie objęcia danego państwa środkami prewencyjnymi, jak i co do tożsamości skali i rodzaju stosowanych sankcji. Niemniej w przypadku krajów UE postulatem powinno być właściwe i sprawne wdrożenie rozporządzenia MiCA, przy dążeniu do jasnego doprecyzowania zakresu definicji legalnej pojęcia tzw. pełnej decentralizacji. Chodzi przede wszystkim o uniknięcie sytuacji, w której działalność zdecentralizowana bezpodstawnie wymykałaby się ramom regulacyjnym bądź też zostałaby stworzona przestrzeń uznaniowości regulatorów co do jej klasyfikacji. Tym samym w odniesieniu do zdecentralizowanych finansów *condicio sine qua non* pozostaje wypracowanie podstawowego mechanizmu klasyfikacji (taksonomii) dla tego pojęcia na poziomie wszystkich krajów członkowskich oraz szerzej – w skali globalnej[79].

Bibliografia

Avgouleas E., Seretakis A., *How Should Crypto Lending Be Regulated Under EU Law?*, „European Business Organization Law Review" 2023, t. 24, z. 3, s. 421–438. https://doi.org/10.1007/s40804-023-00293-3.

Becker K., *Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*, „Law and Critique" 2022, t. 33, s. 113–130. https://doi.org/10.1007/s10978-021-09317-8.

Bierzanek R., Symonides J., *Prawo międzynarodowe publiczne*, Warszawa 2003.

Demarais A., *Backfire: How Sanctions Reshape the World Against U.S. Interests*, New York 2022.

Givant S., Halmos P., *Introduction to Boolean Algebras (Undergraduate Texts in Mathematics)*, New York 2009.

Hufbauer G.C. i in., *Economic Sanctions Reconsidered: Supplemental case histories,* Washington 2007.

Maia G., Vieira dos Santos J., *MiCA and DeFi („Proposal for a Regulation on Market in Cryptoassets" and „Decentralised Finance")*, „Revista Electrónica de Direito" 2022, t. 28, nr 2, s. 57–82.

[79] Potrzebę wprowadzenia jednolitej systematyki dla DeFi i zasobów cyfrowych (ang. *digital assets*) zasygnalizowano m.in. w dokumencie: *Decentralised Finance – Principles for building a robust digital economy*, AFME, 6 VI 2023 r., https://www.afme.eu/ Portals/0/DispatchFeaturedImages/AFME%20DeFi%20Whitepaper.pdf [dostęp: 5 III 2024].

Opałek K., Wróblewski J., *Prawo. Metodologia, filozofia, teoria prawa*, Warszawa 1991.

Opałek K., Wróblewski J., *Zagadnienia teorii prawa*, Warszawa 1969.

Pape R.A., *Why Economic Sanctions Do Not Work*, „International Security" 1997, t. 22, nr 2, s. 90–136.

Pease M., Lamport L., Shostak R., *The Byzantine Generals Problem*, „ACM Transactions on Programming Languages and Systems" 1982, t. 4, z. 3, s. 382–401. https://doi.org/10.1145/357172.357176.

Wilkens R., Falk R., *Smart Contracts. Grundlagen, Anwendungsfelder und rechtliche Aspekte*, Wiesbaden 2019.

Zetzsche D.A., Arner D.W., Buckley R.P., *Decentralized Finance*, „Journal of Financial Regulation" 2020, t. 6, z. 2, s. 172–203. https://doi.org/10.1093/jfr/fjaa010.

Źródła internetowe

Annual value of international reserves of Russia from 2012 to 2022, by type, Statista, https://www.statista.com/statistics/1049298/russia-international-reserves-value-by-type/ [dostęp: 5 III 2024].

Bank of Russia foreign exchange and gold asset management report, Bank of Russia, Moscow 2022, https://www.cbr.ru/Collection/Collection/File/39685/2022-01_res_en.pdf [dostęp: 5 III 2024].

Bitcoin Mining Map, CCAF, https://ccaf.io/cbnsi/cbeci/mining_map [dostęp: 5 III 2024].

BRICS Information Portal, http://infobrics.org/ [dostęp: 5 III 2024].

Busch K.E., Tierno P., *Russian Sanctions and Cryptocurrency*, Congressional Research Service, 4 V 2022 r., https://crsreports.congress.gov/product/pdf/IN/IN11920 [dostęp: 5 III 2024].

Buterin V., *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2014 r., https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [dostęp: 5 III 2024].

Central Bank Digital Currencies. Building Block of the Future of Value Transfer, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/financial-services/in-fs-cbdc-noexp.pdf [dostęp: 5 III 2024].

Central bank digital currencies: foundational principles and core features, Bank for International Settlements, 2020 r., https://www.bis.org/publ/othp33.pdf [dostęp: 5 III 2024].

Cryptocurrencies: a way to evade sanctions?, BAFFI – Centre on Economics, Finance and Regulation, https://baffi.unibocconi.eu/research-units/mints-alternative-monies/newsletter/issue-0/cryptocurrencies-way-eva de-sanctions [dostęp: 5 III 2024].

Crypto-assets relevant pro-vision: Article 5b(2) of Council Regulation (EU) No 833/2014 – frequently asked questions, UE, 21 III 2023 r., https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [dostęp: 5 III 2024].

Decentralised Finance – Principles for building a robust digital economy, AFME, 6 VI 2023 r., https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME%20DeFi%20Whitepaper.pdf [dostęp: 5 III 2024].

Field J., *Sanctions, Russia and 'crypto crime'*, CoinGeek, 7 IV 2023 r., https://coingeek.com/sanctions-russia-and-crypto-crime/ [dostęp: 5 III 2024].

Izenman K., *The Other Side of the Digital Coin: Central Bank Digital Currencies and Sanctions*, RUSI, 26 V 2021 r., https://rusi.org/explore-our-research/publications/commentary/other-side-digital-coin-central-bank-digital-currencies-and-sanctions [dostęp: 5 III 2024].

Karwowski K., *Jeden statek – różni kapitanowie. Grupa BRICS po rozszerzeniu*, Instytut Nowej Europy, 20 III 2024 r., https://ine.org.pl/jeden-statek-rozni-kapitanowie-grupa-brics-po-rozszerzeniu/ [dostęp: 26 III 2024].

Komunikat prasowy Komisji Europejskiej: *Ukraine: EU agrees to extend the scope of sanctions on Russia and Belarus*, 9 III 2022 r., https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1649 [dostęp: 5 III 2024].

Leali G., *France not opposed in principle to cutting Russia from SWIFT: Bruno Le Maire*, Politico, 25 II 2022 r., https://www.politico.eu/article/Frances-le-maire-not-against-cutting-russia-out-of-swift/ [dostęp: 5 III 2024].

Pape R.A., wpis na portalu LinkedIn, https://uk.linkedin.com/posts/robert-pape_someone-asked-my-view-on-how-sanctions-are-activity-6970475273985171456-6ora [dostęp: 5 III 2024].

Pismennaya E., *Russia Values Local Crypto at $200 Billion as Rules Near*, Bloomberg, 1 II 2022 r., https://www.bloomberg.com/news/articles/2022-02-01/russia-values-local-crypto-market-at-200-billion-as-rules-near#xj4y7vzkg [dostęp: 5 III 2024].

Sanctions and Restrictions Against Russia in Response to its Invasion of Ukraine, Ministry of Foreign Affairs Singapore, 5 III 2022 r., https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/03/20220305-sanctions/ [dostęp: 5 III 2024].

Szabo N., *Smart Contracts*, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html [dostęp: 5 III 2024].

Szabo N., *Smart Contracts: Building Blocks for Digital Markets*, 1996 r., https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo. best.vwh.net/smart_contracts_2.html [dostęp: 5 III 2024].

Wilson T., *Rouble-crypto trading soars as sanctions hit Russian currency*, Reuters, 28 II 2022 r., https://www.reuters.com/markets/europe/rouble-crypto-trading-soars-sanctions--hit-russian-currency-2022-02-28/ [dostęp: 5 III 2024].

Wiśniewska I., *Rosyjska gospodarka w roku 2022. Adaptacja i rosnący deficyt budżetu*, OSW, 16 II 2023 r., https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2023-02-16/rosyjska--gospodarka-w-roku-2022-adaptacja-i-rosnacy-deficyt [dostęp: 5 III 2024].

Wpływ sankcji na rosyjską gospodarkę, Rada UE, https://www.consilium.europa.eu/pl/infographics/impact-sanctions-russian-economy/ [dostęp: 5 III 2024].

Wright A., De Filippi P., *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, preprint, SSRN, 12 III 2015 r., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 [dostęp: 5 III 2024]. http://dx.doi.org/10.2139/ssrn.2580664.

Wright C.S., *Bitcoin Is Anything BUT Anonymous*, Bitcoin & Blockchain Tech, 1 IX 2019 r., https://craigwright.net/blog/bitcoin-blockchain-tech/bitcoin-is-anything-but-anonymous/ [dostęp: 5 III 2024].

Rosyjskie źródła internetowe

В ЦБ сообщили о 70% внутрироссийского трафика у национального аналога SWIFT, Известия, 3 VII 2023 r., https://iz.ru/1538263/2023-07-03/v-tcb-soobshchili-o-70-vnutrirossiiskogo-trafika-u-natcionalnogo-analoga-swift [dostęp: 5 III 2024].

ЦБ предложил дать зарубежным банкам доступ к цифровому рублю с 2025 года, RBC.ru, 10 X 2023 r., https://www.rbc.ru/finances/10/10/2023/6523e87b9a7947b24f71b430 [dostęp: 5 III 2024].

Российский аналог SWIFT распространяется на Восток, News.Ru, 27 I 2024 r., https://news.ru/economics/rossijskij-analog-swift-rasshiryaet-svoe-vliyanie [dostęp: 5 III 2024].

Akty prawne

Rozporządzenie Rady (UE) 2024/745 z dnia 23 lutego 2024 r. zmieniające rozporządzenie (UE) nr 833/2014 dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE L z 23 II 2024 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dz. Urz. UE L 150/40 z 9 VI 2023 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849 (Dz. Urz. UE L 150/1 z 9 VI 2023 r.).

Rozporządzenie Rady (UE) 2022/1904 z dnia 6 października 2022 r. w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE LI 259/3 z 6 X 2022 r.).

Rozporządzenie Rady (UE) 2022/576 z dnia 8 kwietnia 2022 r. w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE L 111/1 z 8 IV 2022 r., ze zm.).

Rozporządzenie Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE L 229/1 z 31 VII 2014 r., ze zm.).

Rozporządzenie Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78/6 z 17 III 2014 r., ze zm.).

Rozporządzenie Rady (UE) nr 359/2011 z dnia 12 kwietnia 2011 r. dotyczące środków ograniczających skierowanych przeciwko niektórym osobom, podmiotom i organom w związku z sytuacją w Iranie (Dz. Urz. UE L 100/1 z 14 IV 2011 r., ze zm.).

Rozporządzenie Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczące środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134/1 z 20 V 2006 r., ze zm.).

Ustawa z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. DzU z 2023 r. poz. 1497, ze zm.).

Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców (t.j. DzU z 2023 r. poz. 221, ze zm.).

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. DzU z 2023 r. poz. 1124, ze zm.).

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. DzU z 2022 r. poz. 2360, ze zm.).

Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (t.j. DzU z 2023 r. poz. 753, ze zm.).

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. DzU z 2023 r. poz. 1610, ze zm.).

Rosyjskie akty prawne

Федеральный закон от 31.07.2020 № 259-ФЗ „О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации”, Kremlin.ru, http://www.kremlin.ru/acts/bank/45766/page/1 [dostęp: 5 III 2024].

Федеральный закон от 14.07.2022 № 331-ФЗ „О внесении изменений в отдельные законодательные акты Российской Федерации и о приостановлении действия отдельных положений статьи 5.1 Федерального закона «О банках и банковской деятельности»”, http://publication.pravo.gov.ru/Document/View/0001202207140083?index=1 [dostęp: 5 III 2024].

Федеральный закон от 24.07.2023 № 339-ФЗ „О внесении изменений в статьи 128 и 140 части первой, часть вторую и статьи 1128 и 1174 части третьей Гражданского кодекса Российской Федерации”, http://publication.pravo.gov.ru/document/0001202307240009 [dostęp: 5 III 2024].

Федеральный закон от 24.07.2023 № 340-ФЗ „О внесении изменений в отдельные законодательные акты Российской Федерации”, http://publication.pravo.gov.ru/Document/View/0001202307240024 [dostęp: 5 III 2024].

Angela Pacholczak

Absolwentka studiów doktoranckich na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego.

Kontakt: angelapacholczak@gmail.com

Model infiltracji Jeżowa a zajęcie Krymu przez Federację Rosyjską

Yezhov's infiltration model and the Russian Federation's seizure of Crimea

MAREK ŚWIERCZEK

Agencja Bezpieczeństwa Wewnętrznego
https://orcid.org/0000-0002-0661-0315

Przegląd Bezpieczeństwa Wewnętrznego, 2024, nr 30: 131–157

https://doi.org/10.4467/20801335PBW.24.005.19607

ARTYKUŁ

Abstrakt

Autor dokonał analizy skali zdrady wśród funkcjonariuszy i urzędników państwa ukraińskiego podczas aneksji Krymu przez Federację Rosyjską w 2014 r. Głównym problemem badawczym była próba wyjaśnienia anomalii w działalności służb specjalnych w postaci przyjęcia do rosyjskiej Federalnej Służby Bezpieczeństwa 1400 funkcjonariuszy Służby Bezpieczeństwa Ukrainy. Próbując wyjaśnić ten ewenement w działalności służb specjalnych, autor posłużył się teorią wywiadu i kontrwywiadu ofensywnego rozwijaną w Związku Socjalistycznych Republik Radzieckich od początku lat 20. XX w. oraz ustaleniami psychologii poznawczej dotyczącymi projekcji jako głównego mechanizmu tłumaczenia przez ludzi zachowań innych osób. Na podstawie analizy dorobku teoretycznego sowieckich służb i ustaleń psychologii autor wysunął hipotezę o masowym werbunku przez Rosjan funkcjonariuszy SBU na Krymie na długo przed aneksją. Zdaniem autora głównymi mechanizmami pozyskiwania agentury w celu opanowania organizacji przeciwnika były szeroko rozumiana korupcja oraz kumoterstwo, które to zjawiska są charakterystyczne dla obszaru postsowieckiego.

Słowa kluczowe

aneksja Krymu, FSB, SBU, korupcja jako czynnik zdrady, kontrwywiad ofensywny

Abstract

The author analysed the scale of betrayal among the officers and officials of the Ukrainian state during the annexation of Crimea by the Russian Federation in 2014. The main research problem was an attempt to explain the anomaly in the activities of the special services in the form of recruiting 1,400 officers of the Ukrainian SBU to the Russian FSB. In an attempt to explain this phenomenon in the practice of secret services, the author used the theory of offensive intelligence and counter-intelligence created and developed in the USSR from the early 1920s, as well as the findings of cognitive psychology regarding the phenomenon of projection as the main mechanism for explaining the behavior of other people. Thanks to the synthesis of psychology and the analysis of the theoretical achievements of the Soviet secret services, the author put forward a hypothesis about the mass recruitment of the SBU officers in the Crimea long before the annexation. According to the author, the main mechanisms of mass recruitment of agents in order to control the opponent's organisation were broadly understood corruption and cronyism characteristic to the post-Soviet area.

Keywords

annexation of Crimea, FSB, SBU, corruption as a factor of betrayal, offensive counterintelligence

Dnia 21 lutego 2014 r. prezydent Ukrainy Wiktor Janukowicz podpisał z opozycją porozumienie przewidujące m.in. powrót do konstytucji z 2004 r. (która znacznie ograniczała kompetencje prezydenckie) oraz przeprowadzenie przedterminowych wyborów prezydenckich do końca 2014 r. Jeszcze tego samego dnia Janukowicz wyjechał z Kijowa do Charkowa, aby wziąć udział w zjeździe deputatów południowo-wschodnich obwodów. Utrzymywał potem, że podczas tej podróży doszło do nieudanego zamachu na kolumnę prezydencką[1].

Pod naciskiem wielotysięcznej demonstracji z udziałem uzbrojonych bojówek Prawego Sektora Rada Najwyższa Ukrainy przyjęła 22 lutego uchwałę, w której stwierdzono, że wyjeżdżając z Kijowa, Janukowicz porzucił wykonywanie obowiązków

[1] Zob. wywiad Wiktora Janukowicza udzielony Nikołajowi Zjatkowowi: *Виктор Янукович: «Народ договорится, и Украина станет единой»*, „Аргументы и Факты" 2014, nr 52, wersja online: https://aif.ru/euromaidan/viktor_yanukovich_eksklusivnoe_interview [dostęp: 6 VI 2023]. Później oskarżenie o próbę zamordowania Janukowicza przez opozycję powtórzył Władimir Putin, podkreślając, że gdyby nie pomoc rosyjskich służb specjalnych, Janukowicz zostałby zabity. Zob. wywiad udzielony Andriejowi Kandraszowowi w 2015 r.: *Крым Путь на Родину Документальный фильм Андрея Кондрашова*, YouTube, 4 X 2020 r., https://www.youtube.com/watch?v=PGGNXIQXlcU [dostęp: 2 III 2023].

prezydenckich. Na 25 maja wyznaczono termin nowych wyborów głowy państwa. Za przyjęciem uchwały głosowało 328 deputowanych (w tym posłowie wchodzący do niedawna w skład większości rządowej). Dnia 23 lutego Rada Najwyższa powierzyła przewodniczącemu Ołeksandrowi Turczynowowi pełnienie obowiązków prezydenta.

Z perspektywy władz Federacji Rosyjskiej (FR) oznaczało to niemal całkowitą utratę możliwości wpływu na sytuację polityczną w Ukrainie, a pod względem militarnym – znaczne osłabienie jej pozycji w basenie Morza Czarnego. Rosja spodziewała się wypowiedzenia (przez nowy, nastawiony antyrosyjsko rząd ukraiński) umowy pozwalającej na stacjonowanie na Krymie Floty Czarnomorskiej FR[2]. Mimo że składała się wówczas z ok. 40 okrętów zbudowanych jeszcze w latach 70. XX w., zachowywała pełną zdolność operacyjną[3] oraz była w trakcie intensywnej modernizacji i rozbudowy[4]. Jej stacjonowanie w Sewastopolu zapewniało Rosjanom dostęp nie tylko do Morza Czarnego, lecz także do Morza Śródziemnego, południowego Atlantyku i Oceanu Indyjskiego[5], pomimo prawnych ograniczeń narzucanych przez konwencję z Montreux[6]. Krym dawał FR możliwość operowania na oceanach oraz dominacji militarnej na czarnomorskim teatrze wojny ze względu na opcję rozbudowy rakietowych systemów antyokrętowych oraz przeciwlotniczych (zwłaszcza przy zwiększonych możliwościach wyrzutni S-400)[7].

Gwałtowna zmiana władzy w Ukrainie oznaczała zatem dla Rosji bardzo poważne problemy geopolityczne, jakimi były znaczne zmniejszenie głębi operacyjnej obrony (otuliny państw neutralnych na granicach z Organizacją Traktatu Północnoatlantyckiego) oraz utrata dominującej pozycji w basenie Morza Czarnego, co bardzo osłabiało południową flankę FR. Rosja, wówczas za słaba, aby ryzykować otwarty

---

[2] W 2010 r. Janukowicz podpisał tzw. porozumienie charkowskie przedłużające umowę regulującą stacjonowanie Floty Czarnomorskiej na Krymie do 2042 r. w zamian za obniżenie cen gazu sprzedawanego Ukrainie przez FR. Głosowanie w tej sprawie w Radzie Najwyższej doprowadziło do konfrontacji z użyciem siły pomiędzy przedstawicielami Partii Regionów i opozycji. Zob. *Janukowycz podpisał umowę o stacjonowaniu rosyjskiej floty na Ukrainie*, Portal Spraw Zagranicznych, 29 IV 2010 r., https://psz.pl/162-wschod/janukowycz-podpisal-umowe-o-stacjonowaniu-rosyjskiej-floty-na-ukrainie [dostęp: 7 VI 2023].

[3] Potwierdza to skuteczna blokada Gruzji w czasie wojny w 2008 r.

[4] W ówczesnych planach było – prócz modernizacji starych okrętów – uzupełnienie floty o sześć nowych łodzi podwodnych i sześć nowych fregat, a także o francuski śmigłowcowiec typu Mistral.

[5] *Crimea's Strategic Value to Russia*, Center for Strategic and International Studies, 18 III 2014 r., https://www.csis.org/blogs/post-soviet-post/crimeas-strategic-value-russia [dostęp: 6 VI 2023].

[6] *Convention concernant le régime des détroits* – porozumienie podpisane w 1936 r. regulujące prawo morza w cieśninach czarnomorskich. Dotyczy prawa i zasad przechodzenia przez cieśniny czarnomorskie statków i okrętów nienależących do Turcji, na której wodach terytorialnych znajdują się Bosfor i Dardanele.

[7] *Crimea's Strategic Value to Russia...*

konflikt, odpowiedziała na to zagrożenie działaniami hybrydowymi, z wykorzystaniem sieci agenturalnych budowanych od dawna w Ukrainie[8] oraz maskowanej siły kinetycznej[9]. Dokonała aneksji Krymu oraz uwikłała Ukrainę w długotrwały konflikt na Donbasie, skutecznie blokujący aspiracje tego kraju do członkostwa w NATO, jak również zagarnęła znaczną część ukraińskiego przemysłu ciężkiego i zasobów surowcowych, co jeszcze bardziej pogorszyło trudną sytuację gospodarczą w tym kraju. Utrata Krymu (wraz z niemal 2 mln mieszkańców) oraz masowa emigracja wywołana ośmioletnim konfliktem, który w lutym 2022 r. przekształcił się w pełnoskalową inwazję, sprawiły, że z 52 mln Ukraińców w 1991 r. pozostało na obecnym terytorium ukraińskim od 28 do 34 mln ludzi[10]. Rosyjskie działania hybrydowe, jeszcze zanim przeszły w fazę gorącej wojny, miały zatem skutki o znaczeniu strategicznym dla całego państwa ukraińskiego.

Aneksja Krymu i próba oddzielenia wschodnich i południowo-wschodnich obwodów Ukrainy jako rosyjskie operacje specjalne

Podjęte w 2014 r. działania FR przeciwko Ukrainie miały charakter ciągu operacji specjalnych, w czasie których Rosja realizowała swoje cele geopolityczne. Osiągała je poprzez zabór terytoriów ukraińskich najważniejszych pod względem gospodarczym i militarnym[11], jednak – aż do 2022 r. – bez konieczności prowadzenia pełnoskalowej wojny[12]. Użycie armii było punktowe, zawsze maskowane i na niewielką skalę. Umożliwiał to paraliż ukraińskich centrów decyzyjnych (tj. nowo powstałego rządu oraz kierownictw resortów siłowych) po przejęciu władzy przez opozycję w lutym

[8] Szerzej na temat wykorzystania agentury do realizacji strategicznych celów w Ukrainie zob. M. Świerczek, *Szturm na siedzibę Służby Bezpieczeństwa Ukrainy w Ługańsku w 2014 r. jako przykład operacji służb specjalnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2023, nr 28, s. 52–86. https://doi.org/10.4467/20801335PBW.23.002.17652.

[9] Najpierw były to tzw. zielone ludziki na Krymie, a następnie zgrupowania wojskowe walczące na Donbasie z armią ukraińską i pozorujące, że są siłami donbaskiej samoobrony, pomimo tego, że zamykane w kolejnych kotłach ukraińskie oddziały były dziesiątkowane za pomocą ciężkiego sprzętu, którego separatyści nie mogli posiadać.

[10] O. Danylov, *As of January 1, 2023, the population of Ukraine was 28-34 million*, Mezha.Media, 7 IV 2023 r., https://mezha.media/en/2023/04/07/as-of-january-1-2023-the-population-of-ukraine-was-28-34-million/ [dostęp: 7 VI 2023]. Tak duży margines niepewności wynika z tego, że badacze nie potrafią poprawnie ocenić, czy emigranci wrócą do kraju, czy zostaną na stałe w krajach docelowych.

[11] Jak już wspomniano, próba odebrania Ukrainie całego wschodu oznaczała groźbę dezindustrializacji oraz odcięcia tego kraju od portów, którymi eksportowano zboże.

[12] Irracjonalne jest to, że po dwóch latach trwania wojny nie została ona wypowiedziana przez żadną z walczących stron.

2014 r. Przy czym bierność i brak oporu ze strony Ukraińców, a także ich kolaboracja z najeźdźcami (tajna lub jawna) występowały niemal na wszystkich poziomach ukraińskiej państwowości. Badanie przebiegu kolejnych operacji rosyjskich w Ukrainie wskazuje, że silny wpływ na te procesy miała rosyjska agentura[13]. Rosyjskie siatki wywiadowcze były budowane zarówno z wykorzystaniem politycznych sieci klientelistycznych w instytucjach państwowych (zwłaszcza w resortach siłowych), jak i wśród populacji rosyjskojęzycznej, której obrona przed rzekomym prześladowaniem miała stanowić przykrywkę dla działań FR.

Skala infiltracji

Wskaźnikiem obiektywnym skali rosyjskiej infiltracji instytucji państwa ukraińskiego jest liczba ukraińskich żołnierzy i funkcjonariuszy resortów siłowych oraz urzędników, którzy – po aneksji Krymu – kontynuowali służbę i pracę na rzecz okupantów, odmawiając wyjazdu z półwyspu i powrotu do Ukrainy. Pierwszą próbę podsumowania skali kolaboracji ukraińskich struktur państwowych na Krymie z Rosjanami podjął ówczesny zastępca przewodniczącego Medżlisu Tatarów Krymskich[14] Ilmi Umerow[15]. W wywiadzie udzielonym 3 listopada 2017 r. ukraińskiemu wydaniu gazety „Новое время" stwierdził on, że 100% krymskich funkcjonariuszy milicji i Służby Bezpieczeństwa Ukrainy (SBU), 80% wojskowych oraz 70% pracowników prokuratury przeszło na stronę rosyjską i kontynuowało swoją dotychczasową pracę, tyle że na rzecz sił okupacyjnych[16]. Zdaniem Umerowa dowodziło to, że państwo ukraińskie przez dekady nie prowadziło żadnej pracy ideologicznej wśród ludności Krymu, a Rosjanie od bardzo dawna przygotowywali się do aneksji przez rozbudowę agentury i poddawanie ludności półwyspu intensywnej propagandzie[17]. Stwierdził on, że jednym z elementów wpływania na społeczeństwo i organy państwa na Krymie miało być (równolegle do wieloletniego budowania nastrojów prorosyjskich) przedstawianie Tatarów i ich organizacji jako głównego czynnika ekstremistycznego i wrogiego

[13] Por. M. Świerczek, *Szturm na siedzibę Służby Bezpieczeństwa Ukrainy w Ługańsku...*

[14] Medżlis Tatarów Krymskich (Къырымтатар Миллий Меджлиси) – organizacja Tatarów krymskich, której zadaniem jest reprezentowanie interesów tej społeczności na Krymie.

[15] Ilmi Umerow (ur. w 1957 r.) – ukraiński polityk i działacz społeczny narodowości tatarskiej. W 2017 r. skazany na Krymie pod zarzutem godzenia w integralność terytorialną FR, po czym wydany przez władze rosyjskie Turcji w zamian za dwóch zatrzymanych agentów FSB.

[16] *Замглавы Меджлиса Умеров: Сотрудники СБУ и милиции в Крыму оказались предателями на 100%, военнослужащие - на 80%, прокуратура - на 70%*, New Voice, 5 XI 2017 r., https://nv.ua/ukraine/politics/zamglavy-medzhlisa-umerov-sotrudniki-sbu-i-militsii-v-krymu-okazalis-predateljami-na-100-voennosluzhashchie-na-80-prokuratura-na-70-2135335.html [dostęp: 7 V 2023].

[17] Tamże.

ukraińskiej władzy na Krymie[18]. Był to sposób na odciągnięcie uwagi resortów siłowych od rosyjskiej aktywności. Umerow wskazał, że najdobitniejszym przejawem zdrady było to, że żadna z 300 jednostek ukraińskiego wojska na Krymie nie stawiała oporu oddziałom rosyjskim, które siłowo przejmowały koszary i sprzęt[19].

Jego wypowiedź wywołała burzę w ukraińskich mediach i podsyciła obserwowane od dawna zjawiska – szpiegomanię oraz polityzację powszechnych zarzutów o zdradę[20]. Część komentatorów oskarżała Umerowa o celowe zawyżanie statystyk[21].

W związku z tym dochodzenie poselskie przeprowadził deputat Rady Najwyższej Dmytro Tymczuk, który rozesłał oficjalne zapytania parlamentarne do właściwych ministerstw[22]. Odpowiedzi zawierające urzędowo potwierdzone dane pozwoliły na sporządzenie podsumowania, z uwzględnieniem podziału na poszczególne służby i siły zbrojne[23].

---

[18] Tamże.

[19] Tamże.

[20] W celu uzmysłowienia sobie skali zjawiska warto prześledzić rubrykę ДЕРЖЗРАДА na portalu Ukrinform. Znajduje się tam bardzo duża liczba wpisów dotyczących prawdziwych i domniemanych zdrajców. Zob. https://www.ukrinform.ua/tag-derzzrada [dostęp: 14 VI 2023]. Dobry przykład stanowią też wpisy i artykuły na temat zdrady zamieszczone na portalu Myrotvorets. Zob. https://myrotvorets.news/?s=%D0%B7%D1%80%D0%B0%D0%B4%D0%BD%D0%B8%D0%BA [dostęp: 14 VI 2023].

[21] Por. *Официальная статистика: замглавы Меджлиса завысил количество предателей в Крыму на 10 %*, Inform Napalm, 7 XI 2017 r., https://informnapalm.org/41430-ofitsialnaya-statistika-zamglavy-medzhlisa-zavysil-protsent/ [dostęp: 7 V 2023]; А. Круглов, *На измене, Совершенно Секретно*, 30 X 2014 r., https://www.sovsekretno.ru/articles/bezopasnost/na-izmene/ [dostęp: 7 V 2023]; *„Предатели на 100%": Умеров резко высказался о спецслужбах в Крыму*, OBOZ.UA, 5 XI 2017 r., https://news.obozrevatel.com/society/predateli-na-100-umerov-rezko-vyiskazalsya-o-spetssluzhbah-v-kryimu.htm [dostęp: 7 V 2023]; О. Козаченко, *Умеров жалеет, что в Крыму не стали стрелять по русским*, Полит Навигатор, 3 XI 2017 r., https://m.politnavigator.net/umerov-zhaleet-chto-v-krymu-ne-stali-strelyat-po-russkim.html [dostęp: 7 V 2023]; *Замглавы Меджлиса упрекнул Украину в сдаче Крыма без стрельбы*, Черноморская телерадиокомпания, 6 XI 2017 r., https://blackseatv.com/in-the-spotlight/zamglavy-medzhlisa-upreknul-ukrainu-v-sdache-kryma-bez-strelby/ [dostęp: 7 V 2023]; *Теперь пишут записки в Москву: озвучены масштабы предательства крымчан*, From-UA, 30 XI 2017 r., https://from-ua.org/news/425623-teper-pishut-zapiski-v-moskvu-ozvucheni-masshtabi-predatelstva-krimchan.html [dostęp: 7 V 2023]; *Более 10 тысяч солдат перешли на службу России*, Бездформата, https://angarsk.bezformata.com/listnews/soldat-pereshli-na-sluzhbu-rossii/62518616/ [dostęp: 7 V 2023]; *Сколько военных ВСУ и СБУ перешли на сторону России в 2014 году*, RF-SMI, 20 II 2022 r., https://rf-smi.ru/ykr/71072-skolko-voennyh-vsu-i-sbu-pereshli-na-storonu-rossii-v-2014-godu.html [dostęp: 7 V 2023].

[22] Skan odpowiedzi z ukraińskiego Ministerstwa Obrony. Zob. *Сколько военных из Крыма предали Украину: шокирующие цифры*, Panoptikon, 7 XI 2017 r., https://panoptikon.org/ukraine/98813-skolko-voennykh-iz-kryma-predali-ukrainu-shokirujushhie-cifry.html [dostęp: 4 VI 2023].

[23] Dane przytoczone za: Д. Тымчук, *Сколько крымских силовиков стали предателями Украины*, UA Info, 6 XI 2017 r., https://uainfo.org/blognews/1509980385-skolko-ukrainskiy-silovikov-v-krymu-stali-predatelyami.html [dostęp: 4 VI 2023]; *Тымчук назвал число предателей среди украинских*

Służba Bezpieczeństwa Ukrainy

Na 1 marca 2014 r. we wszystkich jednostkach organizacyjnych na Krymie służyło 1619 funkcjonariuszy, z czego 1235 należało do korpusu oficerskiego. Po aneksji do Ukrainy wyjechało 217 funkcjonariuszy, w tym 210 oficerów. Odsetek zdrajców wyniósł zatem 86,4%, a wśród oficerów – 83%[24].

Ukraińskie Siły Zbrojne

Na 1 marca 2014 r. na Krymie stacjonowało 13 468 żołnierzy Zbrojnych Sił Ukrainy (ZSU), w tym 4737 oficerów. Po przejęciu Krymu przez FR z półwyspu wyjechało 3991 wojskowych, w tym 1649 oficerów. Odsetek zdrajców w ZSU wyniósł więc 70,4%, a wśród oficerów – 65%[25].

Ministerstwo Spraw Wewnętrznych

Nie ma danych dotyczących liczby ukraińskich milicjantów na Krymie. Dostępne są jedynie informacje na temat wojsk wewnętrznych pozostających w gestii MSW i Straży Granicznej.

Na 1 marca 2014 r. na Krymie przebywało 2489 żołnierzy wojsk wewnętrznych. Do Ukrainy wróciło 1398. W szeregach wojsk wewnętrznych było więc 44% zdrajców. Tak stosunkowo niski odsetek wynikał z faktu, że w oddziałach stacjonujących na Krymie było 1265 żołnierzy zasadniczej służby wojskowej z Ukrainy właściwej, którzy w pełnym składzie wrócili do domu. Wśród kadry oficerskiej wojsk wewnętrznych, zwykle pochodzącej z Krymu i tam mieszkającej, odsetek zdrajców wyniósł natomiast 86%[26]. Na 1 marca 2014 r. na Krymie przebywało 1869 funkcjonariuszy Straży Granicznej, w tym 448 oficerów. Do kraju wróciło 479, w tym 226 oficerów. Odsetek zdrajców wyniósł zatem 74%, a wśród oficerów – 50%[27].

Dane ujęte w powyższych statystykach w rzeczywistości mogą być wyższe, gdyż część oficerów mogła wrócić do Ukrainy, aby wystąpić ze służby i przejść na emeryturę, a następnie wrócić do domu na Krymie i podjąć służbę dla Rosjan, zachowując jednocześnie ukraińskie świadczenia emerytalne.

силовиков в Крыму после аннексии, РБК-Україна, 6 XI 2017 r., https://www.rbc.ua/rus/news/tymchuk-nazval-chislo-predateley-sredi-ukrainskih-1509976026.html [dostęp: 4 VI 2023]; *Нарден Тымчук назвал число изменивших присяге крымских силовиков*, Black Sea News, 6 XI 2017 r., https://www.blackseanews.net/read/136189 [dostęp: 5 VI 2023].

[24] Wyliczenia podsumowujące wyniki deputackich zapytań pochodzą z oficjalnej strony D. Tymczuka w serwisie Facebook. Zob. https://www.facebook.com/dmitry.tymchuk/posts/1366726656789319 [dostęp: 9 VI 2023].

[25] Tamże.

[26] Tamże.

[27] Tamże.

Próby wyjaśnienia skali zdrady

W ukraińskich mediach próbowano racjonalnie wyjaśnić, dlaczego doszło do masowej zdrady ukraińskich żołnierzy i funkcjonariuszy. Przedstawiane hipotezy obejmowały kilka czynników, które mogły mieć znaczenie.

- Po pierwsze, ci, którzy zostali na Krymie, mieli tam rodziny, domy i majątki. Wyjazd z okupowanego półwyspu oznaczał utratę wszystkiego. Osłabione państwo ukraińskie nie zapewniało ludziom, którzy pozostali wierni przysiędze, zabezpieczenia materialnego po opuszczeniu Krymu[28].
- Po drugie, według spisu powszechnego w 2001 r. z 2,4 mln mieszkańców Krymu 60,40% było etnicznymi Rosjanami, 24,01% – narodowości ukraińskiej, a 10,11% –Tatarami[29]. Brakuje informacji na temat faktycznej przynależności do wspólnoty językowo-kulturowej, czyli danych mówiących o tym, ilu z krymskich Ukraińców i Tatarów było rosyjskojęzycznych. Można założyć, że struktura etniczna ukraińskich służb i wojska mogła odpowiadać tym odsetkom, przynajmniej w zakresie kadry zawodowej, rekrutującej się zapewne głównie z mieszkańców półwyspu szukających pracy w pobliżu miejsca zamieszkania. Krymscy Rosjanie – lojalni wobec kraju pochodzenia – mogli odrzucić obcą im państwowość ukraińską. Wyższy odsetek zdrajców niż wskazywałaby statystyka dotycząca głównych narodowości mógł być skutkiem np. niechęci do przyjmowania do służby Tatarów (uznawanych za element wywrotowy)[30], a zatem wybór pozostania w służbie mógł być pochodną narodowości. Czynnik etniczny mógł odgrywać główną rolę ze względu na to, że rosyjska propaganda straszyła ludność rosyjską i rosyjskojęzyczną Ukrainy groźbą czystki etnicznej ze strony działaczy Prawego Sektora[31].

---

[28] Tamże.

[29] *Про кількість та склад населення України за підсумками Всеукраїнського перепису населення 2001 року*, https://web.archive.org/web/20071124125111/http://www.ukrcensus.gov.ua/results/general/nationality/ [dostęp: 12 VI 2023].

[30] Zmieniałoby to strukturę narodowościową w resortach siłowych Krymu, gdyż odsetek Rosjan i zrusyfikowanych Ukraińców byłby wyższy niż w całej populacji.

[31] Por. *Корсуньская трагедия - боевики Майдана пытают крымчан, поджёг автобусов. 20.02.2014*, YouTube, 20 II 2017 r., https://www.youtube.com/watch?v=s2TGeF-xbTc&list=PLeuqEfNt-M8zle-TyjJ-n8DXE2Uz9OHm2Ty [dostęp: 23 II 2023]; *Документальный фильм «Корсуньский погром»*, YouTube, 30 VII 2014 r., https://www.youtube.com/watch?v=7FfPTBQ4l38 [dostęp: 22 II 2023]; *„Корсуньский погром": зверства сторонников майдана*, YouTube, 21 VI 2014 r., https://www.youtube.com/watch?v=hlf_AdGbfjE [dostęp: 22 II 2023]; *Корсуньская трагедия Убивали только за то, что они из Крыма 2014 весна*, YouTube, 27 V 2019 r., https://www.youtube.com/watch?v=bqUcM5YBWFw [dostęp: 23 II 2023].

- Po trzecie, Rosja na Krymie nie była państwem obcym. Rosyjska Flota Czarnomorska ściśle współpracowała z ZSU. Oficerowie tych formacji przyjaźnili się, spotykali, byli powiązani więziami koleżeńskimi i rodzinnymi. Przy podejmowaniu decyzji mogli więc stawiać na pierwszym miejscu relacje nieformalne (tj. rodzinno-przyjacielskie). Społeczeństwa Europy Wschodniej – w przeciwieństwie do Zachodu – mają tzw. charakter wspólnotowy, tj. wyżej cenią lojalność wobec członków rodzin i przyjaciół niż wobec państwa[32].
- Po czwarte, ludność Krymu była pod stałym wpływem rosyjskich mass mediów oraz generalnie wspierała prorosyjską Partię Regionów. Zarówno Rosja, jak i działacze Partii Regionów intensywnie propagowali narrację, zgodnie z którą przejęcie przez opozycję władzy w Kijowie było siłowym przewrotem finansowanym przez Zachód. Przy takiej percepcji tych wydarzeń politycznych wybór Rosji (do której uciekł obalony Janukowicz) mógł być postrzegany jako jedyna opcja walki z „puczystami" w sytuacji, gdy „legalny" prezydent uzyskał schronienie w FR.

Chociaż przedstawione hipotezy mają istotne znaczenie w próbach tłumaczenia opisywanych wydarzeń, to w żaden sposób nie wyjaśniają przyjęcia do FSB 86,4% funkcjonariuszy krymskiej SBU. Milicja, straż graniczna, prokuratura czy administracja cywilna są organami państwa o charakterze pozapolitycznym (przynajmniej teoretycznie), wręcz czysto technicznym i niezbędnym przy administrowaniu terenem zamieszkałym przez jakąś populację[33]. Może to powodować, że ich funkcjonariusze będą postrzegali służbę jako zawód, a państwo jedynie jako pracodawcę. Może to sprzyjać kolaboracji z okupantem, zwłaszcza jeśli tworzy on okupacyjną administrację na podstawie własnego systemu prawnego[34]. Siły okupacyjne mogą z kolei wykorzystywać już istniejące instytucje (wraz z ich kadrą), dysponujące wiedzą i doświadczeniem na danym terenie, traktując je pragmatycznie jako niezbędny element administracji, bez względu na przynależność państwową.

Służby specjalne stosują bardzo restrykcyjne metody naboru. Dążą do jak najlepszego rozpoznania przeszłości i sposobu życia kandydata (aby wyeliminować możliwość szantażu) oraz jego ewentualnych związków z grupami potencjalnie groźnymi dla nich. Najważniejsze jest ustalenie, czy kandydat nie pozostaje w kontakcie z obcą

---

[32] Na temat różnic między społeczeństwami wspólnotowymi a zrzeszeniowymi zob. F. Tönnies, *Wspólnota i stowarzyszenie*, Warszawa 1988.

[33] Przykładem zaczerpniętym z historii może być utworzenie przez Niemców jednostek policyjnych w Generalnym Gubernatorstwie (Polnische Polizei im Generalgouvernement), które były uzbrojone i finansowane przez polskie samorządy. Zob. szerzej: A. Hempel, *Policja granatowa w okupacyjnym systemie administracyjnym Generalnego Gubernatorstwa: 1939–1945*, Warszawa 1987.

[34] Za pomocą takiego argumentu bronili się po wojnie tzw. granatowi policjanci. Wskazywali na swoją „usługową" rolę wobec społeczeństwa polskiego, które chronili przed kryminalistami.

służbą specjalną oraz czy istnieją przesłanki mówiące o realnym ryzyku, że takie relacje mogłyby zostać nawiązane w przyszłości. Inaczej rzecz ujmując, warunkami sine qua non dopuszczenia do pracy w służbach specjalnych są brak tzw. ryzyka kontrwywiadowczego kandydata oraz jego lojalność wobec własnego państwa. W związku z tym nawet w czasie pokoju i wobec własnych obywateli stosuje się rozbudowane procedury sprawdzające. W warunkach quasi-wojennych i wobec obywateli obcego państwa rygor sprawdzeń kontrwywiadowczych powinien być znacznie większy. Zwłaszcza jeśli kandydaci już raz zdradzili swoją służbę oraz własne państwo i złamali przysięgę wierności składaną przez funkcjonariuszy resortów siłowych.

Jak zatem doszło do tego, że Rosjanie bez sprawdzenia przyjęli do służby w FSB 1400 funkcjonariuszy krymskiej SBU? Oznaczało to przecież, że będą oni mieli dostęp do systemów informatycznych FSB, tajemnic służbowych i państwowych oraz możliwość awansowania w hierarchii (nie tylko w jednostkach na Krymie, lecz także w centrali). Takie postępowanie jest sprzeczne z elementarnymi zasadami pracy służb specjalnych. Poszukując wyjaśnienia, można by założyć, że taką decyzję Rosjanie podjęli ze względu na niemożność stworzenia struktur bezpieczeństwa z powodu braku własnych kadr. Jednak FSB szacunkowo liczy od 200 000[35] do 350 000[36] funkcjonariuszy, z czego ok. 100 000–120 000 służy w Straży Granicznej[37]. Tak więc na samą służbę wewnętrzną przypada między 80 000 a 230 000 osób. Przy takim zasobie kadrowym oddelegowanie na Krym ok. 2000 funkcjonariuszy nie powinno stanowić problemu[38].

Hipoteza badawcza

Najbardziej prawdopodobnym wyjaśnieniem tego fenomenu jest założenie, że Rosjanie, przyjmując byłych oficerów SBU, nie musieli sprawdzać ich lojalności, gdyż od dłuższego czasu kadra krymskiej SBU była w kontakcie ze służbami specjalnymi FR. Jeśli ta współpraca była długa i wielokrotnie pozytywnie weryfikowana, to nie istniała potrzeba dodatkowego potwierdzania lojalności nowych funkcjonariuszy. Rosyjska agentura w SBU została po prostu masowo przejęta przez FSB.

Takie rozumowanie ma słabość metodologiczną polegającą na tym, że żadna służba wywiadowcza na świecie nie pozyskuje do współpracy niemal całego zasobu

[35] *Численность ФСБ*, https://fsb.dossier.center/number/ [dostęp: 12 VI 2023].

[36] B. Renz, *The Russian Force Structures*, „Russian Analytical Digest" 2007, nr 17, s. 6.

[37] *Численность ФСБ…*

[38] Tysiąc czterystu funkcjonariuszy krymskiej SBU, którzy podjęli służbę w rosyjskich strukturach, stanowiło między 0,4 a 0,7% liczby wszystkich etatów w FSB.

kadrowego przeciwnika. Byłoby to kontrskuteczne, gdyż nowe źródła przekazywałyby te same informacje i otrzymywały za to wynagrodzenie, a przy tym generowałyby konieczność rozbudowy własnych struktur wywiadowczych ze względu na obsługiwanie licznej agentury. Dlatego zmierza się do werbunku jedynie osób uplasowanych na tyle wysoko w strukturze przeciwnika, by móc pozyskiwać w ten sposób informacje zebrane od osób na niższych szczeblach hierarchii służbowej.

Podejmując próbę wyjaśnienia nietypowego sposobu działania rosyjskich służb w odniesieniu do krymskiej SBU, można odwołać się do wyników analiz, które wskazują na istotną różnicę między paradygmatem działania zachodnich i rosyjskich służb specjalnych polegającą na innych celach i metodach działania tych drugich służb. Metody te określa się jako ofensywność (ros. *наступательность*)[39].

Kontrwywiad ofensywny

Należy podkreślić, że sowiecko-rosyjska koncepcja kontrwywiadu różni się diametralnie od tej zachodniej. W myśl założeń pierwszej koncepcji kontrwywiad nie polega na pasywnej ochronie informacji wrażliwych przed działaniami służb wywiadowczych przeciwnika, lecz na aktywnym opanowaniu wywiadu i kontrwywiadu przeciwnika przez plasowanie w tych strukturach własnych agentów („kretów") oraz podsuwanie podwójnych agentów. Na tym jednak rosyjska koncepcja aktywnego kontrywiadu się nie wyczerpuje. Wśród metod pracy operacyjnej kontrwywiadu opisywanych przez rosyjskich autorów zajmujących się działalnością sowieckich służb specjalnych[40] zawsze pojawia się pojęcie *разложение противника*. Pomimo częstego używania tego terminu w pracach rosyjskich historyków brakuje jego definicji, a jednocześnie taki sposób działania traktuje się jako oczywisty atrybut czekistowskiego warsztatu operacyjnego. Przekładając to pojęcie na język polski, należałoby mówić o dezorganizacji, rozkładzie czy też o systemowej destabilizacji wrogiej organizacji.

[39] „Наступательность – образ действий контрразведки обеспечивающий активность и инициативу, достижение максимальных успехов в борьбе с противником. Н. – представляет собой организационно-технический принцип, которым стремятся руководствоваться разведывательные и контр разведывательные органы в своей деятельности. В соответствии с ним сторона действующая наступательно, достигает при прочих равных условиях найлучших результатов" (Ofensywność to sposób działania kontrwywiadu zakładający przejęcie aktywności i inicjatywy, pozwalający osiągnąć maksymalny sukces w walce z wrogiem. Ofensywność – reprezentuje zasadę organizacyjną i techniczną, którą agencje wywiadu i kontrwywiadu starają się kierować w swoich działaniach. Zgodnie z nią najlepsze rezultaty osiąga strona grająca ofensywnie). Zob. *Контрразведывательный словарь*, Москва 1972, s. 171. Tłumaczenia w artykule pochodzą od autora (dop. red.).

[40] W kontekście infiltracji agenturalnej, opanowania kanałów łączności.

Czasem bywa ono używane w rozwiniętej formie – *разложение на корню*, co należy rozumieć jako całkowity, systemowy paraliż organizacji wojskowo-wywiadowczej przeciwnika, uniemożliwiający jakiekolwiek skuteczne działania zaczepno-obronne[41].

Takie podejście do pracy sowiecko-rosyjskich służb specjalnych wynika z założeń teoretycznych sformułowanych na początku lat 20. XX w. przez Aleksandra Kuka, zastępcę naczelnika wydziału agenturalnego wywiadu wojskowego ZSRR Razwiedupr. Główne z nich głosiło, że: *Wywiad tajny nabrał charakteru aktywnego. Ta cecha wywiadu tajnego, jako nosząca znamiona terroryzmu, dezorganizacji życia państwowego i systemu wojskowego strony przeciwnej okazuje się nadzwyczaj ważna i ukazuje wywiad w zupełnie innym świetle niż przed wojną światową*[42]. Zgodnie z tym założeniem wywiad przestał polegać jedynie na zbieraniu informacji wojskowych lub politycznych o przeciwniku, lecz stał się wielowątkową działalnością zmierzającą do możliwie pełnej dezorganizacji aparatu państwowego przeciwnika. Innymi słowy, opisane *разложение противника* było praktycznym zastosowaniem teoretycznych rozważań Kuka, który postulował aktywne paraliżowanie struktur państwowych przeciwnika zamiast pasywnego zbierania informacji o nim.

Na temat rosyjskich metod dezorganizowania wroga – pomimo braku szczegółowych opisów w rosyjskim piśmiennictwie – można wnioskować na podstawie „wykładni" zawartej w okólniku rozesłanym 11 sierpnia 1937 r. przez kierującego Ludowym Komisariatem Spraw Wewnętrznych ZSRR (Народный комиссариат внутренних дел СССР, NKWD) Nikołaja Jeżowa[43]. Pismo to było de facto wyrokiem śmierci dla polskich komunistów pracujących w aparacie partyjno-państwowym ZSRS[44], oskarżanych o przynależność do siatki wywiadowczej pod nazwą Polska Organizacja Wojskowa (POW). Charakteryzując (rzekomą) działalność POW mającą szkodzić interesom ZSRS, Jeżow wymieniał następujące przejawy aktywności:

- infiltracja sowieckiej administracji, aparatu politycznego, gospodarki, armii (głównie kadry średniego i wyższego szczebla), NKWD, aparatu partyjnego oraz Kominternu;

[41] Warto dodać, że „rozkładanie" organizacji przeciwnika – jako termin neutralny konotacyjnie – było nazwą zarezerwowaną dla działań zaczepnych sowieckich służb specjalnych. To samo działanie obcych służb nakierowane na ZSRS określano pejoratywnie nacechowanym słowem *вредительство* (szkodnictwo).

[42] A.I. Kuk, *Kanwa wywiadu agenturalnego*, Warszawa 1994, s. 16.

[43] Nikołaj Iwanowicz Jeżow (ur. w 1895 r., rozstrzelany w 1940 r.) – radziecki działacz partyjny i państwowy, Ludowy Komisarz Bezpieczeństwa Państwowego w latach 1936–1938 odpowiedzialny za realizację stalinowskiego terroru w trakcie tzw. wielkiej czystki (nazwanego od jego nazwiska „jeżowszczyzną").

[44] *Оперативный приказ Народного комиссара внутренних дел Союза ССР Николая Ежова № 00485. 11 августа 1937 г. о польской национальной операции*, https://operacja-polska.pl/nkr/o-operacji-polskiej-nkw/dokumenty/966,00485-11-1937.html [dostęp: 22 X 2019].

- ulokowanie agentów na kluczowych stanowiskach w wywiadzie i kontrwywiadzie (cywilnym i wojskowym) w celu paraliżowania działalności organów mogących wykryć masową infiltrację;
- organizowanie przez polski wywiad systematycznej pracy werbunkowej z wykorzystaniem wysokich pozycji w aparacie państwowym ZSRS, w celu osłabiania na każdym możliwym polu zdolności obronnych ZSRS.

Z treści pisma Jeżowa wynika, że taktyka rozkładania aparatu sowieckiego miała się składać z trzech następujących po sobie etapów:

1) punktowej infiltracji kluczowych miejsc aparatu sowieckiej republiki (chodziło głównie o stanowiska kierownicze w służbach specjalnych, Robotniczo-Chłopskiej Armii Czerwonej, administracji, partii i gospodarce[45]);
2) wsparcia dalszej, niemal masowej infiltracji na niższych szczeblach organizacyjnych przez uplasowane w newralgicznych miejscach „krety"[46];
3) stworzenia rozległej sieci agenturalnej oplatającej gospodarkę oraz polityczno-militarną nadbudowę państwa, której to członkowie – za pomocą trudnych do udowodnienia działań z uwagi na stosowanie maskowania – usiłowali wszelkimi sposobami szkodzić państwu sowieckiemu[47].

[45] Por. „(…) уже определилось, что антисоветской работой организации были охвачены – система НКВД, РККА, Разведупр РККА, аппарат Коминтерна – прежде всего польская секция ИККИ, наркоминдел, оборонная промышленность, транспорт – преимущественно стратегические дороги западного театра войны, сельское хозяйство" (…ustalono już, że antyradziecką pracą tej organizacji były objęte – system NKWD, Armia Czerwona, Departament Wywiadu Armii Czerwonej, aparat Kominternu – przede wszystkim polska sekcja Komitetu Wykonawczego Kominternu, Komisariat Ludowy Spraw Zagranicznych, przemysł obronny, transport – głównie drogi strategiczne zachodniego teatru działań wojennych, rolnictwo). Cyt. za: *Закрытое письмо*…

[46] Por. „Массовая фашистско-националистическая работа среди польского населения СССР в целях подготовки базы и местных кадров для диверсионно-шпионских и повстанческих действий" (Masowa praca faszystowsko-nacjonalistyczna wśród polskiej ludności w ZSRR w celu przygotowania bazy i lokalnego personelu do działań dywersyjnych, szpiegowskich i powstańczych). Cyt. za: *Закрытое письмо*…

[47] Por. „Глубокое внедрение участников организации в компартию Польши, полный захват в свои руки руководящих органов партии и польской секции ИККИ, провокаторская работа по разложению и деморализации партии, срыв единого и народного фронта в Польше, использование партийных каналов для внедрения шпионов и диверсантов в СССР, работа, направленная к превращению компартии в придаток пилсудчины с целью использования ее влияния для антисоветских действий во время военного нападения Польши на СССР" (Głębokie przeniknięcie członków organizacji do Komunistycznej Partii Polski, całkowite przejęcie kierowniczych organów partii i polskiej sekcji Komitetu Wykonawczego Kominternu, prowokacyjna praca na rzecz rozkładu i demoralizacji partii, rozbicie jednolitego i ludowego frontu w Polsce, wykorzystywanie kanałów partyjnych do wprowadzania do ZSRR szpiegów i dywersantów, praca mająca na celu przekształcenie Komunistycznej Partii Polski w dodatek piłsudczyzny w celu wykorzystania jej wpływów do działań antyradzieckich podczas polskiego ataku militarnego na ZSRR). Cyt. za: *Закрытое письмо*…

> Działania te polegały na korumpowaniu i demoralizowaniu sowieckich urzędników, propagowaniu szkodliwych rozwiązań w przemyśle i rolnictwie, prowadzących do rozproszenia i marnotrawstwa środków budżetowych, lobbowaniu za nieskutecznymi lub kontrskutecznymi metodami działania służb specjalnych, administracji i armii (na poziomie zarówno taktycznym, jak i strategicznym[48]).

W historiografii okólnik Jeżowa był traktowany albo jako przejaw powszechnej psychozy panującej w sowieckim aparacie władzy, albo jako dowód cynizmu autora, który chciał zapewnić sobie karierę za pomocą masowych egzekucji zdolniejszych kolegów i dzięki uznaniu ze strony Stalina, cierpiącego podobno na zaawansowaną paranoję. Czasem wysuwano tezę o rzekomym antypolonizmie władz sowieckich, który miał być dziedzictwem czasów carskich.

W procesie wyjaśniania należy sięgnąć – nie wchodząc w rozważania na temat niepotwierdzonego (z powodu braku diagnozy) obłędu Stalina i przyjmując, że sama liczba Polaków zajmujących w ZSRR kierownicze stanowiska[49] falsyfikuje teorie o sowieckim antypolonizmie – do starannie udokumentowanych ustaleń z zakresu psychologii poznawczej, w ramach której zostało opisane zjawisko projekcji jako możliwe wyjaśnienie akcji wymierzonej w POW.

---

[48] Por. „Полный захват и парализация всей нашей разведывательной работы против Польши и систематическое использование проникновения членов организации в ВЧК–ОГПУ–НКВД и Разведупр РККА для активной антисоветской работы. Основной причиной безнаказанной антисоветской деятельности организации в течение почти 20 лет является то обстоятельство, что почти с самого момента возникновения на важнейших участках противопольской работы сидели проникшие в ВЧК крупные польские шпионы (…)" (Całkowite przejęcie i paraliż całej naszej pracy wywiadowczej przeciwko Polsce oraz systematyczne infiltrowanie Czeka-OGPU-NKWD i Zarządu Wywiadu RKKA za pomocą członków organizacji w celu aktywnej pracy antyradzieckiej. Główną przyczyną bezkarnej antysowieckiej działalności tej organizacji przez prawie 20 lat jest fakt, że niemal od samego początku jej istnienia w najważniejszych obszarach antypolskiej pracy działali znaczący polscy szpiedzy, którzy przedostali się do Czeki…). Cyt. za: *Закрытое письмо…*

[49] Minimum 17% aparatu kierowniczego (średniego i wyższego szczebla) NKWD składało się z etnicznych Polaków. W rzeczywistości element polski w NKWD był dużo liczniejszy, gdyż w sowieckim aparacie państwowym pracowała duża liczba ludzi wywodzących się ze spolszczonych rodzin żydowskich, białorusko-litewskich bądź ukraińskich. W ankietach personalnych wpisywali oni jednak – by podkreślić proletariackie korzenie – swoje etniczne pochodzenie, przemilczając związki z językiem polskim i polską kulturą. Sowieci zdawali sobie z tego sprawę. W raportach NKWD dotyczących „operacji" polskiej skrupulatnie informowali, że aresztowano 20 311 Polaków i – w ramach tej operacji – ponad 17 000 przedstawicieli innych nacji (głównie Białorusinów i Żydów). Gdyby te proporcje przełożyć na podany wyżej odsetek Polaków w kierownictwie NKWD, mogłoby to oznaczać, że niemal 1/3 aparatu kierowniczego tej instytucji miała związki z językiem polskim i polską kulturą. Za: А. Зданович, *Польский крест советской контрразведки. Польская линия в работе ЧК-НКВД. 1918-1938*, Москва 2017, s. 169–170, 311–312.

Mechanizm projekcji jako hipoteza tłumacząca działania NKWD

Projekcja na gruncie psychologii jest rozumiana jako mechanizm obronny osobowości polegający na przypisywaniu innym własnych motywacji, poglądów, cech i zachowań. Powszechność występowania zjawiska projekcji wynika z tego, że jednostka projektująca zazwyczaj ma dostęp tylko do własnych myśli, uczuć i zachowań[50], za pomocą których tłumaczy zachowania innych osób[51] (nie da się bowiem w procesie rozumienia innych odwoływać do emocji, przekonań i wiedzy, których się nie ma[52]).

Jeśli przyjmie się, że sowieckie służby masowo infiltrowały obce służby i paraliżowały ich aktywność za pomocą agentury, to – zgodnie z heurystyką dostępności[53] – funkcjonariusze NKWD byli przekonani, że wrogie wywiady robią to samo wobec nich. Kierownictwo NKWD, rozkładając zachodnie aparaty władzy za pomocą „kretów", agentów wpływu i podwójnej agentury, wierzyło, że jest ofiarą symetrycznych działań ze strony przeciwników, realizowanych zbliżonymi metodami i w podobnej skali.

Model infiltracji Jeżowa jako wyjaśnienie masowych zdrad w krymskiej SBU

Jeśli na podstawie powyższych rozważań przyjmie się, że sowieckie służby, a następnie ich kontynuatorki w FR stosowały metody ujawnione przez Jeżowa, to masowa skala zdrady w aparacie państwowym Ukrainy oraz bezproblemowe wchłonięcie przez FSB kadry krymskich służb specjalnych stają się zrozumiałe. Skoro celem rosyjskich służb – zgodnie z opisaną wcześniej metodyką – nie jest pozyskiwanie informacji, lecz przejęcie kontroli nad instytucjami wrogiego państwa w celu sparaliżowania ich działalności za pośrednictwem siatki agentów przenikającej niemal wszystkie szczeble organizacyjne, to masowość werbunków staje się logiczna.

---

[50] Próbą uniknięcia projekcji jako czynnika fałszującego poznanie w naukach społecznych jest rygorystyczne stosowanie metodologii oraz wielość perspektyw poznawczych badacza. Heurystyka dostępności nadal pozostaje jednak głównym źródłem błędów poznawczych. Por. D. Kahneman, P. Slovic, A. Tversky, *Judgment under uncertainty: heuristics and biases*, New York 1982.

[51] Por. T. Kobierzycki, *Filozofia osobowości*, Warszawa 2001, s. 153. Zob. szerzej: A. Freud, *Das Ich und die Abwehrmechanismen,* Wien 1936; O.F. Kernberg, *Borderline Conditions and Pathological Narcissism,* London 1990; K. König, *Abwehrmechanismen*, Göttingen–Zürich 2007; S. Mentzos, *Interpersonale und institutionalisierte Abwehr*, Frankfurt am Main 1994.

[52] To zjawisko jest znane także w tzw. psychologii naiwnej, np. jako przekonanie, że złodzieje wierzą w to, że wszyscy kradną.

[53] Nawykowe odwoływanie się do własnych doświadczeń, emocji i przekonań.

Głównym mechanizmem infiltracji, opisanym przez Jeżowa, było kumoterstwo. Wykorzystując mechanizmy korupcyjne, można było wprowadzać agenturę na niższe szczeble z pomocą „kretów", których wcześniej uplasowano wysoko w hierarchii. Ulokowani agenci musieli otaczać się kolejnymi agentami lub ludźmi w pełni kontrolowanymi i pozbawionymi inicjatywy, aby zabezpieczyć się przed demaskacją przez podwładnych i kolegów. Tym sposobem uagenturowienie i współudział (choćby w formie biernej) schodziły na coraz niższe szczeble atakowanej organizacji.

Znane z obszaru postsowieckiego zjawisko masowych urzędniczych sitw, którym to klikom towarzyszy bierność nienależących do nich osób, ale w pełni im lojalnych ze strachu czy dla własnego interesu, wyjaśnia skuteczność metody nakreślonej przez Jeżowa. Tłumaczy również przyjęcie do FSB niemal 1500 byłych funkcjonariuszy SBU bez ich sprawdzenia. Jeżeli przyjmie się, że w krymskiej SBU były sieci agenturalne sięgające od szczytu do dołu hierarchii oraz że każdy szczebel zabezpieczał swoje bezpieczeństwo, wprowadzając nową agenturę oraz zastraszając i uzależniając od siebie pracowników formalnie niewspółpracujących z Rosjanami, to przejęcie przez Rosję całego zespołu, w pełni kontrolowanego agenturalnie, nie wiązało się z wysokim stopniem ryzyka kontrwywiadowczego.

Z tego wynika, że agenturalny model opanowania instytucji przeciwnika obejmuje dwa najważniejsze elementy:

1) tworzenie za pomocą mechanizmów kumoterskich rozgałęzionych sieci agenturalnych złożonych głównie z kadry zarządczej wszystkich szczebli,
2) klientelistyczne uzależnienie szeregowych pracowników od zinfiltrowanej kadry, aby uzyskać pełną kontrolę nad ich poczynaniami i związać ich z powstałym systemem.

Mechanizm uzależniania podwładnych przez skorumpowaną kadrę nadzorczą jest także powszechny w postsowieckiej rzeczywistości[54]. Składają się na niego:

- selekcja negatywna zarządzanego personelu, polegająca na usuwaniu z zespołu wszystkich niezależnie myślących i samodzielnych pracowników, którzy nie są skłonni do akceptacji niejawnych hierarchii i klientelistycznych zależności;
- podważanie zaufania podwładnych do oficjalnych regulacji przez rozbudowę nieoficjalnych, pozaprawnych sieci relacji oraz zależności, w pełni regulujących stosunki panujące w instytucji i zastępujących prawne podstawy jej funkcjonowania;

[54] Szerzej na temat mechanizmów uzależniania personelu od nieformalnych relacji w służbach specjalnych zob. Г.С. Водолеев, С.Ф. Сидоренко, *Спецнужды и спецслужбы*, Москва 2009.

- całkowity paraliż obiektywnej polityki kadrowej, wskutek czego awans zależy wyłącznie od przełożonych, a nie od indywidualnych umiejętności czy wkładu pracy;
- korupcja, która – poprzez współuczestnictwo podwładnych – wiąże ich z nieoficjalną strukturą zarówno z powodu chęci partycypacji w zyskach, jak i z obawy przed konsekwencjami prawnymi w razie ujawnienia[55].

Ostatni czynnik jest najważniejszy, gdyż korupcja (rozumiana szeroko jako wykorzystanie funkcji publicznej w celu realizacji własnych interesów) jest warunkiem sine qua non wszystkich pozostałych elementów. Obserwacje dotyczące mechanizmów funkcjonujących w ukraińskich strukturach państwowych w czasie ostatniego konfliktu z FR potwierdzają istnienie zależności między zdradą (czyli podjęciem współpracy z rosyjskimi służbami) a wcześniejszą korupcją[56].

Korupcja w krymskiej SBU

Według badań Transparency International Ukraine (Трансперенсі Інтернешнл Україна, TIU), w 2022 r. Ukraina lokowała się pod względem korupcji na 116 miejscu spośród 180 państw świata[57]. W Europie była najbardziej skorumpowanym państwem. Warto przy tym odnotować, że wyniki badań TIU nie do końca oddają skalę zjawiska, gdyż wiele rodzajów korupcji (np. kumoterstwo, faworytyzm czy nepotyzm) nie jest w Ukrainie w ten sposób postrzegane. Traktuje się je jako mechanizmy

[55] Niepoinformowanie o korupcji już jest przestępstwem urzędniczym, więc bierność wynikająca z bezsilności wobec układu staje się skutecznym elementem wiążącym z nieformalnym, agenturalnie tworzonym systemem.

[56] Por. *Генерал-коллекционер СБУ Свиридонов друг Куницына*, ОРД, 20 XII 2009 r., https://ord-ua.com/2009/12/29/general-kollektsioner-sbu-sviridonov-drug-kunitsyina/ [dostęp: 15 VI 2022]; W. Samar, *Russian «moles» in the State Security Service of Ukraine: what is missing in the Kulinich-Sivkovych' case?*, Center of Journalistic Investigations, 26 IV 2023 r., https://investigator.org.ua/investigations/253973/ [dostęp: 16 VI 2023]; *Генерал Кривонос: про зраду в 2014-му, Порошенка, Зеленського, «клоунів» у РНБО і силове звільнення Донбасу*, Радіо Свобода, 19 I 2020 r., https://www.radiosvoboda.org/a/rnbo-kryvonos-donbass-zrada-peremoga/30384758.html [dostęp: 15 VI 2023]; *Корупція та зрада - це неприпустимі речі. І у професійному, і в людському плані. Це не можна пробачати», - Ігор Клименко*, 7 II 2023 r., https://mvs.gov.ua/uk/news/korupciia-ta-zrada-ce-nepripustimi-reci-i-u-profesiinomu-i-v-liudskomu-plani-ce-ne-mozna-probacati-igor-klimenko [dostęp: 15 VI 2023]. Zob. szerzej: A. Савченко, *Антиукраїнець: або Воля до боротьби, поразки чи зради*, Київ 2020.

[57] Transparency International Ukraine, https://www.transparency.org/en/countries/ukraine [dostęp: 16 VI 2023].

społecznie oczywiste[58]. Można zatem zaryzykować hipotezę, że powyższe badania pokazują jedynie skalę łapówkarstwa, a nie korupcji jako złożonego zjawiska.

Służba Bezpieczeństwa Ukrainy od momentu utworzenia, na bazie republikańskiego Komitetu Bezpieczeństwa Państwowego (Комитет государственной безопасности, KGB), była instytucją z predyspozycją do dysfunkcji[59]. Z jednej strony była poddana polityzacji (rozumianej jako aktywne wsparcie politycznych klanów), z drugiej – stałej presji oligarchicznego kapitalizmu, który ściągał najlepszych oficerów do pracy w sektorze prywatnym i z ich pomocą korumpował całą strukturę. Krym był oddalony od centrali w Kijowie i miał specjalny status, a przy tym oferował duże możliwości włączenia się w powszechne rozkradanie majątku państwowego[60], co sprzyjało rozkwitowi korupcji.

W analizie zostanie uwzględniony jedynie okres od 2000 r., kiedy to powoli zaczynała się kończyć anomia lat 90. XX w. spowodowana rozpadem ZSRR. W tym czasie (tj. od 2000 r. do 2014 r.) krymską SBU kierowali kolejno: gen. Aleksandr Swiridonow, gen. Władimir Pszenicznyj, gen. Aleksandr Jakimienko, gen. Władimir Tockij i gen. Giennadij Kołaczew. Podczas 14 lat ich rządów doszło do wielu skandali związanych ze sprzedażą nieruchomości SBU za łapówki[61], rozbudową korupcyjnych relacji z lokalnym biznesem, przestępczością zorganizowaną, administracją, jak również z tzw. kryszowaniem[62] dochodowych firm, rabunkiem stanowisk archeologicznych[63] oraz prowadzeniem firm ochroniarskich we współpracy z bandytami i z International Bodyguard Association, której interesy na obszarze

[58] Badani Ukraińcy odnosili się do korupcji traktowanej jako łapówka. Rzeczywisty poziom korupcji jest zatem zdecydowanie wyższy.

[59] Służba Bezpieczeństwa Ukrainy w związku z masowym odpływem zdolnych funkcjonariuszy składała się niemal wyłącznie z ludzi niemogących odnaleźć się w rynkowej rzeczywistości oraz z garstki oficerów, którym brakowało jedynie kilku lat do emerytury. Niskie zarobki oraz uwarunkowania wynikające z dzikiego kapitalizmu lat 90. XX w. doprowadziły do wysokiego poziomu korupcji. Por. *Генерал-коллекционер СБУ Свиридонов*…

[60] W momencie odłączenia od ZSRR Ukraina miała nieformalny status dziesiątej gospodarki świata, dysponując zarówno żyznym czarnoziemem, jak i przemysłem ciężkim. Trzy dekady później była najuboższym państwem Europy. Zob. *Map of sovereign states in Europe by projected 2023 GDP (PPP) per capita based on international dollars*, https://en.wikipedia.org/wiki/List_of_sovereign_states_in_Europe_by_GDP_(PPP)_per_capita [dostęp: 12 III 2024].

[61] W tym nie tylko budynków polikliniki i przedszkola, lecz także mieszkań kontaktowych wykorzystywanych w pracy operacyjnej. Za: *Генерал-коллекционер СБУ Свиридонов*…

[62] Kryszowanie (ros. *крышевание*) – szeroko pojmowana protekcja oferowana firmom w zamian za haracz lub udział w zyskach.

[63] Na Krymie tzw. czarna archeologia stała się dochodowym biznesem. Kierownictwo SBU początkowo poprzestawało na kradzieży części zatrzymanych artefaktów, a potem przeszło do nielegalnych wykopalisk przy pomocy żołnierzy z oddziału ALFA. Za: *Генерал-коллекционер СБУ Свиридонов*…

postsowieckim reprezentował były pułkownik KGB Josif Linder. Obsada kadrowa krymskiej SBU była poddana stałej selekcji negatywnej, gdyż zmuszano do odejścia nie tylko niepokornych, lecz także kompetentnych oficerów, którzy byliby w stanie zrozumieć charakter tworzonych nielegalnych schematów korupcyjnych[64]. W służbie starano się pozostawić jedynie funkcjonariuszy biernych i w jakimś stopniu uwikłanych w nielegalne interesy kierownictwa.

W prasie pojawiały się informacje na temat zarówno powszechnej korupcji i związków (traktowanych jako oczywiste[65]) krymskiej SBU z rosyjskimi służbami[66], jak i silnego wpływu tureckich służb specjalnych na krymską SBU, mających ją korumpować za pośrednictwem kierownictwa tatarskiego Medżlisu[67]. Brakuje informacji pozwalających na rozstrzygnięcie, czy był to efekt wielostronnej sprzedajności ukraińskich oficerów w celu maksymalizowania zysków, czy też rosyjskie służby specjalne wykorzystywały agenturę w SBU do prowadzenia gier operacyjnych z tureckim wywiadem.

Nawet pobieżny przegląd doniesień medialnych z omawianego okresu wskazuje na zupełną anomię SBU na Krymie[68], wynikającą ze splotu korupcyjnych wpływów, infiltracji przez obce służby specjalne, styku z przestępczością zorganizowaną i lokalnymi sitwami polityczno-gospodarczymi. Istniały więc wszelkie przesłanki do tego, by kadrę krymskiej SBU, zdemoralizowaną korupcją, podlegającą selekcji

---

64 Tamże.

65 Wszyscy kierujący krymską SBU w przeszłości byli albo w KGB, albo w armii radzieckiej. W związku z tym kontakty z kolegami z dawnej służby (zwłaszcza gdy służyli we Flocie Czarnomorskiej) nie były przez nikogo kwestionowane.

66 W. Samar, *Russian «moles»*…

67 Por. *Закрытый доклад СБУ: на турецкие деньги «меджлис» вел разведку для Анкары*, EADaily, 7 IV 2016 r., https://eadaily.com/ru/news/2016/04/07/zakrytyy-doklad-sbu-na-tureckie-dengi-medzhlis-vel-razvedku-dlya-ankary [dostęp: 16 VI 2023].

68 Por. *Коррупция - СТОП! Прокуратура признала действия СБУ не соответствующими законодательству*, LB.ua, 23 V 2011 r., https://lb.ua/news/2011/05/23/97705_korruptsiya_stop_prokuratura_priz.html [dostęp: 16 VI 2023]; М. Галеотти, *«Сейлем» и «Башмаки». Крым и криминал до и после российской аннексии*, Крым.Реалии, 27 X 2014 r., https://ru.krymr.com/a/26658454.html [dostęp: 16 VI 2023]; *Агрессивный крымский боевик Самвел оказался спецагентом Кремля и мог работать в СБУ*, TCH, 20 V 2014 r., https://tsn.ua/ru/politika/agressivnyy-krymskiy-boevik-samvel-okazalsya-specagentom-kremlya-i-mog-rabotat-v-sbu-366551.html [dostęp: 16 VI 2023]; *Новые русские бандиты: кто контролирует Крым*, Україна Кримінальна, 24 III 2014 r., https://cripo.com.ua/investigations/?p=172293/ [dostęp: 16 VI 2023]; *Милиция и СБУ закупили машин на 30 миллионов*, bigmir)net, 15 XII 2010 r., https://auto.bigmir.net/autonews/autoworld/5217854-miliciya-i-sbu-zakupili-masin-na-30-millionov [dostęp: 16 VI 2023]; *Агенты национальной опасности*, dsnews.ua, 28 X 2013 r., https://www.dsnews.ua/economics/agenty-natsionalnoy-opasnosti-28102013090200 [dostęp: 16 VI 2023].

negatywnej i samowoli przełożonych, poddać pełnej kontroli ze strony sieci agenturalnej tworzonej przez FSB.

Podsumowanie

Punktem wyjścia podjętych rozważań było pytanie o możliwe przyczyny bardzo wysokiego odsetka funkcjonariuszy państwa ukraińskiego, którzy w 2014 r. przeszli na stronę Rosjan. Głównym problemem badawczym było – sprzeczne z zasadami regulującymi funkcjonowanie służb specjalnych – przyjęcie do rosyjskiego FSB 1400 funkcjonariuszy krymskiej SBU. Żadna służba nie przyjęłaby bowiem w swoje szeregi setek oficerów służby wrogiego państwa (w dodatku w stanie niewypowiedzianej wojny z nim), zwłaszcza gdy złamali oni przysięgę wierności złożoną w poprzednim miejscu. Wobec funkcjonariuszy SBU deklarujących gotowość pracy w FSB powinny zostać zastosowane wszystkie dostępne procedury sprawdzania lojalności tzw. oferentów (tj. ludzi samorzutnie proponujących służbom specjalnym swoje usługi)[69]. Autor uznał, że jedynym logicznym wyjaśnieniem tego fenomenu jest to, że Rosjanie de facto nie przyjęli do swojej służby neofitów ruskiego miru, lecz ukadrowili agenturę, która wcześniej – poprzez działanie na rzecz Rosji – w pełni udowodniła swoją lojalność. Ponieważ hipotetyczna masowość werbunków stała w sprzeczności z ekonomiką działań wywiadowczych, autor sięgnął w procesie wyjaśniania do koncepcji wywiadu aktywnego sowieckiego teoretyka z lat 20. XX w. oraz – posługując się dorobkiem psychologii poznawczej – zrekonstruował sowiecką metodę masowej infiltracji instytucji przeciwnika w celu wczesnego paraliżowania jej działań zaczepno-obronnych oraz wszelkich prób usprawniania i reformowania zainfekowanej agenturalnie organizacji.

Z przeprowadzonych analiz wynika, że wyjaśnieniem wskazanego fenomenu jest najprawdopodobniej infiltracja na dużą skalę ukraińskich służb na Krymie przez FSB. Autor przyjął, że – zgodnie z opisaną metodyką sowieckiej infiltracji – głównymi mechanizmami leżącymi u podstaw takiego ataku były rozpowszechnione kumoterstwo i nepotyzm oraz immanentna korupcja panujące w zaatakowanej służbie. Wykorzystując te patologie, można bowiem relatywnie łatwo budować pionowe sieci agenturalne i jednocześnie (na skutek współuczestnictwa w korupcji i usuwania osób niezależnie myślących) uzależniać niezwerbowaną część kadry. Wszystkie te czynniki wystąpiły w ogromnym nasileniu w krymskiej SBU, co ułatwiło Rosjanom przejęcie kontroli nad tą instytucją na długo przed aneksją półwyspu.

[69] Zob. szerzej: I.A. Serov, *Work with Walk-ins*, „Studies in Intelligence" 1962, t. 8, nr 1; F. Begoum, *You and Your Walk-In*, „Studies in Intelligence" 1962, t. 6, nr 1.

Można domniemywać, że grupowe przejęcie przez FSB funkcjonariuszy krymskiej SBU zostało zrealizowane w celach propagandowych, gdyż – z punktu widzenia logiki operacyjnej – dla Rosji korzystniejsze byłoby przeniesienie agentury z krymskiej SBU do centrali w Kijowie lub regionalnych jednostek SBU, zwłaszcza z terenów przylegających do strefy działań kinetycznych na Donbasie. Zapewne rolę odegrała też obawa przed procesami karnymi wobec funkcjonariuszy państwa ukraińskiego pracujących na Krymie, których można było oskarżyć jeśli nie o zdradę, to o niedopełnienie obowiązków. Lepszym rozwiązaniem było zatem pozostawienie agentury na półwyspie, aby wykorzystać ją do akcji propagandowej, przy jednoczesnym przerzuceniu do Ukrainy właściwej agentów uplasowanych wsród żołnierzy, funkcjonariuszy i urzędników, którzy wracali do ojczyzny w aurze ukraińskich patriotów[70].

Jeśli hipoteza postawiona w artykule jest prawdziwa, to należy przyjąć, że operacja krymska była de facto operacją służb specjalnych, z jedynie pomocniczą rolą sił zbrojnych. Działania kinetyczne w postaci interwencji armii FR (najpierw maskowanej, potem jawnej) mogły być jedynie końcowym akordem wieloletniego procesu masowej infiltracji i rozkładania instytucji cywilno-wojskowych przeciwnika. Biorąc pod uwagę przytoczone na początku artykułu statystyki unaoczniające skalę zdrady, można zaryzykować hipotezę, że wojska użyto jedynie po to, aby zamaskować rzeczywisty, ukryty mechanizm aneksji. Rosja bowiem – opierając się na masowo zinfiltrowanych ukraińskich strukturach państwowych – mogła zainscenizować „samorzutną" secesję Krymu w sytuacji siłowego przejęcia władzy przez opozycję w Kijowie. Wystarczyłoby przeprowadzić *inscenirowkę*[71] z wykorzystaniem masowych protestów, przyłączenia do nich lokalnej administracji i ogłoszeniem secesji przez krymski parlament. Dzięki ustaleniom Tymczuka wiadomo, że wszystkie instytucje siłowe na Krymie były w pełni kontrolowane przez rosyjską agenturę. Nie było zatem realnej siły, która mogłaby powstrzymać „ludowe referendum", jeśli zostałoby przeprowadzone przez w pełni kontrolowany agenturalnie lokalny parlament. Użycie uzbrojonych formacji FR było wręcz przeszkodą w legitymizacji aneksji, dając Zachodowi pretekst do uznania referendum za nieważne.

Najważniejszym wnioskiem płynącym z powyższej analizy jest konstatacja, że Rosjanom udało się zająć Krym nie na skutek interwencji wojskowej, lecz w drodze systemowej infiltracji i agenturalnego rozkładania instytucji przeciwnika. Taka taktyka agresji jako przedłużenia polityki jest rozwinięciem założeń sowieckich

[70] Identyczną metodę działania stosowało sowieckie GPU podczas wielkich operacji dezinformacyjnych realizowanych w latach 20. i 30. XX w. Zob. szerzej: M. Świerczek, *Jak Sowieci przetrwali dzięki oszustwu. Sowiecka decepcja strategiczna*, Warszawa 2021.

[71] Inscenirowka (ros. *инсценировка*) – gra na potrzeby obcych służb prowadzona przez agenturę i funkcjonariuszy własnej służby.

teoretyków z okresu największych operacji dezinformacyjnych oraz antycznej, chińskiej myśli wojskowej, wskazującej na możliwość odniesienia strategicznego zwycięstwa bez konieczności prowadzenia działań militarnych, jedynie za pomocą systemowego korumpowania i werbowania oficerów i urzędników wrogiego państwa[72].

Problemy badawcze wynikające z powyższej analizy można ująć w postaci dwóch pytań: 1) dlaczego Rosjanie – po aneksji Krymu i częściowym oderwaniu Donbasu od Ukrainy – zdecydowali się w 2022 r. na pełnoskalową operację militarną? oraz 2) co sprawiło, że tym razem ich działania spotkały się ze zdecydowanym oporem państwa ukraińskiego?

Bibliografia

Begoum F., *You and Your Walk-In*, „Studies in Intelligence" 1962, t. 6, nr 1.

Freud A., *Das Ich und die Abwehrmechanismen*, Wien 1936.

Kernberg O.F., *Borderline Conditions and Pathological Narcissism*, London 1990.

Hempel A., *Policja granatowa w okupacyjnym systemie administracyjnym Generalnego Gubernatorstwa: 1939–1945*, Warszawa 1987.

Kahneman D., Slovic P., Tversky A., *Judgment under uncertainty: heuristics and biases*, New York 1982.

Kernberg O.F., *Borderline Conditions and Pathological Narcissism*, London 1990.

Kobierzycki T., *Filozofia osobowości*, Warszawa 2001.

König K., *Abwehrmechanismen*, Göttingen–Zürich 2007.

[72] Por. „Pośród klasy urzędników zawsze znajdują się ludzie skorumpowani, którym pełniony urząd spaczył charakter, a także inni, którzy doświadczyli niesprawiedliwości i zostali skrzywdzeni. Istnieją rzesze pochlebców i sługusów, którzy pożądają bogactw. Ci pozostający zbyt długo na swych wygodnych stanowiskach, a także ci, którzy nie zajęli w swoim mniemaniu odpowiadającego im urzędu, oraz ci, których jedynym pragnieniem jest dobrze wykorzystać czas i okoliczności dla spełnienia swych egoistycznych celów, jak również tacy, którzy są dwulicowi, zmienni, efemeryczni, oraz ci, którzy wciąż czekają na swoją okazję. Możesz być pewny, że wszystkich tych ludzi można w tajemnicy pozyskać na służbę przeciwko ich państwu, zapewniając im godziwe wynagrodzenie w złocie i jedwabiu. Wtedy możesz polegać na realnych informatorach z ich kraju lub na próbach zniweczenia planów zwróconych przeciw tobie. Mogą także swobodnie kreować konflikt pomiędzy władcą a jego doradcami tak, że nie będą oni działać w zgodzie". S. Tzu, *Sztuka wojny*, oprac. J. Paterczyk, https://www.academia.edu/41929781/Sun_Tzu_SZTUKA_WOJNY_czyli_TRZYNA%C5%9ACIE_ROZDZIA%C5%81%C3%93W, s. 80 [dostęp: 21 VI 2023].

Kuk A.I., *Kanwa wywiadu agenturalnego*, Warszawa 1994.

Mentzos S., *Interpersonale und institutionalisierte Abwehr,* Frankfurt am Main 1994.

Renz B., *The Russian Force Structures*, „Russian Analytical Digest" 2007, nr 17, s. 5–7.

Serov I.A., *Work with Walk-ins*, „Studies in Intelligence" 1962, t. 8, nr 1.

Świerczek M., *Jak Sowieci przetrwali dzięki oszustwu. Sowiecka decepcja strategiczna*, Warszawa 2021.

Świerczek M., *Szturm na siedzibę Służby Bezpieczeństwa Ukrainy w Ługańsku w 2014 r. jako przykład operacji służb specjalnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2023, nr 28, s. 52–86. https://doi.org/10.4467/20801335PBW.23.002.17652.

Tönnies F., *Wspólnota i stowarzyszenie*, Warszawa 1988.

Literatura rosyjska i ukraińska

Водолеев Г.С., Сидоренко С.Ф., *Спецнужды и спецслужбы*, Москва 2009.

Зданович А., *Польский крест советской контрразведки. Польская линия в работе ЧК-НКВД. 1918-1938*, Москва 2017.

Контрразведывательный словарь, Москва 1972.

Савченко А., *Антиукраїнець: або Воля до боротьби, поразки чи зради*, Київ 2020.

Źródła internetowe

Crimea's Strategic Value to Russia, Center for Strategic and International Studies, 18 III 2014 r., https://www.csis.org/blogs/post-soviet-post/crimeas-strategic-value-russia [dostęp: 6 VI 2023].

Danylov O., *As of January 1, 2023, the population of Ukraine was 28-34 million*, Mezha.Media, 7 IV 2023 r., https://mezha.media/en/2023/04/07/as-of-january-1-2023-the-population-of-ukraine-was-28-34-million/ [dostęp: 7 VI 2023].

Janukowycz podpisał umowę o stacjonowaniu rosyjskiej floty na Ukrainie, Portal Spraw Zagranicznych, 29 IV 2010 r., https://psz.pl/162-wschod/janukowycz-podpisal-umowe-o-stacjonowaniu-rosyjskiej-floty-na-ukrainie [dostęp: 7 VI 2023].

Map of sovereign states in Europe by projected 2023 GDP (PPP) percapita based on international dollars, https://en.wikipedia.org/wiki/List_of_sovereign_states_in_Europe_by_GDP_(PPP)_per_capita [dostęp: 12 III 2024].

Samar W., *Russian «moles» in the State Security Service of Ukraine: what is missing in the Kulinich-Sivkovych' case?*, Center of Journalistic Investigations, 26 IV 2023 r., https://investigator.org.ua/investigations/253973/ [dostęp: 16 VI 2023].

Transparency International Ukraine, https://www.transparency.org/en/countries/ukraine [dostęp: 16 VI 2023].

Tzu S., *Sztuka wojny*, oprac. J. Paterczyk, https://www.academia.edu/41929781/Sun_Tzu_SZTUKA_WOJNY_czyli_TRZYNA%C5%9ACIE_ROZDZIA%C5%81%C3%93W [dostęp: 21 VI 2023].

Rosyjskie i ukraińskie źródła internetowe

Агенты национальной опасности, dsnews.ua, 28 X 2013 r., https://www.dsnews.ua/economics/agenty-natsionalnoy-opasnosti-28102013090200 [dostęp: 16 VI 2023].

Агрессивный крымский боевик Самвел оказался спецагентом Кремля и мог работать в СБУ, ТСН, 20 V 2014 r., https://tsn.ua/ru/politika/agressivnyy-krymskiy-boevik-samvel-okazalsya-specagentom-kremlya-i-mog-rabotat-v-sbu-366551.html [dostęp: 16 VI 2023].

Более 10 тысяч солдат перешли на службу России, Бездформата, https://angarsk.bezformata.com/listnews/soldat-pereshli-na-sluzhbu-rossii/62518616/ [dostęp: 7 V 2023].

Виктор Янукович: «Народ договорится, и Украина станет единой», „Аргументы и Факты" 2014, nr 52, wersja online: https://aif.ru/euromaidan/viktor_yanukovich_eksklusivnoe_interview [dostęp: 6 VI 2023].

Галеотти М., *«Сейлем» и «Башмаки». Крым и криминал до и после российской аннексии*, Крым.Реалии, 27 X 2014 r., https://ru.krymr.com/a/26658454.html [dostęp: 16 VI 2023].

Генерал-коллекционер СБУ Свиридонов друг Куницына, ОРД, 20 XII 2009 r., https://ord-ua.com/2009/12/29/general-kollektsioner-sbu-sviridonov-drug-kunitsyina/ [dostęp: 15 VI 2022].

Генерал Кривонос: про зраду в 2014-му, Порошенка, Зеленського, «клоунів» у РНБО і силове звільнення Донбасу, Радіо Свобода, 19 I 2020 r., https://www.radiosvoboda.org/a/rnbo-kryvonos-donbass-zrada-peremoga/30384758.html [dostęp: 15 VI 2023].

ДЕРЖЗРАДА, Ukrinform, https://www.ukrinform.ua/tag-derzzrada [dostęp: 14 VI 2023].

Документальный фильм «Корсуньский погром», YouTube, 30 VII 2014 r., https://www.youtube.com/watch?v=7FfPTBQ4l38 [dostęp: 22 II 2023].

Закрытый доклад СБУ: на турецкие деньги «меджлис» вел разведку для Анкары, EADaily, 7 IV 2016 r., https://eadaily.com/ru/news/2016/04/07/zakrytyy-doklad-sbu-na-tureckie-dengi-medzhlis-vel-razvedku-dlya-ankary [dostęp: 16 VI 2023].

Замглавы Меджлиса Умеров: Сотрудники СБУ и милиции в Крыму оказались предателями на 100%, военнослужащие - на 80%, прокуратура - на 70%, New Voice, 5 XI 2017 r., https://nv.ua/ukraine/politics/zamglavy-medzhlisa-umerov-sotrudniki-sbu-i--militsii-v-krymu-okazalis-predateljami-na-100-voennosluzhashchie-na-80-prokuratura--na-70-2135335.html [dostęp: 7 V 2023].

Замглавы Меджлиса упрекнул Украину в сдаче Крыма без стрельбы, Черноморская телерадиокомпания, 6 XI 2017 r., https://blackseatv.com/in-the-spotlight/zamglavy-medzhlisa-upreknul-ukrainu-v-sdache-kryma-bez-strelby/ [dostęp: 7 V 2023].

Козаченко О., *Умеров жалеет, что в Крыму не стали стрелять по русским*, Полит Навигатор, 3 XI 2017 r., https://m.politnavigator.net/umerov-zhaleet-chto-v-krymu-ne-stali-strelyat-po-russkim.html [dostęp: 7 V 2023].

Корупція та зрада - це неприпустимі речі. І у професійному, і в людському плані. Це не можна пробачати», - Ігор Клименко, 7 II 2023 r., https://mvs.gov.ua/uk/news/korupciia--ta-zrada-ce-nepripustimi-reci-i-u-profesiinomu-i-v-liudskomu-plani-ce-ne-mozna-probacati-igor-klimenko [dostęp: 15 VI 2023].

Коррупция - СТОП! Прокуратура признала действия СБУ не соответствующими законодательству, LB.ua, 23 V 2011 r., https://lb.ua/news/2011/05/23/97705_korruptsiya_stop_prokuratura_priz.html [dostęp: 16 VI 2023].

Корсуньская трагедия - боевики Майдана пытают крымчан, поджёг автобусов. 20.02.2014, YouTube, 20 II 2017 r., https://www.youtube.com/watch?v=s2TGeF=-xbTc&list-PLeuqEfNtM8zleTyjJ-n8DXE2Uz9OHm2Ty [dostęp: 23 II 2023].

Корсуньская трагедия Убивали только за то, что они из Крыма 2014 весна, YouTube, 27 V 2019 r., https://www.youtube.com/watch?v=bqUcM5YBWFw [dostęp: 23 II 2023].

„Корсуньский погром": зверства сторонников майдана, YouTube, 21 VI 2014 r., https://www.youtube.com/watch?v=hlf_AdGbfjE [dostęp: 22 II 2023].

Круглов А., *На измене*, Совершенно Секретно, 30 X 2014 r., https://www.sovsekretno.ru/articles/bezopasnost/na-izmene/ [dostęp: 7 V 2023].

Крым Путь на Родину Документальный фильм Андрея Кондрашова, YouTube, 4 X 2020 r., https://www.youtube.com/watch?v=PGGNXIQXlcU [dostęp: 2 III 2023].

Милиция и СБУ закупили машин на 30 миллионов, bigmir)net, 15 XII 2010 r., https://auto.bigmir.net/autonews/autoworld/5217854-miliciya-i-sbu-zakupili-masin-na--30-millionov [dostęp: 16 VI 2023].

Myrotvorets, https://myrotvorets.news/?s=%D0%B7%D1%80%D0%B0%D0%B4%D0%BD%D0%B8%D0%BA [dostęp: 14 VI 2023].

Нардеп Тымчук назвал число изменивших присяге крымских силовиков, Black Sea News, 6 XI 2017 r., https://www.blackseanews.net/read/136189 [dostęp: 5 VI 2023].

Новые русские бандиты: кто контролирует Крым, Україна Кримінальна, 24 III 2014 r., https://cripo.com.ua/investigations/?p=172293/ [dostęp: 16 VI 2023].

Официальная статистика: замглавы Меджлиса завысил количество предателей в Крыму на 10 %, Inform Napalm, 7 XI 2017 r., https://informnapalm.org/41430-ofitsialnaya-statistika-zamglavy-medzhlisa-zavysil-protsent/ [dostęp: 7 V 2023].

Оперативный приказ Народного комиссара внутренних дел Союза ССР Николая Ежова № 00485. 11 августа 1937 г. о польской национальной операции, https://operacja-polska.pl/nkr/o-operacji-polskiej-nkw/dokumenty/966,00485-11-1937.html [dostęp: 22 X 2019].

„Предатели на 100%": Умеров резко высказался о спецслужбах в Крыму, OBOZ.UA, 5 XI 2017 r., https://news.obozrevatel.com/society/predateli-na-100-umerov-rezko-vyiskazalsya-o-spetssluzhbah-v-kryimu.htm [dostęp: 7 V 2023].

Про кількість та склад населення України за підсумками Всеукраїнського перепису населення 2001 року, https://web.archive.org/web/20071124125111/http://www.ukrcensus.gov.ua/results/general/nationality/ [dostęp: 12 VI 2023].

Сколько военных ВСУ и СБУ перешли на сторону России в 2014 году, RF-SMI, 20 II 2022 r., https://rf-smi.ru/ykr/71072-skolko-voennyh-vsu-i-sbu-pereshli-na-storonu-rossii-v-2014-godu.html [dostęp: 7 V 2023].

Сколько военных из Крыма предали Украину: шокирующие цифры, Panoptikon, 7 XI 2017 r., https://panoptikon.org/ukraine/98813-skolko-voennykh-iz-kryma-predali-ukrainu-shokirujushhie-cifry.html [dostęp: 4 VI 2023].

Теперь пишут записки в Москву: озвучены масштабы предательства крымчан, From-UA, 30 XI 2017 r., https://from-ua.org/news/425623-teper-pishut-zapiski-v-moskvu-ozvucheni-masshtabi-predatelstva-krimchan.html [dostęp: 7 V 2023].

Тымчук Д., *Сколько крымских силовиков стали предателями Украины*, UA Info, 6 XI 2017 r., https://uainfo.org/blognews/1509980385-skolko-ukrainskiy-silovikov-v-krymu-stali-predatelyami.html [dostęp: 4 VI 2023].

Тымчук Д., wpis w serwisie Facebook, https://www.facebook.com/dmitry.tymchuk/posts/1366726656789319 [dostęp: 9 VI 2023].

Тымчук назвал число предателей среди украинских силовиков в Крыму после аннексии, РБК-Україна, 6 XI 2017 r., https://www.rbc.ua/rus/news/tymchuk-nazval-chislo-predateley-sredi-ukrainskih-1509976026.html [dostęp: 4 VI 2023].

Численность ФСБ, https://fsb.dossier.center/number/ [dostęp: 12 VI 2023].

Dr Marek Świerczek

Funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Kontakt: m.swierczek@abw.gov.pl

ARTYKUŁY RECENZYJNE

RECENZJE

Narracja zwycięzców? Na marginesie monografii Michaela Wali *Der Stasi-Mythos. DDR-Auslandsspionage und der Verfassungsschutz*[1]

TYTUS JASKUŁOWSKI

Instytut Nauk o Polityce i Administracji,
Uniwersytet Zielonogórski
https://orcid.org/0000-0001-9883-9944

Przegląd Bezpieczeństwa Wewnętrznego, 2024, nr 30: 161–169

https://doi.org/10.4467/20801335PBW.24.006.19608

RECENZJA

Badanie walki służb specjalnych należących w okresie zimnej wojny do przeciwstawnych sojuszy polityczno-wojskowych to zadanie tyleż pasjonujące, co ryzykowne. O ile bowiem w państwach Europy Wschodniej po 1989 r. dochodziło, w różnej formie, do udostępnienia akt byłych resortów spraw wewnętrznych, co pozwalało na prowadzenie, np. przez autora recenzji, kwerendy porównawczej dotyczącej relacji Ministerstwa Spraw Wewnętrznych PRL ze wschodnioniemieckim Ministerstwem Bezpieczeństwa Państwowego (Ministerium für Staatssicherheit, Stasi)[2], o tyle ocena realizowanych przeciwko sobie działań wywiadów lub kontrwywiadów państw

[1] M. Wala, *Der Stasi-Mythos. DDR-Auslandsspionage und der Verfassungsschutz,* Berlin 2023, Ch. Links Verlag, 354 s.

[2] T. Jaskułowski, *Przyjaźń, której nie było. Ministerstwo Bezpieczeństwa Państwowego NRD wobec MSW 1974–1990*, Warszawa 2014.

Organizacji Traktatu Północnoatlantyckiego i Układu Warszawskiego musiała być dokonywana przy o wiele bardziej ograniczonym dostępie do źródeł. Problem wynikał nie tylko ze zniszczenia części dokumentacji służb specjalnych państw socjalistycznych, lecz także z utrudnionego dostępu do akt strony przeciwnej, co stopniowo zmieniało się dzięki postulatom szerszego otwarcia archiwów i liberalizacji podejścia do tej kwestii przez rządy krajów członkowskich NATO. W tym kontekście warto wskazać na powołanie w 2011 r. komisji mającej badać historię, działania oraz kadry Federalnej Służby Wywiadowczej Republiki Federalnej Niemiec (Bundesnachrichtendienst, BND)[3].

Pochodną prac wspomnianego gremium stały się projekty badawcze wspierane przez niemieckie MSW dotyczące walki między służbami specjalnymi dwóch niemieckich państw prowadzonej od 1949 r. do 1989 r. Efektem jednego z tych projektów jest recenzowana praca Michaela Wali, profesora na Uniwersytecie Ruhry w Bochum. Dotyczy ona działań wschodnioniemieckiego Głównego Zarządu Wywiadu (Hauptverwaltung Aufklärung, HVA) Stasi oraz zachodnioniemieckiego kontrwywiadu, czyli Federalnego Urzędu Ochrony Konstytucji (Bundesamt für Verfassungsschutz, BfV). Wala zdobył uznanie jako współautor monografii o nazistowskiej przeszłości personelu BfV[4]. Dość naturalne wydawało się zatem podjęcie się analizy porównawczej obustronnych działań tego kontrwywiadu i służb Niemieckiej Republiki Demokratycznej (NRD). Sąsiednie państwo było priorytetem w aktywności operacyjnej BfV i HVA, nie tylko z racji przynależności do przeciwstawnych sojuszy, statusu państwa frontowego, lecz przede wszystkim z uwagi na ten sam język, względnie cele polityczne takie jak zjednoczenie Niemiec. Potwierdza to zresztą, mimo że ze swej natury subiektywna, memuarystyka byłych szefów wywiadu Stasi, np. Wernera Großmanna[5].

Te wspomnienia stały się jednym z elementów, które skłoniły Walę do podjęcia prac nad omawianym studium. W skrajnych przypadkach stanowiły one bowiem formę bezkrytycznej autoreklamy domniemanej potęgi operacyjnej Stasi w Republice Federalnej Niemiec (RFN)[6], co tym bardziej zachęcało do jej weryfikacji na podstawie dokumentów archiwalnych. Te, choć dostępne dzięki pracy dawnego tzw. Urzędu Gaucka, a obecnie Archiwum Federalnego (Bundesarchiv), pozostawały niekompletne przede wszystkim z uwagi na decyzję o zniszczeniu akt HVA,

[3] Unabhängige Historikerkommission zur Erforschung der Geschichte des Bundesnachrichtendienstes 1945–1968, http://www.uhk-bnd.de/ [dostęp: 3 III 2024].

[4] C. Goschler, M. Wala, *Das Bundesamt für Verfassungsschutz und die NS-Vergangenheit*, Hamburg 2015.

[5] W. Großmann, *Bonn im Blick. Die DDR-Aufklärung aus der Sicht ihres letzten Chefs*, Berlin 2001, s. 46.

[6] *Die Sicherheit. Zur Abwehrarbeit des MfS*, R. Grimmer (red.), Berlin 2003, s. 433.

zaakceptowaną w NRD przez uczestników okrągłego stołu w 1990 r. Część spuścizny zarówno tego ostatniego, jak i kontrwywiadu Stasi jednak pozostała. Co najważniejsze, dotychczas w literaturze przedmiotu nie korzystano z materiałów BfV, które są podstawową dokumentacją dla rzetelnego przeprowadzenia badań porównawczych.

Nawiązując do tytułu niniejszej recenzji, można stwierdzić, że Wala zamierzał wskazać niuanse w trwale istniejącej w mediach tzw. narracji przegranych, czyli wypowiedziach tajnych współpracowników lub funkcjonariuszy Stasi na temat własnych sukcesów w RFN[7]. Czytelnik nie otrzymuje jednak książki będącej kwintesencją narracji zwycięzców, która dotyczy wyłącznie domniemanych sukcesów służb RFN we wschodnich Niemczech, ponieważ Wala uzyskał pełny dostęp do akt BfV z lat 1950–1990 oraz nie unikał tematów najbardziej drażliwych w historii służb, w rodzaju zdrad we własnych szeregach.

Monografia zachowuje ciągłość chronologiczną. Zawarto w niej niezbędne informacje na temat zarówno powstania BfV, jak i przełomu lat 1989 i 1990. Składa się z rozdziałów problemowych poświęconych poszczególnym elementom techniki pracy operacyjnej zachodnioniemieckiego kontrwywiadu. Te z kolei dzielą się na podrozdziały dotyczące konkretnych działań podejmowanych w przypadku wystąpienia podejrzeń natury kontrwywiadowczej, odkrycia zdrady wśród własnych agentów i obecności agentów Stasi, w pracy rozpoznania radioelektronicznego, w operacjach kontrwywiadowczych, wobec uciekinierów z NRD, czy też wobec praktyk, które chętnie opisywano w publicystyce po 1990 r., takich jak werbowanie – przez służby obu niemieckich państw – osób z konkretnych grup zawodowych, np. sekretarek zatrudnionych w instytucjach państwowych. W monografii, mimo zrozumiałego skupienia się na służbach RFN, brakuje jednak odnośników dotyczących równoległego rozwoju Stasi. Ten niewątpliwie już został przebadany, ale osoba, która nie zna literatury na temat aparatu bezpieczeństwa w NRD, może być w trakcie lektury nieco zagubiona, np. w niejasnej dla niej terminologii. W przypadku przygotowania wersji anglojęzycznej warto byłoby zaopatrzyć ją w bardziej rozbudowane przypisy rzeczowe.

Praca sprawia wrażenie uzupełnienia publicystycznego studium Johna Pomfreta[8], przynajmniej w części poświęconej rozpoczęciu polsko-amerykańskiej współpracy wywiadowczej, a także książki Tomasza Kozłowskiego o transformacji MSW w Polsce[9]. Z pewnością nie był to zamysł autorski Wali, ale ponieważ opisuje

[7] G. Gast, *Kundschafterin des Friedens. 17 Jahre Topspionin der DDR beim BND*, Berlin 2016, s. 235.

[8] J. Pomfret, *Pozdrowienia z Warszawy. Polski wywiad, CIA i wyjątkowy sojusz*, Kraków 2022.

[9] T. Kozłowski, *Koniec imperium MSW. Transformacja organów bezpieczeństwa państwa 1989–1990*, Warszawa 2019.

on różne aspekty tworzenia służb specjalnych w państwie podlegającym transformacji demokratycznej, a także rolę sojuszniczych służb w tym procesie, to z uwagi na podobieństwo do zdarzeń w naszym kraju z przełomu lat 1989 i 1990, polski czytelnik może dokonywać porównań do wspomnianych publikacji. Rozdziały o początkach prac koncepcyjnych nad organizacją pierwszych instytucji mających chronić przyszły zachodnioniemiecki rząd przed zagrożeniami zewnętrznymi doskonale ukazują, jak władze USA i Wielkiej Brytanii zdecydowanie wskazywały na potrzebę zbudowania zorientowanego na demokratyczne wartości aparatu bezpieczeństwa o funkcji przede wszystkim kontrwywiadowczej. W tej służbie – przynajmniej w teorii – nie miało być miejsca dla osób, które w jakikolwiek sposób uczestniczyły w pracy organów III Rzeszy, np. Gestapo. Ten wątek narracji zwycięzców Wala podkreśla równie mocno, jak jego trudną implementację. Zresztą zdumiewająco podobna sytuacja była w Polsce po 1989 r., kiedy w miejsce komunistycznych służb specjalnych tworzono m.in. Urząd Ochrony Państwa. Wtedy także enuncjacje dotyczące dalszego zatrudniania ludzi służb z okresu PRL były komentowane przez publicystów[10].

Tworzenie zachodnioniemieckich służb specjalnych po II wojnie światowej było naznaczone permanentnymi sporami kompetencyjnymi ministerstwa spraw wewnętrznych i urzędu kanclerskiego o prawo nadzoru nad nimi. Dyskusje o tym, kto powinien kierować urzędem, prowadziły do walk frakcyjnych, a także prób wywarcia wpływu, jeżeli nie wprost lobbingu, na brytyjskie i amerykańskie władze w celu uzyskania ich poparcia dla konkretnych kandydatów. Dla polskiego czytelnika interesujące mogą być również, zachowane w aktach i przytaczane przez Walę, informacje o konfliktach między przedstawicielami alianckich służb, którzy wyznaczali własnych protegowanych na kierownicze stanowiska w BfV, a także fakt, że Reinhard Gehlen, kojarzony jako twórca BND, był postrzegany przez kanclerza Konrada Adenauera jako idealny kandydat na szefa, ale BfV. Być może to właśnie prowadziło do kolejnych zatargów dotyczących wzajemnego przejmowania uprawnień przez obie instytucje.

Wala rzetelnie omawia brak sukcesów w prowadzeniu pracy operacyjnej w NRD oraz brutalne obustronne oceny dorobku analitycznego BfV i BND. Ta pierwsza uznawała np., że nawet 80% meldunków dostarczanych przez BND ze wschodnich Niemiec w latach 50. XX w. było bezwartościowe (s. 19). Interesujące pozostają (nie tylko w kontekście opozycyjnej aktywności pierwszych kadr polskiego UOP) wątek zatrudniania przez tworzące się BfV pracowników pochodzących ze środowisk antyfaszystowskiego ruchu oporu w Niemczech, szpiegowskie skandale wywoływane w prasie przez niedyskrecję organów ścigania, niejasne

[10] G. Chlasta, *Czterech. Brochwicz, Miodowicz, Niemczyk, Sienkiewicz*, Warszawa 2014, s. 61.

powiązania funkcjonariuszy BfV z pracownikami alianckich służb, przyjmowanie od nich pieniędzy, a także wprost formułowane pytanie o kręgosłup moralny kadry BfV. Co istotne, Wala weryfikował tego typu wskazania przez kwerendę w amerykańskich i brytyjskich archiwach.

W kontekście ujawnianych przez Walę wyzwań i problemów BfV, a także kontrowersyjnych, choć być może racjonalnych pod względem operacyjnym, metod ich rozwiązywania można wskazać potrzebę analizy porównawczej funkcjonowania niemieckich służb dotyczącej okresu po powstaniu RFN w 1949 r. i lat transformacji po przesileniu politycznym w Europie Wschodniej w 1989 r. Na przykład Wala wskazuje, że po II wojnie światowej członkowie SS lub funkcjonariusze Gestapo byli stałymi współpracownikami BfV. Ich formalne zatrudnienie na etat byłoby bowiem zablokowane przez aliantów. Tymczasem 20 lat po rewolucji w 1989 r. w administracji państwowej zjednoczonych Niemiec bez większych problemów zatrudniano dawnych funkcjonariuszy Stasi. Ponad 2700 takich osób pracowało np. w straży granicznej czy w BND, gdzie spotykały ich dawne ofiary[11]. Zarzutem wobec publikacji Wali jest ponadto brak odniesień do działań BfV na kierunkach innych niż wschodnioniemiecki. Próżno szukać w monografii odwołań do akt dostępnych w Instytucie Pamięci Narodowej lub do prac o działalności polskiego wywiadu, np. Witolda Bagieńskiego[12], zgodnych chronologicznie z recenzowaną książką. To po raz kolejny uzasadnia postulat uzupełnienia deficytu badań porównawczych oraz potrzebę tłumaczenia polskich opracowań na języki kongresowe.

Recenzowana publikacja przybliża w zasadzie nieznany obraz pracy kontrwywiadu w państwie, które znajduje się na granicy konfliktu Wschodu z Zachodem. Ta praca polegała na mozolnym przepytywaniu wschodnioniemieckich uchodźców przybywających do RFN, kontroli organizacji socjalistycznych i lewicowych, które z urzędu były podejrzewane o finansowanie lub inspirację przez Stasi, konfliktach z prokuraturą dotyczących wysokości wyroków oraz sposobu interpretacji przepisów kodeksu karnego w kontekście definicji szpiegostwa. Na to wszystko nakładały się braki kadrowe oraz permanentne niedofinansowanie służby. I choć skala wyroków skazujących za szpiegostwo do drugiej połowy lat 60. XX w. była znaczna, gdyż oscylowała między 250 a 360 rocznie, to – jak wskazuje Wala – nie dotyczyła ona przypadków najlepiej przygotowanych agentów przeznaczonych do infiltracji najważniejszych instytucji w RFN. Na tym tle monografia spełnia niezwykle wartościową funkcję – przedstawia rzeczywisty obraz pracy kontrwywiadowczej, zarówno tej

[11] J. Staadt, *Allgegenwärtige Kontrolleure*, Frankfurter Allgemeine Zeitung, 10 VII 2009 r., https://www.faz.net/aktuell/politik/inland/fruehere-stasi-mitarbeiter-allgegenwaertige-kontrolleure-1830551.html [dostęp: 3 III 2024].

[12] W. Bagieński, *Wywiad cywilny Polski Ludowej w latach 1945–1961*, Warszawa 2017.

stricte operacyjnej, jak i analitycznej. Warto zaznaczyć, że praca analityczna w okresie zimnej wojny nie sprowadzała się tylko do prezentowania decydentom politycznym lepiej lub gorzej udowodnionych hipotez dotyczących sytuacji, np. w NRD, lecz także do prowadzenia łatwych w użyciu kartotek, usiłowania selekcji informacji, walki o jak najszybsze korzystanie z elektronicznych systemów przetwarzania danych, względnie ujednolicenie z amerykańską Centralną Agencją Wywiadowczą (Central Intelligence Agency, CIA) systemów przekazywania informacji o potencjalnych współpracownikach Stasi, ponieważ brak standaryzacji przekazu był istotnym problemem. Równie problematyczna stała się polityka alianckich służb, które narzucały BfV tematykę rozpracowań i oczekiwały coraz większych kompetencji nadzorczych wobec kontrwywiadu, do kontroli zatrudniania funkcjonariuszy włącznie. Co najważniejsze, dla BfV głównym źródłem informacji o Stasi, w tym o HVA, stali się nie agenci uplasowani we wschodnich Niemczech, lecz uciekinierzy z NRD zatrudnieni tam w służbie bezpieczeństwa lub innych instytucjach. Sygnalizowana przez Walę skala owych ucieczek w latach 1949–1961 (75 uciekinierów zawodowo związanych ze Stasi) wydaje się niewielka wobec statystyk dotyczących ogólnego transferu ludności z NRD do RFN w tym samym okresie (ponad 3 mln), zatrzymanego budową muru w Berlinie. Dane przytaczane przez Walę dają przeciętnie sześć osób rocznie, które zidentyfikowano jako pracujące w Stasi, tymczasem sam BfV pod koniec lat 60. XX w. rejestrował w swoich kartotekach prawie 1,3 mln nazwisk ludzi, którzy mogli mieć znaczenie operacyjne.

W związku z tym, jaka była, inna niż tylko administracyjna, rola BfV? Wspomniany i pozornie mały odsetek uciekinierów istotnych kontrwywiadowczo zadawał Stasi bolesne straty. Zdrada w 1979 r. tylko jednego oficera HVA, Wernera Stillera, doprowadziła do 16 zatrzymań, 11 kolejnych nakazów aresztowania oraz 14 ucieczek innych agentów zagrożonych dekonspiracją. Tyle tylko, że – zdaniem Wali – 1/4 pracowników Stasi, którzy uciekli do RFN, i tak była porwana później przez te służby w celu osądzenia ich w NRD. Siedmioro z nich stracono, co z kolei nie może być dowodem skuteczności ochrony kontrwywiadowczej RFN, w której pracowały wszak jeszcze amerykańskie, brytyjskie i francuskie służby. W tym kontekście pozostawały znamienne konflikty służb USA i RFN ujawnione przez Walę, doskonale znane recenzentowi z badań dotyczących kontaktów Stasi i polskiego MSW[13], ale być może zaskakujące dla niektórych czytelników. Dotyczyły one prozaicznych spraw, takich jak sprzątanie mieszkań dla uciekinierów ze służb NRD. Lepszego przykładu demitologizacji pracy tajnych służb nie można sobie wyobrazić. Czynią one lekturę recenzowanej książki jeszcze bardziej interesującą.

[13] T. Jaskułowski, *Szpiedzy tacy jak wy. Wywiadowcza (nie)codzienność kontaktów między PRL a NRD 1970–1990*, Warszawa 2015.

Dyskusja o rachunkach za panie sprzątające nie była bez wątpienia największym problemem BfV. Metodologia pracy tej służby koncentrowała się na wyłapywaniu wśród uchodźców z NRD osób podejrzanych o pracę dla Stasi. Obraz masowych werbunków do momentu budowy muru berlińskiego w 1961 r. został połączony przez Walę z szacunkami, według których ok. 20% przypadków w grupie uciekinierów stanowili wykryci przez BfV figuranci szantażowani przez Stasi. Ta sytuacja przypomina działania tej ostatniej podejmowane wobec PRL po rozpoczęciu przesilenia politycznego w 1980 r. Wala sygnalizuje ponadto, że część uciekinierów była przygotowywana przez BfV do ponownego osiedlenia się we wschodnich Niemczech i dostarczania informacji stamtąd. Mur berliński stał się zatem, chociaż nie było to jego głównym zadaniem, instrumentem poprawy ochrony kontrwywiadowczej RFN. Do podobnych celów wykorzystywano system wymiany danych urzędów meldunkowych, dzięki któremu było łatwiej wychwytywać osoby posługujące się fałszywą tożsamością. To właśnie mur berliński oraz monotonna praca osób odpowiedzialnych za przesłuchania i weryfikację ankiet uchodźców z NRD są głównymi bohaterami książki. Odpowiadają za najważniejsze kontrwywiadowcze sukcesy RFN, takie jak zmuszenie do ucieczki łączników kluczowej agentki Stasi w BND Gabriele Gast, a także wykrycie ponad 400 przypadków pracy dla służb NRD do momentu zjednoczenia Niemiec. Co ciekawe, zdaniem Wali, porównywanie rejestrów meldunkowych i monitorowanie osób rzekomo urodzonych w Niemczech i wracających po latach do RFN z emigracji kontynuowano jeszcze do połowy lat 90. XX w.

Obraz zachodnioniemieckiego kontrwywiadu wyłaniający się z pracy Wali nie jest bynajmniej pełen sukcesów. Choć przynajmniej od końca lat 60. XX w., jego zdaniem, BfV miał wiedzieć o procederze uwodzenia przez agentów Stasi sekretarek w zachodnioniemieckich urzędach, co teoretycznie powinno powodować zaostrzenie procedur bezpieczeństwa, to te kobiety nadal pracowały w urzędzie kanclerskim, NATO, MSZ RFN czy też w centralach partii politycznych. Było to przyczyną znacznych strat dla tych instytucji. Banalnie prosta metoda zawierania znajomości z figurantką przez ogłoszenie matrymonialne okazywała się przy tym tak samo skuteczna, jak późniejsza reakcja BfV, czyli odpowiadanie na podejrzane ogłoszenia przez wysyłanie kontrolowanych ofert. Opis tego typu operacji jest jedną z istotnych zalet monografii. Obok sukcesów w prowadzeniu obserwacji kurierów wywiadowczych czy też w wywiadzie radioelektronicznym, Wala wskazuje także na permanentne problemy kompetencyjne w strukturze BfV, które wynikały z federalnej struktury zachodnioniemieckiego państwa, oraz na niedofinansowanie jako generalną bolączkę każdej instytucji państwowej. Tygodniowa praca jednej grupy obserwacyjnej mogła kosztować ponad 15 000 marek RFN. Stąd pieniądze, a właściwie ich brak, stawały się czasami problemem równie istotnym jak zdrajcy

we własnych szeregach. Autor monografii wskazuje przy tym na radykalną nierówność wobec gratyfikacji oferowanych przez przeciwnika. Służby NRD płaciły lepiej, co Wala skonfrontował z przypadkami otrzymywania zaledwie 50 marek RFN za raport wywiadowczy lub przekazanie BfV trzech dokumentów tego rodzaju i grożącymi za to konsekwencjami w NRD, tj. możliwością otrzymania wyroku pozbawienia wolności na 6 lat. Inna sprawa, że BfV podejmował wszelkie kroki zmierzające do wymiany agentów nawet po ujawnieniu w mediach własnych porażek, np. przejścia swojego człowieka na stronę wschodnioniemiecką, a także wiele lat po zjednoczeniu Niemiec prawnokarnie ścigał podwójnych agentów, tj. osoby pracujące oficjalnie dla rządu RFN, a w rzeczywistości np. dla HVA. Nie dziwiło to z uwagi na, rozpatrywane w osobnych rozdziałach, największe klęski BfV, takie jak praca dla Stasi Klausa Kuronia – szefa referatu tzw. szpiegostwa politycznego NRD.

Analizy wywołanych przez niego szkód, sporządzone po 1990 r. i cytowane przez Walę, wskazują na duże straty dla pracy kontrwywiadu, a jednocześnie potwierdzają klasyczny powód decyzji o zdradzie, jakim są pieniądze. Do zdrady na podobnym poziomie, tym razem jednak w HVA, doszło w trakcie rewolucji w NRD i doprowadziła ona do ujawnienia istotnych danych na temat działalności wywiadu Stasi w RFN. Wala wskazuje na balans między finansową motywacją do rozpoczęcia działalności szpiegowskiej, której powodem jest np. alkoholizm, a analizą poszczególnych przypadków, np. reorganizacją BfV przyspieszoną przez ucieczkę innego wysokiego funkcjonariusza, Hansa-Joachima Tiedgego, z zaznaczeniem wyraźnej przewagi służb NRD w kontekście wysokości oferowanych pieniędzy. Nie dziwi zatem ani konstatacja Wali o radykalnym spadku dochodzeń kontrwywiadowczych w latach 80. XX w. z uwagi na zdradę obu wspomnianych funkcjonariuszy, ani determinacja BfV do pozyskiwania jak największej ilości informacji od oficerów Stasi w okresie pokojowej rewolucji w latach 1989–1990. Do momentu formalnego zjednoczenia Niemiec 3 października 1990 r. kontrwywiad RFN, w odróżnieniu od BND, nie miał jednak prawa aktywnie działać, czyli np. pozyskiwać współpracowników, na terytorium NRD. Jednak nawet potem, na co wskazuje Wala, jedynie ok. połowa byłych funkcjonariuszy Stasi była gotowa do rozmów – bez względu na ich charakter i motywację osób biorących w nich udział – z przedstawicielami kontrwywiadu. To skazywało BfV na korzystanie z pomocy w poszukiwaniu agentów, obwarowanej zresztą rozmaitymi i dość dobrze opisanymi w książce warunkami, innych służb, np. CIA.

Recenzowana monografia ma pionierski charakter i prezentuje wyważony obraz działania BfV, który korzysta z atrakcyjności swojego kraju dla uciekinierów i który zdrady na poziomie własnego kierownictwa kompensuje mozolną pracą analityczną. Czy mimo tego są w książce braki, które należałoby uzupełnić? Na podstawie badań recenzenta przeprowadzonych w archiwum Stasi można stwierdzić, że ten resort

wymieniał się doświadczeniami o pracy BfV z MSW PRL[14], w tym korzystał z wiedzy Departamentu II (kontrwywiad) np. w kontekście działań w obozach dla przesiedleńców w RFN. Przeprowadzenie podobnej kwerendy byłoby cenne dla narracji książki. Wala, koncentrując się na pracy operacyjnej BfV, w zasadzie unika oceny opracowań analitycznych tej służby np. na temat sytuacji wewnętrznej NRD. Być może ten obszar stanie się jednak przedmiotem osobnych badań. O ile autor książki odnotował wspomniane wcześniej przypadki Kuronia i Tiedgego, o tyle problem pracy dla Stasi Güntera Guillaumego, pełniącego funkcję sekretarza kanclerza Willy'ego Brandta, komentuje jednym zdaniem. Uzasadnia to stwierdzeniem, że jego sprawa została już omówiona w literaturze. Z punktu widzenia czytelnika z kręgu kulturowego innego niż niemiecki stanowi to istotny deficyt.

Na koniec warto podkreślić, że recenzowana monografia jest tytułem, którego znajomość będzie niezbędna do zrozumienia codziennej pracy kontrwywiadowczej na terenie Niemiec w okresie zimnej wojny. Jednocześnie można mieć nadzieję, że stanie się ona zachętą do dalszych badań, także tych dotyczących Polski. Wala konstatuje wszak, że praca BfV dotyczyła Stasi w 1/4 prowadzonych operacji. Być może kiedyś powstanie zatem monografia o walce z Departamentami I i II MSW PRL, tym bardziej że w książce pojawiały się sygnały o obawach BfV dotyczących tzw. werbunków urlopowych dokonywanych w PRL np. w okresie wakacyjnym. To może stanowić asumpt do dalszych badań.

Dr hab. Tytus Jaskułowski, prof. UZ

Kierownik Katedry Historii Najnowszej i Myśli Politycznej w Instytucie Nauk o Polityce i Administracji Uniwersytetu Zielonogórskiego.

Kontakt: t.jaskulowski@inpa.uz.zgora.pl

[14] T. Jaskułowski, *Przyjaźń, której nie było*…, s. 201.

Monika Krakowska, *Zachowania informacyjne człowieka w kontekście zjawiska epistemicznej bańki informacyjnej. Propozycja nowej koncepcji*[1]

IWONA OSŁOWSKA

Autorka niezależna

https://orcid.org/0000-0002-8625-0072

Przegląd Bezpieczeństwa Wewnętrznego, 2024, nr 30: 171–181

https://doi.org/10.4467/20801335PBW.24.007.19609

RECENZJA

Rozwój technologii sprawił, że wiele przejawów życia współczesnego człowieka wiąże się z wykorzystaniem informacji pozyskiwanych w ramach zachowań informacyjnych (ang. *information behaviour*, *human information behaviour*). Ewolucja tych zachowań skłania badaczy do monitorowania tej problematyki. Wobec nadmiaru informacji otaczających jednostkę, nowych form komunikacji i różnych możliwości zastosowania oraz przetwarzania informacji istotne pozostaje prowadzenie szczegółowych badań nad ludzką infosferą. Znajomość specyfiki procesów informacyjnych jest niezbędna, szczególnie w kontekście mechanizmów filtrowania wiadomości, ponieważ zjawiska takie

[1] M. Krakowska, *Zachowania informacyjne człowieka w kontekście zjawiska epistemicznej bańki informacyjnej. Propozycja nowej koncepcji*, Kraków 2022, Wydawnictwo Uniwersytetu Jagiellońskiego, 335 s.

jak bańki informacyjne, bańki epistemiczne, epistemiczne bańki informacyjne, bańki filtrujące i komory echa[2] w dużym stopniu wpływają na codzienne życie człowieka.

W ten nurt wpisuje się książka Moniki Krakowskiej zatytułowana *Zachowania informacyjne człowieka w kontekście zjawiska epistemicznej bańki informacyjnej. Propozycja nowej koncepcji*. Autorka zawodowo związana z Uniwersytetem Jagiellońskim jest specjalistką w zakresie informatologii i problematyki zachowań informacyjnych oraz specyficznych przestrzeni informacyjnych, ze szczególnym uwzględnieniem zagadnień afektywno-kognitywnych oraz społecznych zachowań informacyjnych człowieka. Monografia Krakowskiej, która ukazała się w 2022 r. nakładem Wydawnictwa Uniwersytetu Jagiellońskiego, jest szczególna. Celem badaczki było przedstawienie nowego konceptu, jakim jest epistemiczna bańka informacyjna. Dotychczasowe badania autorki nad problematyką zachowań informacyjnych są gwarancją wiarygodności i nowatorstwa prowadzonych przez nią dociekań na temat specyficznych przestrzeni informacyjnych.

Zarówno w literaturze polskiej, jak i obcej napisano wiele o różnych aspektach zachowań informacyjnych człowieka. Badania nad tym zagadnieniem prowadzili m.in.: Barbara Kamińska-Czubała, Anna Mierzecka-Szczepańska, Maria Próchnicka, Arkadiusz Pulikowski, Małgorzata Kisilowska, Thomas Wilson, Eli Pariser, Donald O. Case, David Bawden czy Karen E. Fisher. Potwierdza to zestawiona przez Krakowską wyczerpująca, licząca ponad 600 pozycji, bibliografia z lat 1968–2021. Mimo to wciąż mamy niewystarczającą liczbę opracowań przedstawiających holistyczne podejście do procesów informacyjnych podejmowanych przez człowieka. Zagadnieniem, które do tej pory nie było przedmiotem aż tak drobiazgowych rozważań analitycznych, teoretycznych i konceptualnych, pozostaje epistemiczna bańka informacyjna wpływająca na codzienność jednostki. Krakowska za sprawą recenzowanej publikacji zwiększa społeczną świadomość istnienia tego rodzaju mechanizmu.

Pojęcia bańki filtrującej (ang. *filter bubble*) oraz epistemicznej bańki informacyjnej weszły do dyskursu naukowego stosunkowo niedawno. Pierwszy termin wprowadził do obiegu założyciel portalu Upworthy Eli Pariser podczas konferencji TED w 2011 r. i rozwinął w książce *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*[3]. Według Parisera bańka filtrująca to przestrzeń osobista i spersonalizowana, której nie dzielimy z innymi. Zwraca on uwagę na zagrożenia wynikające z obecności algorytmów w social mediach

[2] Komora echa (ang. *echo chamber*) – inaczej komora pogłosowa. Terminem tym określa się środowisko, w którym człowiek pozyskuje tylko informacje i opinie odpowiadające jego poglądom, co dodatkowo prowadzi do ich wzmocnienia. Zob. tamże, s. 189–193.

[3] E. Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, New York 2012.

i wyszukiwarkach internetowych. Po wspomnianej konferencji do obiegu trafiło sformułowanie *filter bubble*, którym określono efekt internetowej personalizacji, blokującej dopływ części informacji do użytkownika.

Terminu „epistemiczna bańka informacyjna" użyto po raz pierwszy na konferencji *ISIC 2018 – The Information Behaviour Conference*, która odbyła się w dniach 9–11 października 2018 r. w Krakowie. Ta nowa koncepcja informatologiczna rozszerza pojęcia bańki informacyjnej, bańki epistemicznej i filtrującej oraz komór echa. Służy do (…) *opisu i charakterystyki heterogenicznych procesów informacyjnych zachodzących w różnych kontekstach i wymiarach*[4]. W następnych latach nie poddano tego pojęcia dogłębnej analizie, co jest o tyle zaskakujące, że coraz częściej wykorzystuje się je w kontekście mechanizmów filtrowania informacji w badaniach z dziedziny kulturoznawstwa, dziennikarstwa, medioznawstwa czy politologii. Na ten aspekt zwraca uwagę Krakowska w swojej monografii. Prowadzenie badań w tym obszarze jest bardzo istotne, gdyż jak wskazuje filozof C. Thi Nguyen, najważniejsze informacje, powstałe w wyniku procesów społecznej selekcji[5], są często blokowane przez bańki epistemiczne będące społecznymi strukturami poznawczymi.

Przedstawione powyżej dwa zjawiska są do siebie podobne tylko w pewnym stopniu, co powoduje, że w codziennym dyskursie mogą być mylone. W monografii badaczka podjęła się nie tylko wyjaśnienia różnic między tymi dwoma terminami, lecz także wypracowania nowej koncepcji epistemicznej bańki informacyjnej. Koncentruje się na zachowaniach informacyjnych podejmowanych w tego rodzaju bańce.

Krakowska buduje narrację wokół źródeł tekstowych wykazanych w bibliografii, m.in. z zakresu informatologii, socjologii, psychologii, filozofii, które zostały uwzględnione w wyniku analizy zawartości wielu baz. Warto w tym miejscu wymienić za autorką choćby kilka z nich na potwierdzenie solidności jej warsztatu badawczego. Sięgnęła m.in. do: Library, Information Science and Technology Abstracts, EBSCO, Academic Research Source eBooks, Academic Research Source eJournals, Academic Search Ultimate.

Literatura, na którą powołuje się Krakowska, to przede wszystkim opracowania anglojęzyczne, gdyż jest to język wiodący w nauce o informacji. Poza tym wykorzystuje także opracowania w języku polskim. Zgromadzenie przez badaczkę tak licznego materiału było niezbędne do prawidłowej oceny zjawiska, co uzasadnia następująco:

> Badania zachowań informacyjnych dotyczą wielu zjawisk i prowadzą do kształtowania się różnych koncepcji, które próbują wyjaśnić sposoby, w jakie

[4] M. Krakowska, *Zachowania informacyjne*…, s. 218.

[5] C.T. Nguyen, *Echo chambers and epistemic bubbles*, „Episteme" 2020, t. 17, nr 2, s. 141–161.

> człowiek podejmuje się informacyjnych praktyk, ale też pozwalają na rozpoznanie heterogeniczności wszelkich aktywności informacyjnych, zarówno na poziomie jednostkowym, jak i społecznym. Coraz częściej koncepcje i zjawiska przenikają się wzajemnie, tworząc specyficzny kontekst dla zachowań informacyjnych, kreując także określoną przestrzeń informacyjną[6].

Nowatorstwo i oryginalny wkład prezentowanej monografii w badania nad zachowaniami informacyjnymi człowieka dotyczy nie tylko samego przedmiotu dociekań, lecz także metodologii. Zgromadzony materiał został przeanalizowany z zastosowaniem różnych metod badawczych, począwszy od metody analizy i krytyki piśmiennictwa (ang. *literature review*), poprzez metodę przeglądu i krytyki literatury z danego zakresu (ang. *scoping literature review/scoping review*), analizę pojęć i koncepcji (ang. *conceptual analysis*) aż do zastosowania techniki kuli śnieżnej (ang. *snowball sampling*). Skorzystanie przez autorkę z tak szerokiego warsztatu badawczego pozwoliło na szczegółowe opisanie nowego konceptu zjawiska epistemicznej bańki informacyjnej.

Głównym celem książki, na co Krakowska zwróciła uwagę we wstępie, było przedstawienie wiedzy na temat zachowań informacyjnych człowieka oraz mechanizmów kształtowania epistemicznej bańki informacyjnej. Badaczka dokonała (…) *krytycznej analizy* (…) *różnorodnych aspektów i uwarunkowań*[7] zachowań informacyjnych, a także uwzględniła interdyscyplinarny wymiar tego zagadnienia. Wielostronne podejście ułatwiło realizację celów szczegółowych przedstawionych we wstępie oraz osadzenie ich w szerszym kontekście zachowań informacyjnych. Czytelnik znajdzie odpowiedzi na wskazane problemy badawcze w kolejnych rozdziałach monografii.

Krakowska za punkt wyjścia do rozważań wybrała analizę aktywności, które człowiek podejmuje w relacji do informacji. Autorka bardzo trafnie dobrała też motto wprowadzające do pierwszego rozdziału zatytułowanego *Zachowania informacyjne człowieka – wybrane konteksty*. Przytoczyła słowa Toma Wilsona:

> (…) zachowania informacyjne odnoszą się do całości działań, w które ludzie się angażują, oraz do interakcji z informacjami w taki czy inny sposób. W rzeczywistości życie jest zachowaniem informacyjnym, ponieważ nie możemy przetrwać bez informacji. Nieustannie przyjmujemy informacje wszystkimi zmysłami. Cały czas zachowujemy się w stosunku do informacji[8].

---

[6] M. Krakowska, *Zachowania informacyjne*…, s. 12–13.

[7] Tamże, s. 17.

[8] T.D. Wilson, *Remodeling the model.* Keynote presentation during the 2020 ISIC Pretoria, South Africa, 28.09–02.10.2020, za: M. Krakowska, *Zachowania informacyjne*…, s. 25.

Jeszcze w ubiegłym wieku wpływ technologii informacyjnych na ludzkie życie nie był tak duży jak dotychczas. Nowe stulecie przyniosło powszechny, szybki i bezpośredni dostęp do informacji za pośrednictwem nowych mediów. W dobie internetu zmieniły się zachowania informacyjne człowieka, na co zwraca uwagę m.in. cytowany przez autorkę monografii Wilson.

Krakowska rozwija jego myśl w pierwszym rozdziale. Badaczka podjęła w nim próbę zdefiniowania zachowań informacyjnych człowieka na podstawie prac m.in. Marci J. Bates, Donalda O. Case'a, Lisy M. Given, Brady'ego D. Lunda, Toma Wilsona, Sabiny Cisek. Kwestia ta od lat budzi szczególne zainteresowanie w środowisku naukowym. Obecnie coraz powszechniejsze ujęcie interdyscyplinarne pozwoliło na wielowątkową analizę ludzkich aktywności informacyjnych. Ze względu na złożoność problematyki autorka prezentuje jedynie wybrane obszary i zagadnienia. Omawia kwestie terminologii z perspektywy nauk o informacji. Prowadzone przez nią badania potwierdzają, że zachowania informacyjne:

> (…) zbudowane są z różnorodnych procesów – nie tylko informacyjnych, ale też poznawczych, psychologicznych, fizjologicznych, oraz aktywności zarówno odwzorowujących stany jednostki, jak i uzależnionych od szerokiego kontekstu, czyli sytuacji, okoliczności, uwarunkowań, wymiaru społecznego, kulturowego, ekspansywnie zachodzących zmian, ewolucji[9].

Autorka wskazuje również na bardzo istotny element, który wpływa na zachowania informacyjne, a mianowicie to, że człowiek nie tylko odbiera informacje przez zmysły, lecz także sam ich poszukuje, monitoruje je, wykorzystuje i rozpowszechnia. Wobec powyższego koncept tego rodzaju zachowań powinien obejmować zarówno działania zamierzone, jak i podejmowane przypadkowo, w toku pozyskiwania informacji. Same procesy informacyjne – na co zwraca uwagę w dalszej części rozdziału – mają w literaturze wiele określeń, jak: pozyskiwanie informacji, poszukiwanie informacji, przypadkowe i nieintencjonalne pozyskiwanie informacji, wyszukiwanie czy wykorzystanie informacji. Autorka odwołuje się do wcześniejszych ustaleń Roberta S. Taylora[10] na temat zachowań informacyjnych. Nawiązuje do jego rozważań i określa tego typu zachowania jako (…) *wszelkie czynności, które sprawiają, że informacja staje się użyteczna*[11]. Na zakończenie tej części opracowania przedstawia ogólną kategoryzację zachowań informacyjnych. Rozpoznanie

[9] M. Krakowska, *Zachowania informacyjne*…, s. 66.

[10] R.S. Taylor, *Information use environments*, w: *Progress in Communication Sciences*, B. Dervin, M.J. Voight (red.), New York 1991, s. 217–255.

[11] M. Krakowska, *Zachowania informacyjne*…, s. 31.

i opisanie ich wybranych kontekstów stało się dla autorki podstawą do dalszego rozpatrywania tego zagadnienia.

W rozdziale drugim *Interdyscyplinarne perspektywy zachowań informacyjnych człowieka* rozwija tę problematykę i zwraca uwagę na konieczność prowadzenia interdyscyplinarnych badań, z wykorzystaniem wiedzy z zakresu informatologii, nauk społecznych, psychologii oraz kognitywistyki. Krakowska przedstawiła zachowania informacyjne w ujęciu kognitywnym, afektywnym, społecznym i ewolucyjnym. Uwzględniła przy tym takie uwarunkowania, jak: potrzeby informacyjne, intencje, emocje, habitus czy bariery informacyjne. Prowadzone przez nią analizy wskazują, że zachowania informacyjne mają dynamiczną naturę. Wykorzystanie przez autorkę różnych metod badawczych i wszechstronne podejście do badanego zagadnienia pozwala czytelnikowi na lepsze zrozumienie procesów, jakie jednostka inicjuje wobec informacji, a także tego, jak jej doświadcza. Człowiek ze względu na różne uwarunkowania (społeczne, psychologiczne, ekonomiczne, behawioralne) może odmiennie reagować na tę samą informację, co prowadzi do inforóżnorodności przestrzeni i środowiska informacyjnego. Skutkuje to brakiem możliwości wypracowania schematu zachowań, co jednocześnie sprzyja szerokiemu analizowaniu ludzkiej aktywności w sferze indywidualnych oraz grupowych zachowań informacyjnych. Dla naukowców zajmujących się tą problematyką jest to korzystne, duży obszar badawczy daje bowiem możliwość poznawczego otwarcia się na opisywaną kwestię. Przedstawione w tej części koncepcje, zjawiska i komponenty zachowań informacyjnych ułatwiają czytelnikowi zrozumienie problematyki, a dla autorki są podstawą do budowania nowego konceptu, tj. epistemicznej bańki informacyjnej.

Rozdział trzeci, czyli *Kontekst oraz przestrzeń zachowań informacyjnych człowieka*, zasługuje na szczególną uwagę, dotyczy bowiem dwóch elementów najważniejszych dla zrozumienia zjawiska zachowań informacyjnych człowieka. Kontekst, o którym pisze badaczka, to istotne ogniwo badań informatologicznych, a jego wielowymiarowość ma wpływ na zachowania informacyjne. Krakowska zwraca uwagę, że kontekst (…) *określa również przestrzeń informacyjną, środowisko, infosferę, inforóżnorodność – zarówno fizycznej, jak i niematerialnej przestrzeni*[12] i sam może pozostawać określony bądź nieokreślony. W takim przypadku – jak zaznacza autorka – wypracowanie uniwersalnej definicji kontekstu jest utrudnione. Tym bardziej że człowiek uczestniczący w procesie pozyskiwania informacji w różny sposób postrzega przestrzeń i środowisko informacyjne, w którym zdobywa informacje. Ponadto zmieniające się formy komunikacji i dynamiczne zmiany w infosferze kształtują to środowisko i sprawiają, że jest ono niejednorodne, zmienne i uzależnione m.in. od czynników: społecznych, ekonomicznych i politycznych. W związku z tym analizując

[12] Tamże, s. 127.

zachowania informacyjne, należy uwzględnić dodatkowe elementy, takie jak: środowisko, społeczność, ogólne tło, w którym dzieje się sprawczość informacyjna[13], oraz intencjonalność, przypadkowość tych zachowań. Poza tym poszczególne sfery informacyjne mogą się zmieniać, rozbudowywać i przenikać. W rezultacie, o czym pisze autorka monografii, człowiek mimo że tworzy własną przestrzeń informacyjną, może funkcjonować w wielu innych, z których czerpie wiedzę, nie zawsze czyniąc to świadomie. Krakowska zwraca uwagę, że tego rodzaju miejsca informacyjne mogą mieć wpływ na zachowania informacyjne jednostki. Nadmiar danych pochodzących w dużej mierze ze środowiska wirtualnego powoduje potrzebę ograniczenia i wykształcenia procesów ochronnych wobec stale rozwijającej się infosfery. Podjęta przez autorkę próba wypracowania uniwersalnej definicji kontekstu ma na celu pomoc w wyznaczeniu zmiennych, które wpływają na zachowania informacyjne jednostki.

Interdyscyplinarne refleksje nad kontekstem i przestrzenią zachowań informacyjnych człowieka stały się dla badaczki podstawą do opracowania nowego konceptu, który wskazała w tytule monografii. Rozważania na temat epistemicznej bańki informacyjnej oraz innych zamkniętych przestrzeni informacyjnych zawarła w dwóch ostatnich rozdziałach. W rozdziale czwartym zatytułowanym *Bańki: filtrująca, epistemiczna i informacyjna oraz komory echa – charakterystyka zjawisk* Krakowska skupia się na zjawisku zamkniętych przestrzeni informacyjnych, które ukształtowały epistemiczną bańkę informacyjną. Formowanie się takich przestrzeni jest związane z infosferą. Nadmiar informacji powoduje reakcję obronną przed szumem informacyjnym i często skutkuje tym, że ludzie sięgają po zaawansowane sposoby i narzędzia ograniczające negatywne konsekwencje. Zjawisko bańki filtrującej jest powszechne. Algorytmy powodują, że człowiek wielokrotnie korzysta wyłącznie z treści jemu dedykowanych, gdyż odrzucają te, które nie pasują do jego wizji świata. Bańka ta uniemożliwia jednostce zetknięcie się z różnymi tematami. Algorytmy, choć momentami wygodne i pomocne, ograniczają kreatywność jednostki i powodują, że koncentruje się na gotowej, skonfigurowanej treści. Niesie to ze sobą wiele zagrożeń, m.in. problemy o podłożu socjalnym (jednostka ma kontakt jedynie z ludźmi o podobnych poglądach). Zamknięty obieg informacji prowadzi do wytworzenia zjawiska określanego mianem komory echa. Mimo wszystko człowiek może podjąć działania, by zwiększyć różnorodność oferowanych mu treści i ograniczyć wpływ algorytmów, o czym autorka pisze w recenzowanej monografii.

Krakowska w tym rozdziale poddała wnikliwemu rozbiorowi strukturę, cechy, uwarunkowania bańki filtrującej, bańki epistemicznej oraz wysp poznawczych[14]

[13] Tamże, s. 167.

[14] Wyspa poznawcza (ang. *cognitive island*) – koncepcja odnosząca się do sytuacji, kiedy przynależność do grupy ekspertów w jakiejś dziedzinie wiedzy może być określona tylko przez członków tej grupy,

i komory echa. Terminu „bańka filtrująca" często używa się zamiennie z określeniem „bańka informacyjna", co wynika z braków w terminologii. Zdaniem autorki w doprecyzowaniu definicji mogłoby pomóc sięgnięcie po wybrane zagadnienia z obszaru zachowań informacyjnych i spojrzenie na nie przez pryzmat bańki informacyjnej. Potwierdza, że różnego typu bańki i konceptualne geografie informacyjne (środowisko informacyjne, przestrzeń informacyjna, horyzonty oraz krajobrazy informacyjne, indywidualne przestrzenie informacyjne, tymczasowe miejsca informacyjne) mogą się przenikać, wywołując zmiany w zachowaniach informacyjnych i relacjach społecznych. Zwraca uwagę na zjawisko gatekeepingu[15] w zamkniętych przestrzeniach i manipulowania informacją. Wspomniane bańki mogą, zdaniem badaczki, stanowić podstawę do opisania zjawiska bańki epistemicznej. Jest to:

> (…) społeczna, nietrwała struktura epistemiczna, w której podmiot poznawczy często przypadkowo i nieświadomie, nieintencjonalnie pomija różne informacje, operując strukturą poznawczą ograniczającą kognitywne procesy rozumienia rzeczywistości i tworzenia wiedzy. To przestrzeń informacyjna wynikająca z architektury środowiska informacyjnego i schematów komunikacji społeczności, łączącej sieci społecznościowe, media i inne źródła informacji, a także zachowania informacyjne wynikające z norm i światopoglądu jednostki, które dzieli z grupą. (…) Charakterystyczne dla bańki epistemicznej jest ograniczenie dostępu do zasobów informacji, brak dostępu do informacji, kreowanie przestrzeni informacyjnej, która składa się z umiarkowanej liczby źródeł informacji, nierozbudowanych horyzontów informacyjnych, które mapują (umieszczając także w umysłowej reprezentacji) wyselekcjonowane i najbliższe, łatwo dostępne źródła informacji, o których jednostka wie i z których korzysta[16].

Bańka epistemiczna może powstawać także w wyniku celowego działania jednostki, która sięga wyłącznie po odpowiadające jej informacje, co może prowadzić do selektywnej ekspozycji (ang. *selective exposure*). Człowiek, tworząc tego rodzaju filtr, ogranicza swoje procesy poznawcze, co może skutkować pojawieniem się dystansu poznawczego. Autorka, omawiając zjawisko bańki epistemicznej, wskazuje, że procesy poznawcze, które ją kształtują, mogą prowadzić do powstania bańki

domeny. Zob. K. Werner, *Poznawcze zamknięcie. Strukturalna niewiedza a problem racjonalności*, „Przegląd Filozoficzny" 2021, nr 1 (117), s. 20.

[15] Gatekeeping – selekcjonowanie i kontrolowanie informacji. Koncepcja osadzona w różnych dziedzinach nauki. Dotyczy zarówno indywidualnych jednostek, jak i organizacji i instytucji kontrolujących dostęp do informacji. Zob. M. Krakowska, *Zachowania informacyjne*…, s. 208–214.

[16] Tamże, s. 178.

poznawczej[17]. Jej zdaniem poznanie epistemiczne (…) *odnosi się do rozpoznania sposobów, w jakie ludzie zdobywają, konstruują, rozumieją i wykorzystują wiedzę*[18]. W przypadku gdy jednostka sięga po wiedzę spoza epistemicznie ograniczonej przestrzeni, opisywane zjawisko ulega zminimalizowaniu, a w sytuacji dalszego poszerzania ścieżek jej pozyskiwania może dojść do rozpadu tytułowych baniek, które mają nietrwałą strukturę.

Rozważania na ten temat autorka kontynuuje w ostatnim rozdziale zatytułowanym: *Epistemiczna bańka informacyjna i jej interdyscyplinarne determinanty w kontekście zachowań informacyjnych*. Podjęła w nim próbę rozpoznania czynników wpływających na specyfikę zachowań informacyjnych oraz zmiennych i koncepcji kształtujących epistemiczne bańki informacyjne. Dokonała pogłębionej analizy tego zjawiska na podstawie wybranych determinant: ewolucyjnych, poznawczych, afektywnych i społecznych. Odwołanie się do nauk społecznych, psychologicznych, biologicznych, kognitywnych, informatologii umożliwiło badaczce wykazanie, że zjawisko bańki może wpływać na zachowania informacyjne. W ten sposób uzyskała podstawę i szeroką perspektywę do dalszego badania z wykorzystaniem nowego konceptu praktyk informacyjnych podejmowanych przez jednostkę. Krakowska zwróciła uwagę na najważniejszą właściwość zachowań informacyjnych, a mianowicie na ich wielowymiarowość, co wynika z cech jednostki inicjującej. Człowiek podejmuje tego rodzaju zachowania na różne sposoby, zarówno świadomie, jak i nieświadomie. Funkcjonuje w przestrzeniach informacyjnych, które się przenikają. Wprawdzie otaczający świat i zachodzące w nim procesy, wpływając na zachowania informacyjne, mogą zamykać go w konkretnym otoczeniu informacyjnym, ale jak wykazano w monografii, człowiek ma możliwość oddziaływania na otaczającą przestrzeń informacyjną i na jej kształt.

Rozważania na temat zachowań informacyjnych jednostki prowadzone przez autorkę w odniesieniu do sformułowanych we wstępie celów szczegółowych, zaowocowały stworzeniem nowej koncepcji. Według niej epistemiczna bańka informacyjna:

> (…) konsoliduje cechy, atrybuty niejednorodnych, heterogenicznych zachowań informacyjnych, wskazuje na ich wielowymiarowość i wieloaspektowość, specyfikę zachowań informacyjnych, które mogą być świadome lub nieuświadomione, celowe lub nieintencjonalne, przypadkowo podejmowane, związane

[17] Bańka poznawcza (ang. *cognitive bubble*) – powstaje w wyniku działania ludzkiego systemu poznawczego „(…) który przetwarza ograniczoną ilość informacji ze względu na ograniczony czas oraz pojemność obliczeniową struktur kognitywnych". Zob. M. Krakowska, *Zachowania informacyjne*…, s. 182–183.

[18] Tamże, s. 171.

> z każdym sensomotorycznym, fizjologicznym, kognitywnym i afektywnym doznawaniem, doświadczeniem informacji i jej aktywnym praktykowaniem, co dotyczy szeregu różnorodnych aktywności i sprawczości człowieka w odniesieniu do informacji[19].

Tego rodzaju bańki bardzo często wpływają na zachowania informacyjne w hermetycznym otoczeniu informacyjnym danej jednostki. Ich wielowymiarowość i oddziaływanie skłania do prowadzenia dalszych badań w tym obszarze, tym bardziej że cechy tożsamości osobistej epistemicznej bańki informacyjnej można rozpatrywać na trzy sposoby, a mianowicie:

> (…) po pierwsze, poprzez jednostkowe zachowania i atrybuty konstytuujące ją. Po drugie, poprzez indywidualnie tworzony konstrukt, który konstytuowany jest w szerszej perspektywie – społecznej, kolektywnie wytwarzanej epistemicznej bańce informacyjnej. (…) Po trzecie, jako zjawisko charakterystyczne dla całej społeczności, ogólne, poprzez szeroką perspektywę epistemicznej bańki informacyjnej skonstruowanej z normatywnych cech i uwarunkowań, kontekstu i przestrzeni informacyjnej, w której funkcjonuje cała społeczność, kultura społeczna lub epistemiczna, cała domena (dziedzina)[20].

Wypracowana przez autorkę definicja epistemicznej bańki informacyjnej wraz z jej cechami tożsamości osobistej może być pomocna w monitorowaniu stopnia wpływu różnego typu zjawisk na zachowania informacyjne człowieka i jego aktywność w infosferze. Badaczka na zakończenie przedstawia obszary, które powinny zostać objęte dalszymi pracami, w kontekście zachowań informacyjnych, m.in. zachowań w środowisku informacyjnym, social mediach czy wpływu instytucji na kształtowanie bądź rozszczelnianie baniek informacyjnych. Jest to katalog otwarty, gdyż zachowania informacyjne stale się zmieniają.

Podsumowując, mamy do czynienia z rzetelną pracą naukową, zawierającą nowatorskie spojrzenie na opracowywane zagadnienie. Książka autorstwa Moniki Krakowskiej to ciekawa lektura dla osób zainteresowanych informatologią oraz nowymi zjawiskami kształtującymi zachowania informacyjne człowieka. Głównymi zaletami tej publikacji są podjęty w niej temat, sposób jego ujęcia i prezentacji oraz przedstawione wnioski. Szczególnie warto podkreślić prekursorskie spojrzenie na różne aspekty zachowań informacyjnych i wykorzystanie przez autorkę modeli, teorii i koncepcji ugruntowanych w informatologicznych badaniach aktywności informacyjnych, których dotychczas nie analizowano dogłębnie w polskiej

[19] Tamże, s. 274–275.

[20] Tamże, s. 274.

literaturze przedmiotu. Pozwoliło to na przedstawienie atrybutów epistemicznej bańki informacyjnej, jej wielowymiarowości, dynamiki i różnorodności, a tym samym na zbudowanie podstaw do dalszych interdyscyplinarnych badań nad tym konceptem i zachowaniami informacyjnymi człowieka.

Dr Iwona Osłowska

Kontakt: i.oslowska@wp.pl

PRACE KONKURSOWE

Wojna i konflikt w cyberprzestrzeni. Piąty teatr wojny[1]

War and conflict in cyberspace. The fifth theatre of war

MACIEJ HEROMIŃSKI

Autor niezależny

https://orcid.org/0009-0007-4137-5326

Przegląd Bezpieczeństwa Wewnętrznego, 2024, nr 30: 185–211

https://doi.org/10.4467/20801335PBW.24.008.19610

ARTYKUŁ

Abstrakt

Celem artykułu jest przedstawienie genezy cyberprzestrzeni oraz typologii zagrożeń związanych z działaniami prowadzonymi w tej sferze zarówno przez podmioty państwowe, jak i pozapaństwowe. Dokonano systematyzacji pojęć z zakresu cyberbezpieczeństwa, zwłaszcza cyberprzestrzeni, która jest traktowana jako nowy teatr wojny, oraz zaprezentowano, jakie właściwości omawianego zjawiska mogą zostać wykorzystane do prowadzenia działań destrukcyjnych w przestrzeni cyfrowej oraz w świecie rzeczywistym. Cyberprzestrzeń staje się dogodnym obszarem do realizacji efektywnych działań, które służą unieszkodliwieniu przeciwnika w krótkim czasie i przy niewielkim nakładzie sił. Autor omówił przykłady realizacji takich działań z pierwszych dwóch dekad XXI w.: cyberwojnę w Estonii, izraelsko-amerykańskie operacje przeciwko irańskim systemom teleinformatycznym oraz cyberstarcia Stanów Zjednoczonych Ameryki z Chinami.

Słowa kluczowe

cyberprzestrzeń, cyberwojna, teatr wojny, cyberataki, Estonia, Federacja Rosyjska, USA, Izrael, Iran, Chiny

[1] Artykuł powstał na podstawie pracy licencjackiej pt. *Wojna i konflikt w cyberprzestrzeni. Piąty teatr wojny* obronionej na Wydziale Nauk Społecznych Uniwersytetu Humanistyczno-Przyrodniczego im. Jana Długosza w Częstochowie (obecnie Uniwersytet Jana Długosza w Częstochowie). Praca została wyróżniona w XII edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

Abstract

The aim of this article is to present the genesis and typology of cyberspace and the threats that result from activities carried out in this area by state and non-state entities. The basic concepts, especially cyberspace, which is treated as a potential new theater of war, have been systematized. It was also presented the characteristics of the studied phenomenon from the point of view of using it to carry out destructive activities in the digital space and in the real world. Cyberspace is becoming an area for carrying out effective activities that serve to neutralize the enemy in a short time and with little effort. To prove his theses, the author uses numerous examples from the actual international relations, such as: the cyberwarfare in Estonia, the Israeli-American operations against Iranian ICT systems and the cyber-clashes between the United States of America and China.

Keywords

cyberspace, cyberwarfare, theater of war, cyberattacks, Estonia, Russian Federation, US, Israel, Iran, China

Wprowadzenie

Wojny towarzyszą ludzkości od początku jej istnienia. Są one wynikiem przede wszystkim ludzkiej skłonności do przemocy, chciwości oraz chęci zdobycia bogactw czy sławy. Oblicze działań wojennych na przestrzeni dziejów się zmieniało, na co miało wpływ kilka czynników, ale do najważniejszych z nich można zaliczyć rozwój technologiczny, społeczny oraz ideologiczny.

Dzięki osiągnięciom technologicznym człowiek tworzył nowe wynalazki i systemy uzbrojenia. Miały się one przyczynić do skuteczniejszego prowadzenia działań militarnych oraz umożliwić najtańszą i najbardziej skuteczną likwidację przeciwników. W ten sposób stworzono m.in. proch strzelniczy, następnie telegram, kolej, radio, telefon, silniki parowe, a później spalinowe, komputery oraz Internet. Rozwój technologiczny przyczynił się również do powstania nowych teatrów wojny. Najstarszym z nich jest przestrzeń lądowa. Wraz z rozwojem żeglugi kolejnym miejscem starć stron konfliktu stała się przestrzeń morska. W związku ze skonstruowaniem pierwszego samolotu i praktycznym wykorzystaniem go w locie powstała następna przestrzeń wojenna – obszar powietrzny. W czasie zimnej wojny człowiek rozpoczął ekspansję w kosmosie, który stał się nowym obszarem rywalizacji państw. Za kolejny teatr wojny uważa się cyberprzestrzeń. Celem artykułu jest przedstawienie jej genezy oraz typologii zagrożeń związanych z prowadzeniem działań przy jej wykorzystaniu.

Zagadnienie zostało omówione na przykładach działań na terenie Estonii, Syrii, Iranu oraz Stanów Zjednoczonych.

Początkowo pojęcie cyberprzestrzeni istniało jedynie w literaturze. Przedstawiono ją np. w publikacjach *Neuromancer* Williama Gibsona (1984 r.), *True Names* Vernora Vinge'a (1981 r.) czy *Web of Angels* Johna M. Forda (1980 r.). Naukowcy z całego świata postawili sobie za cel urzeczywistnienie tychże wizji. Popularność zyskał głównie obraz wykreowany przez Gibsona. Zakładał on, że cyberprzestrzeń to niematerialny, nierealny obszar, który jest wypełniony mnóstwem danych w postaci cyfrowej, a także strefa potencjalnego konfliktu interesów wielkich koncernów. Duży wpływ na pojmowanie tego pojęcia miał Neal Stephenson, autor powieści *Snow Crash* (1989 r.). W swojej twórczości głosił koncepcję, która wskazywała, że cyberprzestrzeń może zostać ukazana w postaci graficznej (takie przedstawienie jest widoczne w filmie *Matrix* w postaci ciągu liczb pojawiających się z góry do dołu ekranu).

Współcześnie to pojęcie jest definiowane jako nieograniczony (pod względem zasięgu i swobody korzystania) środek komunikacji międzyludzkiej. Zaczęto je również utożsamiać z Internetem, jest to jednak uproszczenie, gdyż cyberprzestrzeń składa się z elementów fizycznych (takich jak komputery) oraz niefizycznych (nie mają one granic geograficznych czy fizycznych; można zaliczyć do nich wszelkie oprogramowania lub wspomniany Internet).

Rozwój fizycznych środków teleinformatycznych rozpoczął się już w drugiej połowie XIX w., kiedy wynaleziono telegrafię i telefonię. Wydarzenia te dały początek myśli technologicznej nakierowanej na przesyłanie informacji w nieograniczony sposób. Kolejnym krokiem w tworzeniu cyberprzestrzeni było wynalezienie radiotelefonu oraz zwiększenie efektywności druku na początku XX w. Największy przełom naukowy, nazywany komputeryzacją, dokonał się w trakcie i po zakończeniu zimnej wojny. Trudno jednak wskazać dokładny czas rozpoczęcia tego procesu. Przyjmuje się, że nastąpiło to w drugiej połowie XX w. wraz z początkiem rewolucji informatycznej, której efekty są szczególnie widoczne w XXI w. Wpłynęła ona na większość sfer życia człowieka – kulturową, społeczną, gospodarczą czy polityczną.

Pierwotnie technologia teleinformatyczna była wykorzystywana głównie przez wojsko, jednak z czasem stała się bardziej dostępna i została rozpowszechniona również w sektorze cywilnym. Postawiło to nowe wyzwania przed władzami państw i organizacji międzynarodowych, które przeniosły część swojej działalności do cyberprzestrzeni. Tym samym pojawiły się nowe zagrożenia związane z tą sferą. Dzielą się one na dwie podstawowe kategorie: zagrożenia ustrukturalizowane i nieustrukturalizowane. Pierwsze z nich są związane z działalnością zorganizowanych grup, które dysponują wyspecjalizowanym sprzętem technicznym. Grupy te najczęściej motywują swoje działania celami politycznymi, wojskowymi, religijnymi i gospodarczymi. Do zagrożeń ustrukturalizowanych należą: cyberterroryzm,

cyberszpiegostwo, operacje zbrojne w cyberprzestrzeni oraz cyberwojna. Zagrożenia nieustrukturalizowane natomiast cechują się niskim stopniem zorganizowania. Prowadzone są z zamiarem osiągnięcia celów politycznych, społecznych lub indywidualnych. Do tego typu zagrożeń zalicza się: haking, haktywizm, zwłaszcza haktywizm patriotyczny, oraz cyberprzestępczość. Warto jednak podkreślić, że granice między tymi kategoriami są płynne i mogą się dynamicznie zmieniać. To znaczy, że zagrożenia nieustrukturalizowane mogą się przerodzić w ustrukturalizowane, np. w momencie, gdy kilku samotnych hakerów zdecyduje się współpracować w ramach organizacji terrorystycznej.

Rosyjska dezinformacja w cyberprzestrzeni

Dezinformacja stanowi jedno z najbardziej efektywnych narzędzi realizowania polityki. Polega na przeprowadzaniu różnego rodzaju operacji psychologicznych w celu wymuszenia na ofierze (odbiorcy) określonego zachowania, ukrycia swoich prawdziwych zamiarów i stworzenia fałszywej rzeczywistości, m.in. na wykorzystywaniu fałszywych lub na wpół prawdziwych informacji. Podmiot będący celem ataku często nie jest świadomy skali zagrożenia z racji deficytu swojej wiedzy, stąd też jego potencjalna reakcja może okazać się nieskuteczna. Dezinformacja sprowadza się również do manipulowania prawdziwymi informacjami przez nieujawnianie lub zmianę ich treści. W ten sposób stwarza się częściowo fałszywą wiadomość, która może ułatwić wpłynięcie na decyzję albo opinię odbiorcy lub całych grup społecznych. Istotnym elementem odróżniającym dezinformację od wprowadzania w błąd jest czas oddziaływania. Pierwsza z nich przewiduje, że fałszywe informacje mają wpływać na ofiarę i jej decyzję w dłuższej perspektywie czasowej[2].

Współcześnie przestrzenią najczęściej wykorzystywaną do szerzenia dezinformacji jest cyberprzestrzeń. Wynika to z jej ogólnodostępności. Fałszywe dane mogą zostać szybko rozpowszechnione na całym świecie, bez generowania nadmiernych kosztów[3]. Metody wprowadzania tych fałszywych danych zmieniały się na przestrzeni lat. Na początkowym etapie stosowania dezinformacji wykorzystywano czynnik ludzki. Wraz z postępem technologicznym środkami manipulacji stawały się prasa, radio, telewizja, a obecnie również technologie teleinformatyczne[4].

[2] T. Kacała, *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego" 2015, nr 2, s. 51. https://doi.org/10.15804/ppk.2015.02.03.

[3] J. Gerlach, *Wpływ prasy, radia, telewizji i internetu na współczesne zachowania nabywcze*, „Współczesne Problemy Ekonomiczne" 2018, nr 2, s. 10. https://doi.org/10.18276/wpe.2018.18-01.

[4] V. Volkoff, *Dezinformacja – oręż wojny*, Warszawa 1991, s. 119.

Jednym z krajów stosujących dezinformację na wielką skalę jest Federacja Rosyjska (FR). Rozwój rosyjskiej dezinformacji przypadł na okres rewolucji bolszewickiej, ale jej początki sięgają czasów carskich. Początkowo służyła ona wprowadzaniu w błąd za pomocą spreparowanych informacji. Z czasem stała się narzędziem prowadzenia walki informacyjnej z blokiem zachodnim (szczególnie w okresie zimnej wojny).

Federacja Rosyjska wykorzystuje przestrzeń teleinformatyczną do szerzenia dezinformacji na skalę globalną. Nie postrzega jednak cyberprzestrzeni jako odrębnego teatru wojny. Przedstawiciele władz Rosji w oficjalnym przekazie nie używają określenia „cyberprzestrzeń", lecz „przestrzeń informacyjna". Jest ona eksploatowana do prowadzenia walki informacyjnej, która według FR polega na oddziaływaniu na świadomość danej populacji[5]. Realizowanie rosyjskich operacji w przestrzeni informacyjnej spoczywa na Federalnej Służbie Bezpieczeństwa FR (Федеральная служба безопасности Российской Федерации, FSB), Służbie Wywiadu Zagranicznego FR (Служба Внешней Разведки Российской Федерации, SWR), Głównym Zarządzie Wywiadowczym Sztabu Generalnego Sił Zbrojnych FR (Главное разведывательное управление Генерального штаба Вооружённых сил Российской Федерации, GRU FR) oraz Agencji Badań nad Internetem (Агентство интернет-исследований, do 2023 r. tzw. fabryka Prigożyna). Podlegają im różne rosyjskie agencje prasowe, takie jak Sputnik czy Baltnews, odpowiedzialne za rozpowszechnianie dezinformacji. Niektóre z nich przekazują wiadomości w wielu wersjach językowych[6]. Działania dezinformacyjne są prowadzone również za pomocą mediów społecznościowych, takich jak Facebook, X (dawniej Twitter), i serwisu YouTube oraz fałszywych kont zakładanych na forach lub w mediach społecznościowych przez tzw. trolle[7] czy boty[8].

---

[5] O. Bieniek, *Cyberprzestrzeń w rosyjskiej przestrzeni informacyjnej*, „Wiedza Obronna" 2017, nr 3–4, s. 42–43.

[6] T. Chłoń, K. Kozłowski, *Wybrane studia przypadku systemowych działań dezinformacyjnych: Rosja i Chiny*, w: R. Kupiecki i in., *Platforma przeciwdziałania dezinformacji: budowanie odporności społecznej. Badania i edukacja*, Warszawa 2021, s. 36-37.

[7] Słowo „troll" wywodzi się z mitologii greckiej i oznacza 'potwora'. W skandynawskich bajkach trollami są stworzenia psotne i podstępne. Współcześnie słowo to odnosi się do zjawiska trollowania (ang. *trolling*). Polega ono na działaniu mającym na celu wywołanie sporu między członkami grupy internetowej. Takie osoby często stosują agresywną i wulgarną retorykę. W swojej aktywności wykorzystują również elementy dezinformacji. Trolle najczęściej działają na forach i w grupach dyskusyjnych. Zob. D. Jachyra, *Trollowanie – antyspołeczne zachowania w Internecie, sposoby wykrywania i obrony*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Informatica" 2011, nr 28, s. 253.

[8] Boty to programy lub aplikacje, które po zaprogramowaniu wykonują określone czynności. Obecnie są wykorzystywane na wiele sposobów. Mogą służyć do publikowania określonych informacji na danej stronie internetowej bez ingerencji człowieka. Boty często są programowane tak, aby ich działania przypominały ludzkie zachowania. W ramach dezinformacji tego typu programy mogą być

Jednym z przykładów wpływu rosyjskiej dezinformacji w cyberprzestrzeni na określone grupy społeczne jest pierwsza cyberwojna w Estonii w 2007 r. Cyberwojna to skomplikowane zjawisko, polegające na wykorzystywaniu sprzętu teleinformatycznego do dokonywania ataków na systemy potencjalnych ofiar. Zasadniczymi celami prowadzenia tego typu działań są: pozyskanie informacji, które przechowuje się (gromadzi) w danej sieci, dokonanie zniszczeń w sieciach, modyfikacja danych lub przejęcie kontroli nad niektórymi funkcjami. Ustalenie granic cyberprzestrzeni jest niemożliwe, a co za tym idzie – nie sposób określić granic danego obszaru oddziaływania (zainteresowania) państwa, które prowadzi w niej działalność. Z tego powodu bardzo trudno rozstrzygnąć, kiedy zwykły atak na daną sieć informatyczną staje się działaniem wojennym.

Estonia po 1991 r. dążyła do odcięcia się od związków z Rosją. W tym celu ukierunkowała swoją politykę na zbliżenie z Zachodem. Rząd w Tallinie podjął starania o akces do NATO i Unii Europejskiej, które miały stanowić gwarancję bezpieczeństwa dla tego kraju w związku z jego niekorzystnym położeniem geopolitycznym[9]. Federacja Rosyjska, mimo że ostatecznie zaakceptowała niepodległość Estonii, nie pogodziła się z utratą wpływów w tej republice[10].

Estońska przestrzeń teleinformatyczna od początku lat 90. XX w. jest jedną z najbardziej rozwiniętych wśród państw europejskich. Obywatele za pośrednictwem internetu mogą np. brać udział w głosowaniach czy składać deklaracje podatkowe. Cyberprzestrzeń tego państwa była pierwszą wykorzystaną jako teatr wojny[11]. Jedną z przyczyn ataku w tej cyberprzestrzeni była decyzja rządu w Tallinie z 2007 r. o przeniesieniu pomnika radzieckiego żołnierza (znanego także jako Brązowy Żołnierz, pomnik Armii Czerwonej)[12] znajdującego się w centrum stolicy. Relokacja tego

stosowane do masowego, automatycznego wysyłania określonych informacji do wielu użytkowników internetu. Zob. A. Grycuk, *Fake news, trolle, boty i cyborgi w mediach społecznościowych*, „Analizy BAS" 2021, nr 1, s. 4–5; F. Bryjka, *Wykrywanie i zwalczanie dezinformacji – zarys skryptu. Materiał pomocniczy do sylabusa zajęć akademickich*, w: R. Kupiecki i in., *Platforma przeciwdziałania dezinformacji: budowanie odporności społecznej. Badania i edukacja*, Warszawa 2021, s. 114.

[9] Estonia graniczy z Litwą i Rosją, ma dostęp do Morza Bałtyckiego, a także bogatą linię brzegową. Jest zaliczana do państw znajdujących się w rosyjskiej strefie wpływów, a FR dąży do ich zwiększenia w regionie bałtyckim. Zob. P. Bryczek-Wróbel, *Sytuacja geopolityczna Estonii w polityce zagranicznej Federacji Rosyjskiej*, „Polityka i Społeczeństwo" 2021, t. 19, nr 3, s. 32. https://doi.org/10.15584/polispol.2021.3.2.

[10] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, s. 184.

[11] S. Wierzbicki, *Wojny cybernetyczne jako element niekonwencjonalnej konfrontacji międzypaństwowej. Pragmatyczna rzeczywistość, nieunikniona przyszłość*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2015, t. 2, nr 1, s. 140–141.

[12] Pomnik upamiętniający poległych w II wojnie światowej powstał w 1947 r., w okresie gdy Estonia była republiką związkową ZSRR. Przedstawia on bezimiennego żołnierza Armii Czerwonej, który

obiektu na podmiejski cmentarz wojenny spotkała się ze sprzeciwem mniejszości rosyjskiej zamieszkującej Estonię[13] oraz społeczeństwa Rosji[14], przez które pomnik Brązowego Żołnierza jest postrzegany jako symbol walki Związku Radzieckiego z nazistami. Społeczeństwo Estonii uznaje go natomiast za symbol okupacji radzieckiej, która trwała od 1940 r. do 6 września 1991 r. W odwecie FR przeprowadziła kampanię dezinformacyjną – forsowano tezę, że władze Estonii dążą do zlikwidowania pomnika. Spowodowało to zwiększenie napięcia na ulicach Tallina i doprowadziło do licznych demonstracji. W zamieszkach przeciwko decyzji estońskiego rządu wzięło udział ok. 1500 osób[15].

W związku z tym, że za potencjalnego inspiratora wydarzeń została uznana Rosja, konflikt ten nazywa się „rosyjsko-estońską wojną o historię"[16]. Wśród ekspertów nie brakuje opinii, że za częścią ataków mogli stać również haktywiści, działający niezależnie od rosyjskich władz, ale sympatyzujący z ich decyzjami[17]. Przeciwko estońskim systemom zastosowano liczne ataki typu DDoS[18]. Doszło do naruszenia infrastruktury krytycznej tego państwa. Strony rządowe oraz sektor prywatny, w tym serwisy informacyjne, oświatowe, strony bankowe oraz handlowe, zostały zablokowane na trzy tygodnie. Pierwszego z ataków dokonano 28 kwietnia 2007 r. przy użyciu sieci botnet. Szczytowy moment rosyjskiej ofensywy na estońską sieć nastąpił w obchodzonym przez Rosję Dniu Zwycięstwa, tj. 9 maja[19]. Trwał aż do 19 maja. Do prowadzenia działań wykorzystano w tym czasie ok. 85 000 zainfekowanych

w lewej ręce trzyma hełm. Mowa ciała (lekko pochylona głowa) może wskazywać na żałobę bohatera po poległych towarzyszach. Zob. A. Schmidt, *The Estonian Cyberattacks*, w: *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, J. Healey (red.), Vienna 2013, s. 2.

13 Na przełomie pierwszej i drugiej dekady XXI w. stanowiła ona ok. 24,8% ludności Estonii (ok. 320 000 osób). Zob. M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 186.

14 A. Schmidt, *The Estonian Cyberattacks*…, s. 1–2.

15 I. Juurvee, M. Mattiisen, *The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict*, International Centre for Defence and Security, sierpień 2020 r., https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf, s. 16–18 [dostęp: 8 IV 2024].

16 S. Wierzbicki, *Wojny cybernetyczne*…, s. 141.

17 M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 149.

18 Atak DDoS (ang. *distributed denial of service*) – atak na system komputerowy lub usługę sieciową przeprowadzony równocześnie z wielu komputerów w celu uniemożliwienia działania przez zajęcie wszystkich wolnych zasobów. Za: Wikipedia, https://pl.wikipedia.org/wiki/DDoS [dostęp: 8 IV 2024] – przyp. red.

19 W tym dniu każdego roku dochodziło do demonstracji przed usuniętym pomnikiem radzieckiego żołnierza. Po przeciwnych stronach stawała mniejszość rosyjska oraz Estończycy. Starcia ograniczały się jednak do potyczek słownych. W 2006 r. manifestacje zaczęły się nasilać. Zob. A. Schmidt, *The Estonian Cyberattacks*…, s. 2.

komputerów[20]. Wśród zaatakowanych systemów należy wskazać sieci dwóch największych banków w Estonii – Hansapanku i SEB Ühispanku, które były zmuszone do wstrzymania transakcji zagranicznych oraz zawieszenia wszystkich usług świadczonych w internecie. Estońskie banki oszacowały straty na kwotę ok. miliona dolarów[21]. Ofiarą padły również strony internetowe serwisów informacyjnych. Wśród nich znalazł się jeden z największych dzienników –„Postimees"[22].

W odpowiedzi na agresję na estońską cyberprzestrzeń państwa członkowskie NATO podjęły decyzję o wsparciu estońskiej obrony. W tym celu do Tallina wysłano grupę ekspertów w dziedzinie cyberbezpieczeństwa, którzy mieli wspomóc lokalnych informatyków w zneutralizowaniu skutków ataków. Niestety, pomoc ta okazała się niedostateczna i ujawniła bezsilność Sojuszu wobec tego typu zagrożeń[23]. Należy dodać, że incydentu związanego z rosyjskim atakiem nie uznano za wystarczający do uruchomienia art. 5 traktatu północnoatlantyckiego, ponieważ agresji na przestrzeń teleinformatyczną państwa członkowskiego NATO nie można było wówczas nazwać operacją militarną[24].

Sytuacja zmieniła się dopiero w 2016 r., kiedy podczas szczytu NATO w Warszawie więcej uwagi poświęcono cyberprzestrzeni. Uznano wtedy, że wrogie działania prowadzone w tym teatrze wojny wobec państw członkowskich Sojuszu będą stanowiły podstawę do uruchomienia art. 5. Sekretarz generalny Jens Stoltenberg zapowiedział, że cyberprzestrzeń będzie traktowana na równi z powietrzem, ziemią i morzem[25].

W konsekwencji wojny w estońskiej cyberprzestrzeni w 2011 r. podjęto decyzję o powołaniu specjalnej jednostki obrony cybernetycznej w Estońskiej Lidze Obrony (Cyber Defence Unit of the Estonian Defence League)[26]. W jej skład wchodzą

---

[20] A. Małecka, *Nation-State Cyber Operations Legal Considerations: An Estonian Case Study*, „Safety & Defense" 2021, t. 7, s. 101. https://doi.org/10.37105/sd.139.

[21] S. Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, „Journal of Strategic Security" 2011, t. 4, nr 2, s. 52. http://dx.doi.org/10.5038/1944-0472.4.2.3.

[22] S. Wierzbicki, *Wojny cybernetyczne*…, s. 141.

[23] J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, rozprawa doktorska, Białystok 2017, s. 271 (rozprawa jest dostępna w wersji elektronicznej: https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/5875/1/J_Worona_%20Cyberprzestrzen_a_%20prawo_miedzynarodowe_Status_quo_i_perspektywy.pdf).

[24] S. Wierzbicki, *Wojny cybernetyczne*…, s. 141–142.

[25] N. Bochyńska, *Art. 5 Traktatu NATO a działania w cyberprzestrzeni. Czy istnieją „granice" dla cyberwojny?*, CyberDefence24, 17 III 2022 r., https://cyberdefence24.pl/cyberbezpieczenstwo/art-5-traktatu-o-nato-a-dzialania-w-cyberprzestrzeni-czy-istnieja-granice-dla-cyberwojny [dostęp: 7 V 2022].

[26] K. Kaska, A.M. Osula, J. Stinissen, *The Cyber Defence Unit of the Estonian Defence League. Legal, Policy and Organisational Analysis*, Tallinn 2013, https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf, s. 13–14 [dostęp: 8 IV 2024].

ochotnicy, inżynierowie, pracownicy banków, korporacji i ministerstw. W razie ataku na przestrzeń teleinformatyczną jednostka ta ma podlegać dowództwu wojskowemu[27].

Ataki na estońską cyberprzestrzeń nie były szczególnie groźne dla obywateli Estonii, nie wpłynęły nawet w znaczącym stopniu na infrastrukturę krytyczną. Rosyjska agresja spowodowała głównie ograniczenia w sprawnym funkcjonowaniu państwa i społeczeństwa. Utrudniono bowiem komunikację i korzystanie ze środków finansowych, a dostęp do informacji ograniczono lub zablokowano. To, że skala oraz metody działań użyte przez agresora w tej cyberwojnie nie wyrządziły większych szkód, nie oznacza, że kolejny atak nie okaże się dużo poważniejszy i nie doprowadzi do większego paraliżu funkcjonowania struktur państwa i społeczeństwa[28].

Walka w cyberteatrze: Izrael–USA–Iran. Stuxnet, Duqu i Flame

Izrael, który powstał po zakończeniu II wojny światowej, znalazł się w niezwykle trudnej sytuacji geopolitycznej. Otaczały go państwa arabskie, których zamiarem była likwidacja państwa żydowskiego. Konflikt zainicjowany pod koniec lat 40. XX w. nieprzerwanie trwa do dziś. Izrael, chociaż walczący w osamotnieniu, nie tylko nie dał się pokonać, lecz także powiększył swoje terytorium kosztem sąsiadów.

Szczególnym zagrożeniem dla Tel Awiwu był irański program nuklearny. Projekt zakładał utworzenie w Iranie sieci 23 elektrowni atomowych[29]. Kraj ten był gotowy do jego realizacji już w 1959 r. Wtedy to Stany Zjednoczone sprzedały władzom w Teheranie pierwszy reaktor jądrowy. Z uwagi na wybuch rewolucji w 1979 r. plan został odroczony[30]. Po przejęciu władzy reżim Chomeiniego[31]

---

[27] K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 17, s. 25.

[28] S. Wierzbicki, *Wojny cybernetyczne*…, s. 142.

[29] M. Sahimi, *Iran's Nuclear Program. Part I: Its History*, 2 X 2003 r., https://www.iranwatch.org/library/sahimi-irans-nuclear-program-part-i-its-history-10-2-03 [dostęp: 7 V 2022].

[30] Pierwsze sprzeciwy wyrażano już w 1977 r., kiedy władza pod presją administracji amerykańskiego prezydenta Jimmy'ego Cartera nieco uelastyczniła swoje restrykcyjne rządy. Studenci i intelektualiści masowo kierowali petycje, w których domagali się przestrzegania zasad konstytucyjnych i liberalizacji życia społecznego, a podczas spotkań w Instytucie Goethego w Teheranie elity intelektualne po raz pierwszy publicznie skrytykowały legitymizację władzy Mohammada Rezy Pahlawiego. Zob. S. Mazurek, *Rewolucja islamska w Iranie – przyczyny, przebieg, konsekwencje*, „Nurt SVD" 2017, nr 1, s. 48.

[31] Ruhollah Chomeini (1902–1989) – ortodoksyjny wyznawca islamu, duchowny i polityk irański. Po 16-letnim wygnaniu powrócił do Iranu. W 1979 r. przeprowadził rewolucję i obalił monarchię. Doprowadził do ustanowienia państwa religijnego, czyli Islamskiej Republiki Iranu. Pozostał zagorzałym przeciwnikiem USA i innych państw Zachodu. Kierował licznymi przedsięwzięciami wspierającymi

podjął decyzję o wznowieniu prac nad programem nuklearnym. Miał on stać się czynnikiem rozwoju Iranu jako mocarstwa regionalnego. Podstawą koncepcji była działalność następujących ośrodków: stacji wzbogacania uranu w Komie, elektrowni atomowej w Buszehrze, stacji przetwarzania uranu w Isfahanie, centrum wzbogacania uranu w Natanz, fabryki ciężkiej wody w Araku oraz ośrodków badań atomowych (wśród wielu z nich można wskazać centra badań w Teheranie i w Bonabie)[32].

Pod koniec lat 90. XX w. wywiad Stanów Zjednoczonych i Izraela uzyskał dane, które wskazywały na istnienie tajnych planów rozwoju broni nuklearnej Iranu[33]. Irańska opozycja przedstawiła dowody świadczące o pracach prowadzonych nad rozwojem tego typu broni. Pod koniec 2002 r. podobne oskarżenia wobec teherańskiego reżimu wysunęły Stany Zjednoczone. Niepokój wśród elit politycznych USA i ich europejskich sojuszników wynikał z obawy przed rosnącym zagrożeniem dla Izraela, wojsk amerykańskich, z niepewnego status quo na Bliskim Wschodzie, a także możliwości rozpowszechnienia się broni masowego rażenia wśród ugrupowań terrorystycznych.

W celu udaremnienia dalszych prac nad produkcją broni jądrowej przez Iran zrealizowano wiele przedsięwzięć dyplomatycznych. Zabiegi te nie przyniosły jednak oczekiwanych rezultatów. Brak porozumienia z władzami Iranu zmusił państwa członkowskie oraz Radę Bezpieczeństwa ONZ do nałożenia na to państwo dotkliwych sankcji[34]. Irański reżim pomimo tych działań kontynuował rozwój technologii broni atomowej. Spowodowało to załamanie relacji na linii Tel Awiw––Teheran, które do 1979 r. opierały się na bliskiej współpracy. Iran podejrzewał Izrael o chęć ingerowania w jego sytuację wewnętrzną, strona izraelska zaś widziała w irańskim reżimie zagrożenie własnego bezpieczeństwa narodowego. Izrael zakładał w związku z tym przeprowadzenie uderzenia prewencyjnego, które miałoby na celu zatrzymanie rozwoju programu atomowego. Poglądy zbliżone do Tel Awiwu miały Stany Zjednoczone, ponieważ Iran stanowił zagrożenie amerykańskiej

rozwój radykalizmu islamskiego. Zob. J. Kukułka, *Historia współczesna stosunków międzynarodowych 1945–2000*, Warszawa 2007, s. 232–233; S. Jones, *The Islamic Republic of Iran: An introduction*, House of Commons Library, 11 XII 2009 r., https://researchbriefings.files.parliament.uk/documents/RP09-92/RP09-92.pdf, s. 8 [dostęp: 8 IV 2024].

[32] K. Szymczyk, *Irański program nuklearny jako czynnik warunkujący stosunki międzynarodowe w obszarze i poza obszarem MENA*, w: *Bezpieczeństwo narodowe i międzynarodowe w rejonie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*, R. Bania, K. Zdulski (red. nauk.), Łódź 2012, s. 148.

[33] Informacja na ten temat została przekazana opinii publicznej dopiero w 2002 r. Zob. M. Kaniewska, *Między kijem a marchewką – Organizacja Narodów Zjednoczonych wobec programu nuklearnego Iranu*, w: *Stabilizacja czy destabilizacja? Społeczność międzynarodowa wobec programu nuklearnego Iranu*, A. Malantowicz, Ł. Smalec (red. nauk.), Warszawa 2014, s. 56.

[34] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar…*, s. 254.

pozycji na Bliskim Wschodzie[35]. W przeciwieństwie do Izraela jednak amerykański rząd nie dopuszczał możliwości przeprowadzenia operacji militarnej. Waszyngton starał się także zahamować izraelskie dążenia do uderzenia wyprzedzającego. Dokonywał tego przez redukcję wsparcia militarnego wysyłanego władzom w Tel Awiwie. Ponadto rozmieszczenie ośrodków atomowych wymagałoby przeprowadzenia jednoczesnego bombardowania odległych od siebie celów. Realizacja operacji wojskowej, która miałaby zniszczyć irański przemysł atomowy, równałaby się ze stanowczą odpowiedzią militarną ze strony Teheranu. Izraelska agresja mogłaby się również spotkać z poważną reakcją świata arabskiego, w tym ugrupowań terrorystycznych (np. Hezbollahu). Obawiano się także zablokowania przez stronę irańską cieśniny Ormuz[36], która stanowi główny punkt transportu surowców energetycznych. Użycie broni konwencjonalnej nie gwarantowało przerwania prac nad programem atomowym, mogło jedynie doprowadzić do jego opóźnienia[37].

Przedstawiony bilans ryzyka, ewentualnych zysków i strat zmusił Izrael oraz Stany Zjednoczone do podjęcia innych kroków. Półśrodkiem w rozwiązaniu tego problemu było zaangażowanie służb specjalnych w dokonywanie zabójstw naukowców odgrywających najważniejszą rolę w realizacji programu atomowego. W wyniku tych pozamilitarnych działań w latach 2007–2012 zlikwidowano pięciu irańskich specjalistów, ale nie miało to istotnego wpływu na rozwój programu[38].

Kolejnym sposobem na zatrzymanie irańskich aspiracji było wykorzystanie cyberprzestrzeni. Izrael już na początku XXI w. dysponował rozwiniętą infrastrukturą teleinformatyczną. Ponadto miał doświadczenie w prowadzeniu działań ofensywnych w tym obszarze w związku ze zrealizowaną przez niego operacją „Orchard"[39].

---

[35] J. Dobbins i in., *Coping with a Nuclearizing Iran*, Santa Monica 2011, s. 11.

[36] H. Ajili, N. Rezaee, *Iranian Military Capabilities and Possibility of Blocking Hormuz Strait by Iran*, „Cywilizacja i Polityka" 2020, nr 18, s. 61. https://doi.org/10.15804/cip202005.

[37] J. Zanotti i in., *Israel: Possible Military Strike Against Iran's Nuclear Facilities*, Congressional Research Service, 28 IX 2012 r., https://sgp.fas.org/crs/mideast/R42443.pdf, s. 41–43 [dostęp: 7 V 2022].

[38] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 254.

[39] Operacja ta została przeprowadzona w 2007 r. na terytorium Syryjskiej Republiki Arabskiej i miała na celu zatrzymanie syryjskich aspiracji do zwiększenia wpływów w regionie. Syria dążyła do stworzenia broni jądrowej. Pierwszą elektrownię atomową zbudowała we współpracy z Koreańską Republiką Ludowo-Demokratyczną na początku XXI w. Izraelski wywiad uzyskał jednak informację, że jest ona wykorzystywana również w celach militarnych. Stanowiło to zagrożenie bezpieczeństwa Izraela. Rząd w Tel Awiwie podjął decyzję o interwencji zbrojnej na terenie tego państwa. W celu zabezpieczenia swojego lotnictwa przed systemami przeciwlotniczymi przeciwnika zastosowano ataki w cyberprzestrzeni. Izrael we współpracy z amerykańskimi agencjami opracował program SUTER. Powstał on w trzech generacjach. Pierwsza dawała możliwość śledzenia informacji pokazywanych na syryjskich radarach. Druga była bardziej agresywna – pozwalała na przejęcie kontroli nad siecią i sensorami ofiary ataku. Trzecia umożliwiała sterowanie systemami w zainfekowanej sieci

Rozwój zdolności w przestrzeni wirtualnej został wymuszony na Izraelu z powodu rosnącego zagrożenia cyberterroryzmem ze strony lokalnych grup terrorystycznych. Wewnątrz struktur izraelskich służb specjalnych zostały utworzone wyspecjalizowane zespoły do walki w przestrzeni teleinformatycznej.

Izraelskie możliwości oddziaływania w sieci przesądziły o formie działań, jakie zamierzano podjąć, aby powstrzymać irański program nuklearny. Za cel obrano zakłady produkujące wzbogacony uran. Uznano, że obiektem, którego uszkodzenie najskuteczniej wpłynie na rozwój broni jądrowej, będą wirówki służące do wytwarzania wzbogaconego uranu. Dlatego, aby je zniszczyć, postanowiono wprowadzić do oprogramowania sterującego pracą tych urządzeń wirus komputerowy o nazwie W32.Stuxnet (początkowo nazwany W32.Temphid)[40]. Ten akt sabotażu nie tylko nie pozwolił na oddzielenie uranu, lecz także doprowadził do trwałego uszkodzenia części zaatakowanych urządzeń[41].

Fora specjalistyczne zaczęły udostępniać informacje o tym złośliwym oprogramowaniu w czerwcu 2010 r. Pierwszy kontakt z wirusem miała białoruska firma VirusBlokAda[42] w dniu 17 czerwca. Stworzony przez nią raport na temat nowego zagrożenia wskazywał, że oprogramowanie powinno zostać zaliczone do kategorii najbardziej niebezpiecznych. Po zainfekowaniu komputera program rozpoczynał proces ukrywania swojej obecności w systemie. Wykorzystywał do tego luki oraz błędy systemu operacyjnego. Dodatkowo wirus dezorientował programy antywirusowe, co również wpływało na zdolność ukrycia swojej obecności na danym nośniku. W lipcu 2010 r. Siemens zaobserwował, że Stuxnet atakuje stworzone przez tę firmę systemy przemysłowe SCADA. W dniu 20 lipca przedsiębiorstwo Symantec wykryło łączność tego wirusa ze zdalnymi serwerami dowodzenia i kontroli. Ślady infekcji Stuxnetem odkryto w wielu państwach świata. Według przeprowadzonych badań zaatakowano ok. 100 000 komputerów, m.in. w Indiach, Indonezji, Chinach,

(w tym systemami rakietowymi lub radarami). SUTER sprawia, że operatorzy zaatakowanej sieci mają wrażenie, że system działa prawidłowo. W wyniku paraliżu systemów obrony przeciwlotniczej siły powietrzne Izraela dokonały skutecznego zniszczenia reaktora w okolicach miasta Dajr az-Zaur. Zob. S. Dygnatowski, P. Dygnatowski, Ł. Domżał-Drzewicki, *Analiza wykorzystania rozwiązań strukturalnych w obszarze cyberbezpieczeństwa na przykładzie operacji Orchard*, „Journal of KONBiN" 2019, t. 49, nr 1, s. 293–296. http://dx.doi.org/10.2478/jok-2019-0014.

[40] *Wirus Stuxnet (robak Stuxnet)*, w: *Vademecum bezpieczeństwa informacyjnego*, t. 2, O. Wasiuta, R. Klepka (red.), Kraków 2019, s. 514.

[41] J.P. Farwell, R. Rohozinski, *Stuxnet and the Future of Cyber War*, „Survival. Global Politics and Strategy" 2011, t. 53, nr 1, s. 28. https://doi.org/10.1080/00396338.2011.555586.

[42] Przedsiębiorstwo to zajmuje się dystrybucją oprogramowania antywirusowego. Zob. https://www.anti-virus.by/ [dostęp: 9 IV 2024].

Korei Południowej i Australii, przy czym 60 000 zainfekowanych systemów znajdowało się na terenie Iranu[43].

W 2010 r. irański prezydent Mahmoud Ahmedinejad potwierdził szkody wyrządzone przez robaka Stuxnet w infrastrukturze krytycznej. Przyjmuje się, że w wyniku serii ataków zostało uszkodzonych ok. 1000 wirówek działających w zakładach w miejscowości Natanz. Irańskie władze, manipulując danymi, nie podały dokładnych informacji na temat poniesionych strat[44]. W tym samym roku 30 września opracowano interesujący i precyzyjny raport na temat sposobu działania tego wirusa oraz jego specyfiki. W tym okresie wzrosło też zainteresowanie społeczności międzynarodowej problemem ataków w cyberprzestrzeni oraz pochodzeniem tego robaka. Eksperci zaznaczali, że poziom zaawansowania Stuxnetu wskazuje na to, że mógł on powstać tylko w wyspecjalizowanym ośrodku rządowym.

Władze Iranu od początku twierdziły, że inicjatorem tych ataków były Stany Zjednoczone, które współpracowały z Izraelem. Przy czym ograniczenie wysiłków Iranu ukierunkowanych na stworzenie broni jądrowej poparły również państwa arabskie, m.in. Arabia Saudyjska, Egipt czy Jordania, które obawiały się zbyt dużego wpływu reżimu ajatollahów na Bliskim Wschodzie. Obecnie jednak przyjmuje się, że za atakiem na irańską cyberprzestrzeń stały izraelskie służby specjalne, które współpracowały ze Stanami Zjednoczonymi. Państwa te uchodzą za jedne z najlepiej przygotowanych do działań militarnych w omawianym teatrze wojny[45].

Stuxnet nie był jedynym złośliwym robakiem wykorzystywanym w tym konflikcie. W październiku 2011 r. grupa informatyków z Uniwersytetu Technologii i Ekonomii w Budapeszcie odkryła złośliwe oprogramowanie Duqu. Jego nazwa pochodzi od pliku, który tworzył się na zainfekowanym systemie .DQ. Ustalono, że został on oparty na technologii oraz kodzie wykorzystanych do stworzenia Stuxnetu. Zasady jego działania były podobne do pierwowzoru, ale używano go do innych celów[46]. Zdolności keyloggera[47] pozwalały mu na rejestrowanie aktywności użytkownika komputera. Podobnie jak Stuxnet, Duqu cechował się wysokim poziomem skomplikowania, ale jego szczególnym atrybutem był trudny do zidentyfikowania język programowania. Zdolności Duqu były jednak znacznie ograniczone

[43] S. Wierzbicki, *Wojny cybernetyczne*…, s. 145.

[44] K. Kowalczewska, *Wpływ nowoczesnych technologii na współczesne konflikty zbrojne*, Warszawa 2022, s. 24.

[45] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 256–258.

[46] B. Bencsáth i in., *Duqu: A Stuxnet-like malware found in the wild. Technical Report by Laboratory of Cryptography and System Security (CrySys)*, 14 X 2011 r., https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf, s. 5 [dostęp: 8 IV 2024].

[47] Keylogger – rodzaj oprogramowania lub urządzenia rejestrującego klawisze naciskane przez użytkownika. Za: Wikipedia, https://pl.wikipedia.org/wiki/Keylogger [dostęp: 8 IV 2024] – przyp. red.

w porównaniu z możliwościami poprzednika. Ślad jego działalności wykryto w kwietniu 2011 r. (prawdopodobnie pierwszy atak z użyciem Duqu przeprowadzono pod koniec 2010 r.) i, jak się wydaje, mógł zostać wykorzystany do zainfekowania komputerów w ośmiu krajach, m.in. w Iranie, we Francji oraz w Indiach[48].

Duqu został zaliczony do grupy trojanów. Nie służył do ingerowania w integralność zainfekowanego systemu, lecz był stosowany jako program szpiegowski. Za jego pomocą cyberżołnierz mógł pozyskać dane zawarte na zaatakowanym komputerze, w tym informacje na temat używanych klawiszy, specyfikacje zainfekowanego sprzętu teleinformatycznego oraz innych urządzeń znajdujących się w jednej sieci, a ponadto mógł dokonywać zrzutów z ekranu danego komputera. Ten złośliwy program stanowi wręcz idealne narzędzie służące do rozpoznania infrastruktury informatycznej, nad którą można przejąć kontrolę przez uzupełnienie programu o komponenty Stuxnetu[49].

W listopadzie 2011 r. Iran potwierdził obecność Duqu w sieciach komputerowych związanych z programem atomowym. Strona irańska informowała, że skutecznie zwalcza ataki we własnej cyberprzestrzeni. Trudno jednak ocenić wiarygodność tego przekazu, ponieważ nie są znane ani konsekwencje ataków przeprowadzonych za pomocą tego złośliwego programu, ani szczegóły kontrakcji irańskich specjalistów[50].

W maju 2012 r. wykryto kolejny złośliwy program, który miał kilka cech wspólnych ze Stuxnetem i Duqu. Był to Worm.W32.Flame (ang. *flame* oznacza 'płomień', 'ogień')[51]. Grupy badawcze podjęły pracę nad analizą tego wirusa po ataku na systemy teleinformatyczne irańskiego Ministerstwa ds. Ropy Naftowej oraz inne podmioty związane z infrastrukturą energetyczną. Hakerzy za pomocą tego programu usuwali dane z twardych dysków komputerów znajdujących się w irańskim ministerstwie. Flame był bardziej skomplikowany niż oba wirusy przedstawione wcześniej. Prawdopodobnie został wykorzystany już kilka lat przed jego wykryciem, ale ustalenie dokładnej daty jego pierwszego użycia jest niemożliwe, gdyż w celu ukrycia tej informacji cyberżołnierze modyfikowali daty utworzenia zainfekowanych plików[52]. Na podstawie niektórych analiz wskazuje się, że być może

[48] S. Wierzbicki, *Wojny cybernetyczne*…, s. 143–145.

[49] B. Bencsáth i in., *The Cousins of Stuxnet: Duqu, Flame and Gauss*, „Future Internet" 2012, nr 4, s. 979–980. https://doi.org/10.3390/fi4040971.

[50] E. Chein, L. OMurchu, N. Falliere, *W32.Duqu. The precursor to the next Stuxnet*, https://www.usenix.org/system/files/conference/leet12/leet12-final11.pdf, s. 1–2 [dostęp: 7 V 2022].

[51] K. Majdan, *Wykryto nowe „cyberzagrożenie". „Z czymś takim jeszcze się nie spotkaliśmy"*, na Temat, 29 V 2012 r., https://natemat.pl/16397,wykryto-nowe-cyberzagrozenie-z-czyms-takim-jeszcze-sie-nie-spotkalismy [dostęp: 7 V 2022].

[52] B. Bencsáth i in., *The Cousins of Stuxnet*…, s. 980.

powstał on w 2008 r.[53] Został opracowany w celu pozyskiwania informacji z zaatakowanych komputerów. Podobnie jak Duqu wykorzystywał do tego keyloggery, ale miał także szeroki wachlarz innych narzędzi[54]. Przy ich użyciu haker mógł uzyskać kontrolę nad kamerą lub mikrofonem komputerowym i nagrywać obraz oraz dźwięki z otoczenia, uzyskiwać dostęp do podłączonych nośników danych czy też wykorzystać technologię Bluetooth do wyszukiwania telefonów w pobliżu zainfekowanego sprzętu[55].

Rozpowszechnienie Flame'a następowało w momencie podłączenia nośnika pamięci (za pomocą USB) do komputera stanowiącego cel ataku lub za pomocą lokalnej sieci. Program ten przez śledzenie ruchów w sieci tworzył listę haseł, a także pozyskiwał inne dane wrażliwe. Następnie przesyłał je do serwerów dowodzenia i kontroli. Po osiągnięciu zamierzonych celów wirus samoczynnie usuwał się z twardego dysku[56].

Chińsko-amerykańskie cyberstarcie

Współpraca chińsko-amerykańska o szczególnym charakterze została nawiązana po zakończeniu II wojny światowej. Relacje załamały się jednak po wojnie domowej wygranej w 1949 r. przez komunistów pod przywództwem Mao Tse-tunga. Doszło również do walk pomiędzy tymi państwami podczas wojny koreańskiej w latach 1950–1953. Unormowanie stosunków nastąpiło pod koniec lat 70. XX w., kiedy władze USA oficjalnie uznały Chińską Republikę Ludową (ChRL) za państwo. Relacje te jednak wciąż były napięte. Wynikało to z odmiennych stanowisk odnośnie do niezależności Tajwanu, nieakceptowania przez Waszyngton autorytarnego systemu politycznego Chin oraz braku poszanowania praw człowieka w tym państwie[57].

Po rozpadzie Związku Radzieckiego w 1991 r. rola USA na arenie międzynarodowej wzrosła. Wpisywało się to w ideę nowego ładu światowego, proklamowaną przez prezydenta George'a Busha. Zakładała ona wykorzystanie potencjału militarnego i ekonomicznego oraz instrumentów wpływu politycznego do kreowania

[53] A. Zakrzewski, *Jak to jest z tym Stuxnetem, Flamem, Duqu?*, „DLP Expert" 2013, nr 1, s. 9–13.

[54] *First Stuxnet – Now the Flame Virus*, The Availability Digest, czerwiec 2012 r., www.availabilitydigest.com/public_articles/0706/flame_virus.pdf, s. 2 [dostęp: 10 V 2022].

[55] J.P. Farwell, R. Rohozinski, *The New Reality of Cyber War*, „Survival. Global Politics and Strategy" 2012, t. 54, nr 4, s. 109. https://doi.org/10.1080/00396338.2012.709391.

[56] K. Zetter, *Odliczając do dnia zero. Stuxnet, czyli prawdziwa historia cyfrowej broni*, Gliwice 2014, s. 285–287.

[57] *1949–2023 U.S.-China Relations*, Council on Foreign Relations, https://www.cfr.org/timeline/us-relations-china [dostęp: 10 V 2022].

pozycji lidera w skali globalnej. Cele te zostały doprecyzowane przez prezydenta Billa Clintona, który jako priorytety polityki zagranicznej wskazał także wzmacnianie bezpieczeństwa, rozwijanie dobrobytu Stanów Zjednoczonych oraz promowanie demokracji[58]. Przedstawione założenia stanowiły przeszkodę w utrzymaniu stabilnych relacji z Chinami. Również dynamiczny rozwój ChRL i jej rosnące możliwości oddziaływania na politykę Azji Wschodniej oraz w przestrzeni globalnej wywoływały konflikt interesów między oboma państwami. Dlatego Stany Zjednoczone dążyły do działań mających na celu ograniczenie wzrostu chińskiej potęgi oraz wpływów w różnych rejonach świata (m.in. w Afryce, gdzie dochodziło do rywalizacji o surowce energetyczne). Kursy polityczne kolejnych amerykańskich prezydentów zakładały zmianę polityki zagranicznej, która miała obejmować sprawy dotyczące Azji Wschodniej[59].

Polityka Pekinu była ukierunkowana dwutorowo. Po pierwsze, skupiała się na utrzymaniu niepodległości, suwerenności oraz integralności terytorialnej ChRL, a po drugie, dążono do wprowadzania odpowiednich reform oraz wywierania wpływu w środowisku międzynarodowym. Warto podkreślić, że według oficjalnego stanowiska Pekinu te założenia miały być realizowane w sposób pokojowy. Wraz ze wzrostem chińskiego potencjału i wpływów władze ChRL zaczęły jednak ingerować w stosunki międzynarodowe z wykorzystaniem różnych narzędzi[60].

Wśród czynników, które miały wpływ na powstanie i narastanie napięcia między USA a ChRL, należy wskazać:

- brak wspólnego wroga – po upadku ZSRR nie pojawiły się zagrożenia, które wymagałyby wspólnego działania,
- wyrównanie poziomów rozwoju – wskazywana była rywalizacja między potęgą „wschodzącą", jaką były Chiny, a potęgą „schodzącą", reprezentowaną przez Stany Zjednoczone,
- różnice ideologiczne, czyli klasyczny konflikt pomiędzy ustrojem komunistycznym a demokratycznym[61].

Otwarte działania zbrojne między tymi państwami są jednak mało prawdopodobne. Wynika to głównie z tego, że zarówno Chiny, jak i Stany Zjednoczone

[58] J. Zając, *Polityka zagraniczna USA*, w: *Polityka zagraniczna. Aktorzy – potencjały – strategie*, Warszawa 2011, s. 61–64.

[59] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 297–298.

[60] J. Marszałek-Kawa, *Polityka zagraniczna ChRL: aspiracje, możliwości, paradoksy*, w: *Polityka zagraniczna. Aktorzy – potencjały – strategie*, T. Łoś-Nowak (red.), Warszawa 2011, s. 115.

[61] J.K. Park, *A Report of the CSIS Korea Chair. China–U.S. Relations in East Asia. Strategic Rivalry and Korea's Choice*, Center for Strategic and International Studies, kwiecień 2013 r., https://ciaotest.cc.columbia.edu/wps/csis/0028481/f_0028481_23160.pdf, s. 7–9 [dostęp: 8 IV 2024].

dysponują arsenałem broni atomowej[62]. Dlatego Pekin rozpoczął rozwijanie wielu projektów oraz programów, które można wykorzystać w ramach działań asymetrycznych i hybrydowych z zastosowaniem systemów zdolnych do niszczenia amerykańskich satelitów oraz realizacji operacji ofensywnych w cyberprzestrzeni[63].

Chińska Republika Ludowa w zakresie rozwoju nowoczesnych technologii informatycznych przez długi okres pozostawała daleko za stroną amerykańską. Ten stan rzeczy należy już jednak do przeszłości. Obecnie to właśnie Chiny nadają ton w obszarze nowych technologii, zwłaszcza tych wykorzystywanych w cyberprzestrzeni[64].

Rewolucja informatyczna w Chinach nastąpiła bardzo szybko, świadczy o tym m.in. ogromna liczba internautów w tym kraju. Powstało także wiele bardzo dużych korporacji, takich jak Baidu (która stworzyła wyszukiwarkę internetową), DXY.cn (media społecznościowe) czy Huawei (zajmujący się produkcją sprzętu komputerowego i telekomunikacyjnego)[65]. Ponadto w ChRL wyprodukowano komputery obliczeniowe, będące najprawdopodobniej najpotężniejszym sprzętem tego rodzaju na skalę światową. Są one wykorzystywane m.in. do łamania szyfrów oraz prowadzenia operacji militarnych w cyberprzestrzeni. W wyniku zaostrzającej się rywalizacji między ChRL a Stanami Zjednoczonymi oraz dynamicznego rozwoju technologii informatycznych konflikt między tymi państwami przeniósł się do cyberprzestrzeni[66].

Do pierwszego incydentu wynikającego z tej rywalizacji doszło w 1999 r. W związku ze zbombardowaniem przez lotnictwo NATO ambasady ChRL w Belgradzie – w ramach operacji militarnej prowadzonej przeciwko tzw. trzeciej Jugosławii – Chińczycy przeprowadzili w odpowiedzi serię masowych cyberataków[67]. Jednym z nich był atak typu DDoS, za pomocą którego na trzy dni zablokowano strony Białego Domu. Drugim modelowym działaniem chińskiego cyberwojska stało się masowe wysyłanie spamu na pocztę elektroniczną amerykańskiej administracji. W ten sposób zamierzano ją przeciążyć i sparaliżować. Ostatnim rodzajem ataku były włamania na strony internetowe Departamentu Energii oraz Departamentu Spraw Wewnętrznych, na których zamieszczono hasła sprzeciwu

---

62 Tamże.

63 S. Kumar, *Asymmetric Capabilities of China's Military*, Institute of Peace and Conflict Studies, 19 XI 2008 r., https://www.ipcs.org/comm_select.php?articleNo=2735 [dostęp: 10 V 2022].

64 F.S. Reeder i in., *Updating U.S. Federal Cybersecurity Policy and Guidance. Spending scarce taxpayer dollars on security programs that work*, Center for Strategic and International Studies, październik 2012 r., https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/121019_Reeder_A130_Web.pdf, s. 1–2 [dostęp: 8 IV 2024].

65 M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 307.

66 J. Carr, *Inside Cyber Warfare*: *Mapping the Cyber Underworld*, Beijing–Cambridge–Farnham–Köln–Sewastopol–Taipei–Tokyo 2010, s. 2.

67 Tamże.

wobec interwencji zbrojnej USA i państw NATO na obszarze Kosowa. Oficjalnie do przeprowadzonych ataków przyznały się grupy chińskich haktywistów. Ich działalność spotkała się z aprobatą władz[68].

Kolejne starcie w cyberprzestrzeni pomiędzy ChRL i USA nastąpiło w kwietniu i maju 2001 r. Operacje w tym przypadku były prowadzone przez obie strony. Ich przyczyną było zderzenie się w przestrzeni powietrznej nad Morzem Południowochińskim chińskiego myśliwca J-8 z amerykańskim samolotem zwiadowczym EP-3[69]. Incydent spowodował wzrost napięcia na linii Pekin–Waszyngton. W wyniku tego zdarzenia haktywiści ze Stanów Zjednoczonych dokonali włamań do ok. 1000 chińskich witryn internetowych. W odpowiedzi chińskie środowiska hakerów w maju przeprowadziły serię ataków na podobną liczbę amerykańskich stron. Tym razem jednak władze ChRL uznały działania własnych hakerów za sprzeczne z prawem i zakwalifikowały je jako cyberterroryzm[70].

W wyniku utraty poparcia władz część chińskich grup hakerskich przekształciła się w firmy zajmujące się bezpieczeństwem teleinformatycznym. W związku z pełną kontrolą przestrzeni teleinformatycznej w Chinach opisywane przedsiębiorstwa zostały jednak zmuszone do współpracy ze służbami specjalnymi Państwa Środka. Oficjalnie Pekin nigdy nie potwierdził kooperacji z sektorem prywatnych firm z branży bezpieczeństwa IT, ale większość ekspertów uważa, że chińskie władze korzystały ze złośliwego oprogramowania i technik stworzonych przez wspomniane grupy hakerskie[71].

Zmiana stanowiska Pekinu w związku z działalnością haktywistów w operacjach przeciwko Stanom Zjednoczonym była spowodowana koniecznością dokonania zmian w taktyce prowadzenia chińskich operacji w cyberprzestrzeni. Chińska Republika Ludowa skupiła się bowiem na skrytym działaniu na amerykańskich serwerach w celu pozyskiwania informacji niejawnych.

W latach 2002–2003 w ramach kampanii „Titan Rain"[72] Chińczycy włamali się za pomocą programów typu trojan m.in. do amerykańskich systemów Departamentu Obrony, Departamentu Stanu, Departamentu Energii, Departamentu Bezpieczeństwa Krajowego, komputerów struktur wchodzących w skład amerykańskiej

[68] B. Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, The US-China Economic and Security Review Commission, 9 X 2009 r., https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf, s. 36–37 [dostęp: 8 IV 2024].

[69] S. Wierzbicki, *Wojny cybernetyczne*…, s. 139.

[70] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 311–312.

[71] B. Krekel, *Capability of the People's Republic of China*…, s. 37–38.

[72] J. Andress, S. Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Waltham 2011, s. 11.

armii oraz NASA, a także do systemów informatycznych największych amerykańskich koncernów[73]. W wyniku tych działań ChRL uzyskała informacje dotyczące: systemów informatycznych wykorzystywanych w amerykańskich myśliwcach, danych technicznych napędów kosmicznych oraz planów paneli słonecznych wykorzystywanych w sprzęcie kosmicznym. Po ujawnieniu w 2005 r. tych ataków władze w Pekinie stanowczo zaprzeczyły, że są ich sprawcami[74].

W sierpniu 2006 r. ofiarą chińskiego cyberataku padł Pentagon. W wyniku włamania do wojskowej sieci NIPRNET grupy hakerskie z terytorium ChRL wykradły około 20 terabajtów danych[75]. W 2008 r. wykryto ingerencję w bazy danych prezydenckich kampanii wyborczych obu stron – Partii Republikańskiej i Partii Demokratycznej. Ślady pozostawione przez hakerów wskazywały, że ataki były przeprowadzone z terytorium Państwa Środka[76].

Do ponownego ataku na Pentagon doszło w 2009 r. Według oficjalnego przekazu w wyniku włamania pochodzącego z terytorium Chin pozyskano dane na temat amerykańskiego programu zbrojeniowego Joint Strike Fighter (zakładającego modernizację lotnictwa oraz systemów obrony przeciwlotniczej). Podczas neutralizacji skutków tego cyberataku odkryto, że program zbrojeniowy był inwigilowany od 2007 r., przy czym metody szyfrowania plików wykorzystane przez hakerów uniemożliwiły określenie, jakie informacje zostały utracone. Chińska Republika Ludowa za pośrednictwem swojej ambasady w USA zaprzeczyła, jakoby władze w Pekinie prowadziły działania cyberprzestępcze, a oskarżenia uznano za fałszywe i mające na celu szerzenie poczucia zagrożenia rzekomo wynikającego z chińskiej działalności w cyberprzestrzeni[77].

Największa wykryta chińska kampania przeciwko amerykańskiej przestrzeni teleinformatycznej także rozpoczęła się w 2009 r. Operacja „Aurora" miała na celu przeprowadzenie ataków na serwery ponad 30 korporacji Stanów Zjednoczonych. Do stycznia 2010 r. stwierdzono naruszenie integralności sieci takich firm, jak: Google, Adobe Systems, Yahoo!, Morgan Stanley (zajmującej się obsługą finansową) oraz Dow Chemical Company (działającej w przemyśle chemicznym). Atak

[73] R. Wydra, *Relacje Chin i Stanów Zjednoczonych w cyberprzestrzeni*, „Security, Economy & Law" 2017, nr 3, s. 103. https://doi.org/10.24356/SEL/16/6.

[74] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 312–313.

[75] J.C. Mulvenon, *Chinese Cyber Espionage. Hearing on Chinese Hacking: Impact on Human Rights and Commercial Rule of Law*, Washington 2013, s. 29.

[76] L. Glendinning, *Obama, McCain computer 'hacked' during election campaign*, The Guardian, 7 XI 2008 r., https://www.theguardian.com/global/2008/nov/07/obama-white-house-usa [dostęp: 10 V 2022].

[77] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 316–317.

zagroził również systemom informatycznym instytucji innych państw świata, w tym Niemiec, Wielkiej Brytanii i Tajwanu[78].

Jednym ze złośliwych programów użytych podczas operacji „Aurora" był trojan Hydraq. Jego instalacja na komputerze następowała w momencie wejścia na zainfekowaną stronę internetową. Następnie program przeszukiwał zawartość dysków twardych, po czym kopiował zamieszczone na nich dane. Po zaszyfrowaniu przechwyconej zawartości wysyłał ją do Chin[79]. Skala przeprowadzonych ataków spowodowała ostrą reakcję ze strony Stanów Zjednoczonych, wzywających ChRL do przeprowadzenia transparentnego śledztwa. Strona chińska zlekceważyła jednak żądania USA[80].

W lipcu 2011 r. doszło do kolejnego poważnego ataku na amerykańskie korporacje z sektora obronnego. W wyniku cyberwłamań wykradziono ok. 24 000 plików. Oficjalne stanowisko USA jednoznacznie nie wskazywało sprawcy, lecz sugerowało, że hakerzy przeprowadzili operacje z terytorium Chin[81].

Na początku 2013 r. ofiarami chińskich cyberataków padły największe amerykańskie media, takie jak „The New York Times", „The Wall Street Journal" i „The Washington Post". W przypadku pierwszego z nich włamania na komputery dziennikarzy tej gazety trwały przez cztery miesiące. Jedną z prawdopodobnych przyczyn przeprowadzenia tych działań była publikacja artykułu, w którym opisano majątek chińskiego premiera Wena Jiabao[82]. Hakerzy poszukiwali również materiałów, które miały posłużyć do opracowania kolejnych tekstów o członkach chińskiego rządu.

W lutym 2013 r. Departament Bezpieczeństwa Krajowego ujawnił, że w czasie sześciu miesięcy została przeprowadzona seria cyberataków na infrastrukturę krytyczną Stanów Zjednoczonych. Podczas włamań do sieci 23 przedsiębiorstw gazowych hakerzy uzyskali dane dostępu administracji sieci, ich specyfikację oraz informacje na temat dostępu do systemów kontroli gazociągów[83].

Raport opublikowany w 2013 r. przez korporację Mandiant potwierdził większość opinii ekspertów na temat źródeł cyberataków w przestrzeni teleinformatycznej Stanów Zjednoczonych. Ponadto wskazywał, że część grup hakerskich

---

78 Tamże.

79 Tamże, s. 317.

80 B. Johnson, *US asks China to explain Google hacking claims*, The Guardian, 13 I 2010 r., https://www.theguardian.com/technology/2010/jan/13/china-google-hacking-attack-us [dostęp: 10 V 2022].

81 C. Lefkow, *24,000 files stolen from defense contractor: Pentagon*, phys.org, 15 VII 2011 r., https://phys.org/news/2011-07-stolen-defense-contractor-pentagon.html [dostęp: 10 V 2022].

82 *New York Times 'hit by hackers from China'*, BBC News, 31 I 2013 r., https://www.bbc.com/news/world-asia-china-21271849 [dostęp: 10 V 2022].

83 M. Clayton, *Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage*, The Christian Science Monitor, 27 II 2013 r., https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage [dostęp: 10 V 2022].

rzeczywiście jest komponentem Biura II w Departamencie III Sztabu Generalnego Chińskiej Armii Ludowo-Wyzwoleńczej, która to jednostka zajmuje się prowadzeniem działań w cyberprzestrzeni[84].

Stany Zjednoczone nie tylko są ofiarą chińskich ataków. Według danych ujawnionych przez amerykańską Agencję Bezpieczeństwa Narodowego (National Security Agency) w 2011 r. USA przeprowadziły w odwecie 231 cyberataków na systemy Chin, Rosji, Iranu i Korei Północnej[85].

Podsumowanie

Wzrost popularności technologii teleinformatycznych, wynikający z kilku czynników (głównie z dostępności, niskich kosztów pozyskania, utrzymania oraz naprawy narzędzi teleinformatycznych w przypadku awarii lub ataku oraz ich stosunkowo prostej obsługi), sprawił, że cyberprzestrzeń stała się również elementem życia codziennego. Dzięki niej można komunikować się w czasie rzeczywistym z odbiorcą, który znajduje się w odległym miejscu, przy niewielkim nakładzie finansowym. Internet (jeden z głównych elementów, na które składa się cyberprzestrzeń) jest również ogromną bazą danych.

Zwiększający się wpływ cyberprzestrzeni na życie jednostek i państw był widoczny także w czasie pandemii COVID-19. Przestrzeń teleinformatyczna umożliwiła podtrzymanie ciągłości pracy niektórych elementów państwa, takich jak oświata czy służba zdrowia. Wraz ze wzrostem powszechności dostępu do tej przestrzeni powstają także różnego typu zagrożenia. Największe z nich to działalność cyberprzestępców. Dysponując wieloma narzędziami, najczęściej dążą oni do kradzieży środków finansowych z kont bankowych oraz tożsamości. Z tego rodzaju zagrożeniami muszą się mierzyć również instytucje państwowe. Źródłem niebezpieczeństwa jest także aktywność w cyberprzestrzeni grup i organizacji terrorystycznych. Świat rzeczywistości wirtualnej stał się wręcz idealnym miejscem do szerzenia ekstremizmu religijnego i islamistycznej propagandy.

Przedstawione w artykule przypadki stanowią dowód na to, że cyberprzestrzeń może się stać niebezpiecznym teatrem działań. Jeśli podmiot podejmujący wrogą aktywność dysponuje umiejętnościami oraz odpowiednimi narzędziami, jest w stanie sparaliżować państwo bez użycia siły militarnej. Działania w sieci nie przypominają konwencjonalnych operacji wojennych. Szkody wywołane udanym,

[84] *APT1: Exposing One of China's Cyber Espionage Units*, https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf [dostęp: 10 V 2022].

[85] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar*…, s. 325.

zwłaszcza masowym atakiem mogą być jednak większe niż te będące skutkiem walki zbrojnej pomiędzy dwoma lub więcej podmiotami stosunków międzynarodowych. Zakłada się, że ataki hakerskie nie przyniosą raczej bezpośrednich ofiar w ludziach. Nie można jednak wykluczyć celowego uderzenia w większe skupiska ludzkie, np. w przypadku ataku na elektrownię jądrową, zakłady chemiczne czy sieci transportowe.

Ataki na infrastrukturę krytyczną polegające na włamaniu się do jej systemów zazwyczaj wiążą się z zakłóceniem jej pracy, a w niektórych przypadkach również z jej zniszczeniem. Tak się stało w wyniku zainfekowania przez izraelskich hakerów irańskich ośrodków wzbogacających uran. Ponadto na skutek tej operacji Stuxnet uderzył w systemy informatyczne wielu innych państw, co wskazuje na to, że tego rodzaju oprogramowanie może się stać bronią obosieczną.

Cyberataki mogą służyć również jako wsparcie podczas konwencjonalnych działań militarnych. Przykładem takiego wykorzystania przestrzeni teleinformatycznej jest operacja „Orchard". W pierwszej fazie polegała ona na wprowadzeniu w błąd systemów informatycznych sterujących siecią radarową sił zbrojnych Syrii. W kolejnej fazie izraelskie lotnictwo wykonało skuteczne uderzenie na ośrodek prowadzący badania nad bronią jądrową. Cyberprzestrzeń jest wykorzystywana także przez podmioty stosunków międzynarodowych do pozyskiwania nowoczesnych technologii oraz systemów uzbrojenia. Szczególnie aktywne działania tego typu prowadzi ChRL. Dokonując włamań do systemów teleinformatycznych innych państw, pozyskuje dane, które służą jej do rozwijania swojej gospodarki, sił zbrojnych czy też do prowadzenia polityki.

Przestrzeń wirtualna jest też obszarem oddziaływania na opinię społeczną w szerszym, globalnym ujęciu. Dzięki swobodnej wymianie informacji zarówno pojedynczy hakerzy, jak i instytucje państwowe mogą w dowolny sposób kreować zachowania jednostek i zbiorowości ludzkich, skłaniając je do określonych działań lub zaniechania aktywności. Ten stan rzeczy budzi uzasadnione zaniepokojenie, zwłaszcza w instytucjach odpowiedzialnych za bezpieczeństwo państwa. Aby skutecznie przeciwdziałać zagrożeniom występującym w przestrzeni wirtualnej i reagować na nie, należy budować i rozwijać własne systemy obronne i ofensywne.

Wzrost zainteresowania przeniesieniem działalności do przestrzeni wirtualnej ze strony różnych graczy, a przede wszystkim aktorów państwowych, spowodował powstanie zjawiska cyberwojny, której pierwszą ofiarą była Estonia w 2007 r. W przyszłości cyberwojownicy, zorganizowani w ramach określonych grup czy jednostek wojskowych danego kraju, będą prawdopodobnie prowadzić cyberoperacje przeciwko zasobom strategicznym oraz infrastrukturze krytycznej kraju obranego za cel. Działania te mają lub będą miały na celu sparaliżowanie funkcjonowania państwa, a więc nie tylko infrastruktury rządowej, lecz także całego systemu

infrastruktury krytycznej, od której działania w szerokim zakresie jest uzależnione bezpieczeństwo społeczne.

Rozwój przestrzeni wirtualnej sprawia, że zjawisko cyberwojny może odgrywać coraz większą rolę. Przykład operacji „Orchard" pokazuje, jak istotnymi narzędziami prowadzenia działań wojennych są technologie teleinformatyczne. Izraelskie służby włamały się na syryjskie systemy komputerowe i „oślepiły" radary. Tym samym nadały operacjom w rzeczywistości wirtualnej nowy wymiar. Najprawdopodobniej kolejny konflikt na poziomie globalnym rozpocznie się w cyberprzestrzeni i tam też może się zakończyć.

Bibliografia

Ajili H., Rezaee N., *Iranian Military Capabilities and Possibility of Blocking Hormuz Strait by Iran*, „Cywilizacja i Polityka" 2020, nr 18, s. 59–80. https://doi.org/10.15804/cip202005.

Andress J., Winterfeld S., *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Waltham 2011.

Bencsáth B. i in., *The Cousins of Stuxnet: Duqu, Flame and Gauss,* „Future Internet" 2012, nr 4, s. 971–1003. https://doi.org/10.3390/fi4040971.

Bieniek O., *Cyberprzestrzeń w rosyjskiej przestrzeni informacyjnej*, „Wiedza Obronna" 2017, nr 3–4, s. 35–48.

Bryczek-Wróbel P., *Sytuacja geopolityczna Estonii w polityce zagranicznej Federacji Rosyjskiej*, „Polityka i Społeczeństwo" 2021, t. 19, nr 3, s. 23–35. https://doi.org/10.15584/polispol.2021.3.2.

Bryjka F., *Wykrywanie i zwalczanie dezinformacji – zarys skryptu. Materiał pomocniczy do sylabusa zajęć akademickich*, w: R. Kupiecki i in., *Platforma przeciwdziałania dezinformacji: budowanie odporności społecznej. Badania i edukacja*, Warszawa 2021, s. 113–136.

Carr J., *Inside Cyber Warfare: Mapping the Cyber Underworld*, Beijing-Cambridge-Farnham-Köln-Sewastopol-Taipei-Tokyo 2010.

Chłoń T., Kozłowski K., *Wybrane studia przypadku systemowych działań dezinformacyjnych: Rosja i Chiny*, w: R. Kupiecki i in., *Platforma przeciwdziałania dezinformacji: budowanie odporności społecznej. Badania i edukacja*, Warszawa 2021, s. 33–60.

Dobbins J. i in., *Coping with a Nuclearizing Iran*, Santa Monica 2011.

Dygnatowski S., Dygnatowski P., Domżał-Drzewicki Ł., *Analiza wykorzystania rozwiązań strukturalnych w obszarze cyberbezpieczeństwa na przykładzie operacji Orchard*, „Journal of KONBiN" 2019, t. 49, nr 1, s. 290–298. http://dx.doi.org/10.2478/jok-2019-0014.

Farwell J.P., Rohozinski R., *Stuxnet and the Future of Cyber War*, „Survival. Global Politics and Strategy" 2011, t. 53, nr 1, s. 23–40. https://doi.org/10.1080/00396338.2011.555586.

Farwell J.P., Rohozinski R., *The New Reality of Cyber War*, „Survival. Global Politics and Strategy" 2012, t. 54, nr 4, s. 107–120. https://doi.org/10.1080/00396338.2012.709391.

Gerlach J., *Wpływ prasy, radia, telewizji i Internetu na współczesne zachowania nabywcze*, „Współczesne Problemy Ekonomiczne" 2018, nr 2, s. 5–12. https://doi.org/10.18276/wpe.2018.18-01.

Grycuk A., *Fake news, trolle, boty i cyborgi w mediach społecznościowych,* „Analizy BAS", 2021, nr 1, s. 1–12.

Herzog S., *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses,* „Journal of Strategic Security" 2011, t. 4, nr 2, s. 49–60. http://dx.doi.org/10.5038/1944-0472.4.2.3.

Jachyra D., *Trollowanie – antyspołeczne zachowania w Internecie, sposoby wykrywania i obrony*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Informatica" 2011, nr 28, s. 253–261.

Kacała T., *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa*, „Przegląd Prawa Konstytucyjnego" 2015, nr 2, s. 49–65. https://doi.org/10.15804/ppk.2015.02.03.

Kaniewska M., *Między kijem a marchewką – Organizacja Narodów Zjednoczonych wobec programu nuklearnego Iranu*, w: *Stabilizacja czy destabilizacja? Społeczność międzynarodowa wobec programu nuklearnego Iranu*, A. Malantowicz, Ł. Smalec (red.), Warszawa 2014, s. 55–66.

Kowalczewska K., *Wpływ nowoczesnych technologii na współczesne konflikty zbrojne*, Warszawa 2022.

Kukułka J., *Historia współczesna stosunków międzynarodowych 1945–2000*, Warszawa 2007.

Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015.

Liedel K., Piasecka P., *Wojna cybernetyczna – wyzwanie XXI wieku,* „Bezpieczeństwo Narodowe" 2011, nr 17, s. 15–28.

Małecka A., *Nation-State Cyber Operations Legal Considerations: An Estonian Case Study*, „Safety & Defense" 2021, t. 7, s. 99–108. https://doi.org/10.37105/sd.139.

Marszałek-Kawa J., *Polityka zagraniczna ChRL: aspiracje, możliwości, paradoksy*, w: *Polityka zagraniczna. Aktorzy – potencjały – strategie*, T. Łoś-Nowak (red.), Warszawa 2011, s. 104–127.

Mazurek S., *Rewolucja islamska w Iranie – przyczyny, przebieg, konsekwencje*, „Nurt SVD" 2017, nr 1, s. 38–55.

Mulvenon C.J., *Chinese Cyber Espionage. Hearing on Chinese Hacking: Impact on Human Rights and Commercial Rule of Law*, Washington 2013.

Schmidt A., *The Estonian Cyberattacks*, w: *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, J. Healey (red.), Vienna 2013.

Szymczyk K., *Irański program nuklearny jako czynnik warunkujący stosunki międzynarodowe w obszarze i poza obszarem MENA*, w: *Bezpieczeństwo narodowe i międzynarodowe w rejonie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*, R. Bania, K. Zdulski (red. nauk.), Łódź 2012, s. 145–155.

Vademecum bezpieczeństwa informacyjnego, t. 2, O. Wasiuta, R. Klepka (red.), Kraków 2019.

Volkoff V., *Dezinformacja – oręż wojny*, Warszawa 1991.

Wierzbicki S., *Wojny cybernetyczne jako element niekonwencjonalnej konfrontacji międzypaństwowej. Pragmatyczna rzeczywistość, nieunikniona przyszłość*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2015, t. 2, nr 1, s. 134–148.

Worona J., *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Białystok 2017.

Wydra R., *Relacje Chin i Stanów Zjednoczonych w cyberprzestrzeni*, „Security, Economy & Law" 2017, nr 3, s. 100–108. https://doi.org/10.24356/SEL/16/6.

Zając J., *Polityka zagraniczna USA*, w: *Polityka zagraniczna. Aktorzy – potencjały – strategie*, T. Łoś-Nowak (red.), Warszawa 2011, s. 61–80.

Zakrzewski A., *Jak to jest z tym Stuxnetem, Flamem, Duqu?*, „DLP Expert" 2013, nr 1.

Zetter K., *Odliczając do dnia zero. Stuxnet czyli prawdziwa historia cyfrowej broni*, Gliwice 2014.

Źródła internetowe

1949–2023 U.S.-China Relations, Council on Foreign Relations, https://www.cfr.org/timeline/us-relations-china [dostęp: 10 V 2022].

About Company, http://anti-virus.by/en/index.shtml.

APT1: Exposing One of China's Cyber Espionage Units, https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf [dostęp: 8 IV 2024].

Bencsáth B. i in., *Duqu: A Stuxnet-like malware found in the wild. Technical Report by Laboratory of Cryptography and System Security (CrySys)*, 14 X 2011 r., https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf [dostęp: 8 IV 2024].

Bochyńska N., *Art. 5 Traktatu NATO a działania w cyberprzestrzeni. Czy istnieją „granice" dla cyberwojny?*, CyberDefence24, 17 III 2022 r., https://cyberdefence24.pl/cyberbezpieczenstwo/art-5-traktatu-o-nato-a-dzialania-w-cyberprzestrzeni-czy-istnieja-granice-dla-cyberwojny [dostęp: 7 V 2022].

Chein E., OMurchu L., Falliere N., *W32.Duqu. The precursor to the next Stuxnet*, https://www. usenix.org/system/files/conference/leet12/leet12-final11.pdf [dostęp: 7 V 2022].

Clayton M., *Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage*, The Christian Science Monitor, 27 II 2013 r., https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage [dostęp: 10 V 2022].

First Stuxnet – Now the Flame Virus, The Availability Digest, czerwiec 2012 r., www.availabilitydigest.com/public_articles/0706/flame_virus.pdf [dostęp: 10 V 2022].

Glendinning L., *Obama, McCain computer 'hacked' during election campaign*, The Guardian, 7 XI 2008 r., https://www.theguardian.com/global/2008/nov/07/obama-white-house-usa [dostęp: 10 V 2022].

Johnson B., *US asks China to explain Google hacking claims*, The Guardian, 13 I 2010 r., https://www.theguardian.com/technology/2010/jan/13/china-google-hacking-attack-us [dostęp: 10 V 2022].

Jones S., *The Islamic Republic of Iran: An introduction*, House of Commons Library, 11 XII 2009 r., https://researchbriefings.files.parliament.uk/documents/RP09-92/RP09-92.pdf [dostęp: 8 IV 2024].

Juurvee I., Mattiisen M., *The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict*, International Centre for Defence and Security, sierpień 2020 r., https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf [dostęp: 8 IV 2024].

Kaska K., Osula A.M., Stinissen J., *The Cyber Defence Unit of the Estonian Defence League. Legal, Policy and Organisational Analysis*, Tallinn 2013, https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf [dostęp: 8 IV 2024].

Krekel B., *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* The US-China Economic and Security Review Commission, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf [dostęp: 8 IV 2024].

Kumar S., *Asymmetric Capabilities of China's Military*, Institute of Peace and Conflict Studies, 19 XI 2008 r., https://www.ipcs.org/comm_select.php?articleNo=2735 [dostęp: 10 V 2022].

Lefkow C., *24,000 files stolen from defense contractor: Pentagon*, phys.org, 15 VII 2011 r., https://phys.org/news/2011-07-stolen-defense-contractor-pentagon.html [dostęp: 10 V 2022].

Majdan K., *Wykryto nowe „cyberzagrożenie". „Z czymś takim jeszcze się nie spotkaliśmy"*, na Temat, 29 V 2012 r., https://natemat.pl/16397,wykryto-nowe-cyberzagrozenie-z-czym-s-takim-jeszcze-sie-nie-spotkalismy [dostęp: 7 V 2022].

New York Times 'hit by hackers from China', BBC News, 31 I 2013 r., https://www.bbc.com/news/world-asia-china-21271849 [dostęp: 10 V 2022].

Park J.K., *A Report of the CSIS Korea Chair. China – U.S. Relations in East Asia. Strategic Rivalry and Korea's Choice*, Center for Strategic and International Studies, kwiecień 2013 r., https://ciaotest.cc.columbia.edu/wps/csis/0028481/f_0028481_23160.pdf [dostęp: 8 IV 2024].

Reeder F.S. i in., *Updating U.S. Federal Cybersecurity Policy and Guidance. Spending scarce taxpayer dollars on security programs that work*, Center for Strategic and International Studies, październik 2012 r., https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/121019_Reeder_A130_Web.pdf [dostęp: 8 IV 2024].

Sahimi M., *Iran's Nuclear Program. Part I: Its History*, 10 II 2003 r., https://www.iranwatch.org/library/sahimi-irans-nuclear-program-part-i-its-history-10-2-03 [dostęp: 8 IV 2024].

Zanotti J. i in., *Israel: Possible Military Strike Against Iran's Nuclear Facilities*, Congressional Research Service, 28 IX 2012 r., https://sgp.fas.org/crs/mideast/R42443.pdf [dostęp: 7 V 2022].

Maciej Heromiński

Absolwent Wydziału Nauk Społecznych Uniwersytetu Jana Długosza w Częstochowie na kierunku bezpieczeństwo narodowe, ze specjalizacją bezpieczeństwo państwa. Interesuje się zagadnieniami związanymi z cyberprzestrzenią oraz polemologią.

Kontakt: m.herominski21@gmail.com

Biały wywiad w zarządzaniu bezpieczeństwem informacji[1]

Open-source intelligence in information security management

MACIEJ WITCZAK

Autor niezależny

https://orcid.org/0009-0002-8199-5865

Przegląd Bezpieczeństwa Wewnętrznego, 2024, nr 30: 213–240

https://doi.org/10.4467/20801335PBW.24.009.19611

ARTYKUŁ

Abstrakt

Wywiad oparty na źródłach otwartych stanowi zagrożenie systemu bezpieczeństwa informacji w organizacji (biznesie, siłach zbrojnych), a nawet w całym państwie. Celem artykułu jest przybliżenie tego zagadnienia, przedstawienie zagrożeń ze strony białego wywiadu oraz wskazanie sposobów przeciwdziałania im. Część teoretyczna jest uzupełniona praktyczną analizą przypadku i potwierdza postawioną hipotezę: pozyskanie informacji ze źródeł jawnych jest możliwe, jednak nie zawsze pozwala na uzyskanie kompleksowego produktu wywiadowczego. Ponadto zarządzanie bezpieczeństwem informacji pozwala na minimalizowanie ryzyka pozyskania danych ze źródeł otwartych. W drugiej części zawarto rekomendacje i zaproponowano uniwersalny model zarządzania bezpieczeństwem informacji w organizacji.

Słowa kluczowe

biały wywiad, OSINT, zarządzanie bezpieczeństwem informacji, ISM

[1] Artykuł powstał na podstawie pracy magisterskiej pt. *Biały wywiad w zarządzaniu bezpieczeństwem informacji* obronionej na Wydziale Zarządzania Akademii Wojsk Lądowych im. gen. Tadeusza Kościuszki we Wrocławiu. Praca została nagrodzona w XII edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

Abstract

Open-source intelligence (OSINT) poses a threat to the information security system in an organisation (business, armed forces) and even in a whole state. The aim of the article is to provide an overview of this issue, to present the threats posed by open source intelligence and to identify ways of countering them. The theoretical part is complemented by a practical case study and confirms the hypotheses: gathering information from the open sources is possible, but it does not always allow for a comprehensive intelligence product. Moreover, the information security management minimises the risk of collecting data from the open sources. The second part provides recommendations and proposes a universal model of information security management in an organisation.

Keywords

open source intelligence, OSINT, information security management, ISM

Ikona myśli strategicznej Sun Tzu już w starożytności zauważył, że (…) *mądrzy władcy i przebiegli dowódcy pokonują przeciwników i dokonują wybitnych czynów, ponieważ z wyprzedzeniem zdobywają wiedzę o wrogu*[2]. Dlatego informacje od zarania dziejów były podstawą zwycięstw w sferze militarnej i cywilnej. Współcześnie można je uzyskać na wiele sposobów, a ich źródła mogą być mniej lub bardziej jawne. W artykule podjęto temat pozyskiwania informacji ze źródeł jawnych, czyli dostępnych i łatwych do zdobycia dla każdego, przedstawiono możliwości i zagrożenia ze strony rozpoznania otwartoźródłowego (ang. *open-source intelligence*, OSINT) oraz nakreślono właściwy kierunek zarządzania bezpieczeństwem informacji (ang. *information security management*, ISM) w kontekście zagrożenia białym wywiadem. Podjęty problem badawczy jest próbą odpowiedzi na pytanie: jak zarządzać bezpieczeństwem informacji w organizacji, aby zminimalizować ryzyko pozyskania ich przez biały wywiad? W tym celu postawiono trzy hipotezy badawcze. Po pierwsze, przypuszcza się, że wywiad otwartoźródłowy pozwala na wejście w posiadanie informacji niejawnej. Po drugie, w niektórych przypadkach kompleksowe rozpoznanie obiektu wyłącznie tą metodą jest niemożliwe. Po trzecie, ryzyko pozyskania informacji przez biały wywiad można redukować odpowiednim ISM. Badania przeprowadzono przy użyciu metody studiów literaturowych oraz studium przypadku.

[2] S. Tzu, *Sztuka wojny. Traktat*, Gliwice 2012, s. 80.

Tematyka wykorzystywania źródeł jawnych oraz używania danych z nich zebranych nieustannie zyskuje na popularności. Terminy „prywatność" i „cyberbezpieczeństwo" pojawiają się coraz częściej w debacie publicznej[3]. W odpowiedzi na to zainteresowanie rynek wydawniczy przedstawia bogatą ofertę pozycji na temat OSINT oraz bezpieczeństwa informacji. Te źródła koncentrowały się jednak na ukazaniu możliwości OSINT, brakowało natomiast rzetelnych i wyczerpujących opracowań na temat zarządzania bezpieczeństwem informacji w kontekście pozyskania ich przez biały wywiad. Niniejszy artykuł powstał w celu wypełnienia choć w pewnym stopniu zaistniałej luki.

Informacja oraz zarządzanie informacją i jej bezpieczeństwem

Pochodzenia terminu „informacja" należy szukać w łacińskim słowie *informatio* – 'wyobrażenie', 'zawiadomienie', 'wyjaśnienie', potocznie 'jakakolwiek wiadomość'[4]. Jej elementami są dane, które rozpatrywane osobno nie mają wartości informacyjnej. Dopiero ich połączenie umożliwia nadanie im miana informacji[5]. Powstało wiele definicji tego pojęcia, niezależnie jednak od ich liczby informację można rozpatrywać w czterech głównych znaczeniach:

1) rzecz – produkt określonego procesu, ma źródło i odbiorcę i można mu przypisać właściwości, takie jak treść, forma, wartość, użyteczność,
2) mierzalna wielkość – wynika z konieczności ilościowej charakterystyki potrzebnej do oceny skuteczności komunikacji,
3) potencjał – zdolność do zmiany na skutek zmniejszenia niepewności wobec rozważanych rzeczy,
4) zmiana – odnosi się do jej roli w procesie kształtowania postaw i zachowań, może dokonywać się bezpośrednio przez odniesienie do zmiany zamierzonej, w postaci zalecenia, instrukcji lub ostrzeżenia albo pośrednio[6].

Informacjom przypisuje się określone cechy. Przede wszystkim istnieją obiektywnie, niezależnie od świadomości ludzi, a ich zbiór jest niewyczerpalny (nie zużywają się w procesie wykorzystania). Muszą być wyrażone wiadomością za pośrednictwem nośników materialnych oraz wymagają ciągłej aktualizacji. Mogą

[3] Na przykład od 2016 r. odbywa się w październiku kampania Europejskiego Miesiąca Cyberbezpieczeństwa. Zob. www.bezpiecznymiesiac.pl [dostęp: 29 XII 2023].

[4] K. Liedel, *Zarządzanie informacją w walce z terroryzmem*, Warszawa 2010, s. 42.

[5] W. Krztoń, *Zarządzanie informacją w procesach decyzyjnych organizacji*, „Modern Management Review" 2017, nr 3, s. 84.

[6] Za: K. Liedel, *Zarządzanie informacją*…, s. 43–44.

występować w systemie jako czynnik sprawczy, przez odwołanie się do zjawisk niewystępujących w przeszłości i obecnie, ale mogących pojawić się w przyszłości (oraz tych, które nigdy nie istniały i nie zaistnieją). Mogą być przetwarzane, powielane i transportowane w czasie i w przestrzeni, mogą podlegać też celowym lub przypadkowym deformacjom albo fałszowaniu[7].

Informacja może mieć określoną wartość, która opisuje stopień spełnienia potrzeb użytkowników. Składają się na nią dwa czynniki: jakość i użyteczność[8]. Jakość to stopień spełnienia wymagań stawianych przez system decyzyjny w zakresie aktualności (otrzymania informacji w wymaganym czasie), pełności (zawarcia rzeczywistych informacji o stanie rzeczy) i niezawodności (określenia wpływu zakłóceń i zniekształceń na informacje)[9]. Użyteczność to cecha, która określa wpływ informacji na prawidłowość i trafność (zmniejszenie niewiedzy) w podejmowaniu decyzji[10].

Aby zapanować nad coraz większą ilością informacji, jest konieczne odpowiednie zarządzanie nimi. „Zarządzanie informacją" to termin, który pojawił się na początku lat 70. XX w. w czasie rewolucji technologicznej w masowym, komputerowym przetwarzaniu danych, będącym dziś podstawową funkcją zarządzania organizacją[11].

Gromadzenie, przetwarzanie i dystrybucja informacji to typy działalności informacyjnej. Gromadzenie jest elementem procesu decyzyjnego i znajduje zastosowanie w jednej z funkcji zarządzania, czyli planowaniu (w klasyfikacji funkcji zarządzania rozumianego jako planowanie, organizowanie, motywowanie i kontrola). Samo gromadzenie informacji nie wymaga szczegółowego opisywania, należy jednak pamiętać o ryzyku przesytu danych, co może powodować wprowadzenie chaosu informacyjnego i rozproszenie uwagi odbiorcy (ang. *attention crash*). Przetwarzanie to funkcja dostępna dla posiadacza urządzenia mobilnego. W podstawowym pakiecie niemal każdego z nich jest dostępne oprogramowanie do obróbki obrazu, dźwięku i tekstu, zatem modyfikacja informacji nie stanowi problemu. Dystrybucja informacji polega na przekazywaniu ich bez względu na bariery czasu i przestrzeni oraz ponoszenie opłat, przy wykorzystaniu dostępnej technologii[12].

---

[7] K. Liedel, *Zarządzanie informacją*…, s. 45; K. Liedel, P. Piasecka, T. Aleksandrowicz, *Analiza informacji. Teoria i praktyka*, Warszawa 2012, s. 34–35.

[8] K. Liedel, *Zarządzanie informacją*…, s. 51.

[9] Tamże, s. 49.

[10] Tamże, s. 50.

[11] W. Krztoń, *Zarządzanie informacją w procesach decyzyjnych*…, s. 91.

[12] M. Nowina-Konopka, *Infomorfoza. Zarządzanie informacją w nowych mediach*, Kraków 2017, s. 81.

Informacja w kontekście bezpieczeństwa osób fizycznych i organizacji (w tym przedsiębiorstw i całych państw) odgrywa obecnie olbrzymią rolę. Rozpatrując zagadnienie bezpieczeństwa informacyjnego państwa, należy uwzględnić:

- informacje jako zasób strategiczny oraz podstawowy czynnik wytwórczy, generujący część dochodu narodowego[13],
- uzależnienie procesów decyzyjnych w sektorach gospodarki od systemów przesyłania i przetwarzania informacji,
- fakt, że współczesna rywalizacja między adwersarzami przenosi się na poziom walki informacyjnej, a mass media mogą być wykorzystywane do zakłócania informacyjnego[14].

Dlatego stwierdzenie, że (…) *bez racjonalnie ukształtowanej sfery informacyjnej nie może efektywnie funkcjonować współczesne społeczeństwo, państwo – jego administracja, nauka i szkolnictwo, kultura, gospodarka narodowa, siły zbrojne*[15], jest zgodne z prawdą. Informacja to kluczowy element współczesnych konfliktów, wykorzystuje się ją zarówno jako broń, jak i cel, a sfera informacyjna jest traktowana jako odrębne środowisko walki[16]. W 2014 r. podczas szczytu NATO w Newport w Walii przyjęto przełomową wówczas deklarację o możliwości przywołania art. 5 traktatu północnoatlantyckiego w razie najpoważniejszych cyberataków. Podczas kolejnego szczytu w Warszawie w 2016 r. cyberprzestrzeń uznano za współczesne pole walki, obok ziemi, powietrza, morza i przestrzeni kosmicznej. Ponadto, według Bolesława Balcerowicza walka informacyjna może być (…) *zjawiskiem autonomicznym, komponentem wspierającym działania militarne bądź głównym, wpieranym działaniami militarnymi*[17]. Koncepcja walki informacyjnej, mimo militarnego rodowodu, znajduje zastosowanie także w sferze politycznej, gospodarczej, kulturalnej, naukowej, sektorze publicznym i prywatnym[18].

Polityka bezpieczeństwa informacji wymusza zatem korzystanie z mechanizmów, które będą zabezpieczać prawidłowe przetwarzanie informacji (zapewnią bezpieczeństwo informacyjne). W celu stosowania właściwych zabezpieczeń opracowano System Zarządzania Bezpieczeństwem Informacji (SZBI), którego wdrożenie i użytkowanie zgodnie z wymaganiami międzynarodowej normy *ISO/IEC 27001*

[13] K. Liedel, P. Piasecka, T. Aleksandrowicz, *Analiza informacji*…, s. 18.

[14] Zob. tamże; K. Liedel, *Zarządzanie informacją*…, s. 55.

[15] Za: K. Liedel, P. Piasecka, T. Aleksandrowicz, *Analiza informacji*…, s. 9.

[16] Tamże, s. 16–17.

[17] Tamże, s. 21.

[18] Tamże.

stanowi podstawę certyfikacji systemu bezpieczeństwa[19]. W rozumieniu wskazanej normy bezpieczeństwo informacyjne obejmuje:

1) poufność – dostęp wyłącznie dla uprawnionych osób,
2) spójność – monitorowanie procesu przetwarzania informacji w celu uniemożliwienia nieautoryzowanej modyfikacji,
3) dostępność – zawsze, gdy osoba uprawniona tego potrzebuje[20],
4) niezaprzeczalność – możliwość udowodnienia, że zdarzenia lub działania miały miejsce i wywołał je określony podmiot,
5) niezawodność – zamierzone, spójne i zachowane skutki[21].

Głównym celem SZBI jest takie zarządzanie ryzykiem, aby zminimalizować możliwość wystąpienia incydentów i zagrożeń. Poza wskazaną normą w polskim systemie prawnym istnieje jeszcze kilka pozycji, które poruszają tematykę bezpieczeństwa informacji (nie ma bowiem jednego aktu prawnego obejmującego to zagadnienie). Najistotniejsze z nich to:

- *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*,
- *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*,
- *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych*.

Ważne są również m.in.: *Ustawa z dnia 29 września 1994 r. o rachunkowości*, *Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne*. Bezpieczeństwo informacyjne na szczeblu państwowym reguluje także *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* oraz *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*[22]. W dalszej części artykułu omówiono najważniejsze pozycje.

Konstytucja jako ustawa zasadnicza kodyfikuje powszechne prawodawstwo kraju. W jej zapisach można znaleźć fragmenty związane z bezpieczeństwem informacji oraz z prawem do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o życiu osobistym (art. 47). W art. 51 jest wskazane, że:

[19] J. Krawiec, *System Zarządzania Bezpieczeństwem Informacji – zabezpieczenia*, „Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie" 2017, nr 1 (38), s. 46.

[20] J. Łuczak, M. Tyburski, *Systemowe Zarządzanie Bezpieczeństwem Informacji ISO/IEC 27001*, Poznań 2009, s. 12–17.

[21] Dodatkowe dwa atrybuty wyróżniono w normie *PN-ISO/IEC 27000:2014*. Za: S. Stanek, *Podejmowanie decyzji w warunkach zagrożenia bezpieczeństwa informacyjnego organizacji*, Wrocław 2016, s. 30.

[22] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [dostęp: 19 XII 2023].

1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.
2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Szczególnej ochronie podlegają informacje niejawne. Zgodnie z ustawą o ochronie informacji niejawnych (OIN) informacje niejawne to takie, (…) *których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania* (art. 1). Inne, pozanormatywne definicje wskazują, że ujawnienie informacji niejawnej osobie nieuprawnionej może mieć negatywny wpływ na organizację, jej członków albo na osoby z nią współpracujące (akcjonariuszy, partnerów, pracowników, klientów) oraz może obejmować informacje handlowe, marketingowe, finansowe, specyfikacje techniczne i inne o szczególnym znaczeniu dla funkcjonowania organizacji[23].

Obowiązująca ustawa określa zasady OIN rozumiane jako: klasyfikowanie i przetwarzanie informacji niejawnych, organizowanie ich ochrony, zasady organizacji kontroli stanu ich zabezpieczenia i stosowania środków bezpieczeństwa fizycznego. Ustawa definiuje kolejne klauzule niejawności: zastrzeżone, poufne, tajne, ściśle tajne (art. 5). W celu prawidłowego przetwarzania informacji niejawnych są organizowane szkolenia w zakresie OIN (art. 19–20) oraz jest przeprowadzana procedura sprawdzająca dotycząca rękojmi zachowania tajemnicy (art. 2 pkt 2). Zajmują się tym Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego. Służby te realizują zadania w zakresie OIN, w tym prowadzenie kontroli przestrzegania przepisów ustawy, postępowań sprawdzających, doradztw i szkoleń czy zapewnianie OIN wymienianych między Rzeczpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi (art. 10 ust. 1).

Kolejnym ważnym dokumentem jest *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2020*. Określono w nim cele strategiczne, takie jak cyberbezpieczeństwo i bezpieczeństwo przestrzeni informacyjnej, oraz sposoby ich realizacji. Cele te obejmują (…) *zwiększenie poziomu ochrony informacji w sektorze publicznym,*

[23] K. Mitnick, W. Simon, *Sztuka podstępu. Łamałem ludzi, nie hasła*, Gliwice 2016, s. 297.

militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji[24] przez m.in.:

- zbudowanie (…) *zdolności do ochrony przestrzeni informacyjnej*,
- stworzenie jednolitego systemu komunikacji strategicznej państwa, (…) *którego zadaniem powinno być prognozowanie, planowanie i realizowanie spójnych działań komunikacyjnych, przy wykorzystaniu szerokiej gamy kanałów komunikacji i mediów*,
- aktywne przeciwdziałanie dezinformacji przez (…) *stworzenie procedur współpracy z mediami informacyjnymi oraz społecznościowymi, przy zaangażowaniu obywateli i organizacji pozarządowych*,
- dążenie do (…) *zwiększenia świadomości społecznej o zagrożeniach związanych z manipulacją informacją poprzez edukację w zakresie bezpieczeństwa informacyjnego*[25].

Armie różnych państw świata także dostrzegają zarówno korzyści ze sprawnego zarządzania informacją w organizacji, jak i potrzebę bezpieczeństwa w tym zakresie. Wojsko Polskie dba o bezpieczeństwo informacji o żołnierzach i wykonywanych przez nich zadaniach. Kampania pod hasłem „#ŚwiadomiZagrożeń" zwraca uwagę na problem udostępniania w sieci danych personalnych, zdjęć infrastruktury krytycznej lub jednostek wojskowych, geolokalizacji czy terminów ćwiczeń wojskowych.

Obecnie nie tylko organizacje są zainteresowane tematyką bezpieczeństwa informacji. To zagadnienie nurtuje zwykłych ludzi, do czego przyczynił się efekt Snowdena[26]. Tajne dokumenty National Security Agency (NSA), które zostały upublicznione w 2013 r. przez Edwarda Snowdena, ujawniły, że służby specjalne przy wykorzystaniu technologii są w stanie prowadzić inwigilację obywateli, większą niż można było przypuszczać. Innymi słowy (…) *NSA była w stanie podsłuchiwać niemal wszystko i każdego, w kraju i za granicą, za zgodą sądu i bez niej*[27]. Te informacje spowodowały zmianę na niemal wszystkich poziomach społecznych – począwszy od stosunków dyplomatycznych, przez ustawodawstwo krajowe i międzynarodowe, aż do sposobu myślenia przeciętnych ludzi. Pytano, kto kontroluje kontrolujących. Efekt Snowdena wywołał dyskusję o publikowaniu własnych danych w sieci oraz zweryfikował mit anonimowości w internecie. Była to nauka także dla agencji wywiadowczych.

---

[24] *Strategia Bezpieczeństwa Narodowego*…, s. 20.

[25] Tamże, s. 21.

[26] Edward J. Snowden (ur. 1983) – amerykański sygnalista (ang. *whistleblower*), były pracownik CIA i zleceniobiorca NSA oraz informatyk samouk, który według szacunków upublicznił ok. 1,7 mln dokumentów poufnych, tajnych i ściśle tajnych, co uznano za największy wyciek informacji niejawnych w historii Stanów Zjednoczonych. Za: M. Nowina-Konopka, *Infomorfoza*…, s. 238–242.

[27] T. Aleksandrowicz, „*Efekt Snowdena*", Wszystko Co Najważniejsze, 7 VI 2014 r., https://wszystkoconajwazniejsze.pl/tomasz-aleksandrowicz-efekt-snowdena/ [dostęp: 11 IV 2022].

Przekonały się, że powszechna inwigilacja i gromadzenie niezliczonej ilości informacji nie mają sensu, gdyż (…) *trzeba wiedzieć, co się chce wiedzieć i co musimy wiedzieć. Inaczej będziemy wiedzieć wszystko – i nic*[28].

Biały wywiad – charakterystyka, potencjał i ograniczenia, źródła OSINT

Przypomniane na początku artykułu słowa Sun Tzu nie tracą na aktualności. Organy państwa od dawna poszukiwały informacji pomocnych w podejmowaniu decyzji, od których zależało bezpieczeństwo wewnętrzne i zewnętrzne. W tym celu wykorzystywano agentów i informatorów (źródła osobowe), przechwytywano dokumenty oraz stosowano metody przypisywane dziś białemu wywiadowi. Początkowo opierały się one na czytaniu materiałów pisanych, co znacznie ułatwił druk wynaleziony w połowie XV w. Kolejne źródła otwarte, pierwowzór dzisiejszych gazet, pojawiły się w XVII w. W późniejszych latach rosła liczba wynalazków, które wpłynęły na dostępność informacji. Dzięki telegrafowi, radiu, telefonowi, telewizji, a następnie komputerowi można dziś przesyłać szybko i na duże odległości niezliczone ilości informacji[29].

Zagraniczne instytucje wywiadowcze określały te działania początkowo jako wywiad jawny (ang. *overt intelligence*). Rodzime pojęcie białego wywiadu było używane znacznie wcześniej niż angielskojęzyczny akronim OSINT[30]. W polskiej literaturze biały wywiad jest przeciwieństwem czarnego – twardego i operacyjnego, który zdobywa informacje w sposób tajny, a czasem nawet nielegalny. Biały wywiad wyróżnia się brakiem konieczności naruszania prywatności lub łamania prawa. Przymiotnik „biały" sugeruje, że ta metoda jest na swój sposób niewinna[31]. Praktyka udowadnia jednak, że między tymi dwoma sposobami działania istnieje szerokie spektrum szarości[32].

Współczesny OSINT jest domeną przede wszystkim cywilną, a jego głównym beneficjentem pozostają wciąż służby specjalne. Jak podaje Andrzej Nowosad, według stanu wiedzy na 2005 r. wywiady obcych państw pozyskiwały 95% informacji

---

[28] Tamże.

[29] Za: A. Wojciulik, *Rola „białego wywiadu" w działalności służb specjalnych na przestrzeni wieków*, w: *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipkowski, W. Mądrzejowski (red.), Warszawa 2011, s. 46–47.

[30] B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015, s. 15.

[31] W. Filipkowski, W. Mądrzejowski, *Wstęp*, w: *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipkowski, W. Mądrzejowski (red.), Warszawa 2011, s. 14.

[32] B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 16–17.

ze źródeł jawnych, 4% z półjawnych i jedynie 1% ze źródeł tajnych[33]. Wydaje się, że wraz z postępem technologicznym stosunek udziału poszczególnych dziedzin wywiadowczych zmienił się na korzyść białego wywiadu. Informacje ze źródeł otwartych analizuje się dziś według czterech następujących po sobie etapów i są one klasyfikowane jako:

1) *Open Source Data* – surowe dane ze źródła nieobjętego klauzulą tajności,
2) *Open Source Information* – dane po wstępnej analizie, zgrupowane i przekazane osobom zarządzającym,
3) *Open Source Intelligence* – wybrane dane przekazane wyselekcjonowanej grupie odbiorców według założeń określonych przez składającego zapytanie (ang. *request for information*),
4) *Validated Open Source Intelligence* – dane zweryfikowane, z przypisanym wysokim poziomem pewności[34].

Informacje zebrane z wykorzystaniem OSINT przynoszą wiele korzyści związanych z rozpoznaniem celu. Wyróżnia się trzy najważniejsze funkcje OSINT: podstawową, naprowadzającą i komplementarną. Funkcja podstawowa oznacza użycie technik białego wywiadu w przypadku niedostępności źródeł operacyjnych albo braku konieczności ich wykorzystania. Funkcja naprowadzająca może sygnalizować zagrożenia i potrzebę objęcia danego podmiotu zainteresowaniem operacyjnym. Funkcja komplementarna wobec źródeł operacyjnych pozwala na uzupełnianie informacji zdobytych różnymi metodami, dzięki czemu można zbudować kompleksowy obraz analizowanego problemu[35]. Biały wywiad zapewnia ponadto takie korzyści, jak:

- łatwa dostępność informacji,
- szybkość pozyskiwania informacji,
- ilość, różnorodność, jakość i przejrzystość informacji,
- niskie koszty analizy uzyskanych informacji[36].

Biały wywiad pozwala na znacznie szybsze pozyskiwanie informacji w porównaniu z działaniami operacyjnymi. Nie wymaga odbywania spotkań czy dostarczania zdobytych informacji. Otwarte źródła zapewniają niemal nieograniczoną ilość

[33] A. Nowosad, *Metody i techniki pozyskiwania i przetwarzania informacji medialnej na potrzeby białego wywiadu*, „Państwo i Społeczeństwo" 2005, nr 2, s. 59.

[34] B. Stromczyński, P. Waszkiewicz, *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo" 2014, nr 5, s. 149.

[35] T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*, w: *Rola mediów w przeciwdziałaniu terroryzmowi*, K. Liedel, P. Piasecka (red.), Warszawa 2009, s. 85–86.

[36] Por. B. Saramak, *Wykorzystanie otwartych źródeł informacji…*, s. 31; *Rozpoznanie ze źródeł otwartych DD-2.9(A),* Ministerstwo Obrony Narodowej, Centrum Doktryn i Szkolenia Sił Zbrojnych, Bydgoszcz 2020, s. 2-2.

informacji, a w związku ze swoją specyfiką są dużo tańsze niż ich odpowiedniki, takie jak źródła osobowe czy systemy techniczne, np. satelitarne[37]. Zalety OSINT zostały dostrzeżone przez służby specjalne oraz policyjne. Masowe pozyskiwanie danych przy użyciu OSINT pozwala skuteczniej wypełniać zadania ustawowe tych służb. Podejmują one działania mające na celu zapewnienie bezpieczeństwa struktur państwa, porządku publicznego oraz obywateli. Jednymi z największych zagrożeń są współcześnie terroryzm i organizacje o charakterze przestępczym. Dzięki OSINT można realizować zadania przeciwdziałania organizacjom tego typu. W ocenie ekspertów korporacji RAND[38] 70–80% kluczowych dla antyterroryzmu informacji pochodzi ze źródeł otwartych, pozostałą część pozyskuje się przez wywiad operacyjny[39]. Tomasz Aleksandrowicz zauważył, że terroryści z powodzeniem wykorzystują internet „w walce o medialność", ponieważ jest on bardziej efektywnym narzędziem niż tradycyjne media[40]. Według stanu wiedzy na 2012 r. Al-Kaida publikowała swoje informacje na niemal 6000 stron internetowych[41]. Sieć zapewnia terrorystom nieskrępowany dostęp do odbiorców ze środowiska opiniotwórczego oraz daje możliwość publikowania treści pozbawionych kontroli, obróbki redakcyjnej czy cenzury[42]. Działania propagandowe terrorystów mogą koncentrować się na uzyskaniu rezultatów pozytywnych (pozyskanie sympatyków) lub negatywnych (skutki psychologiczne – wywołanie strachu i poczucia zagrożenia)[43]. Źródła otwarte można wykorzystać w walce z organizacjami terrorystycznymi w kilku obszarach. Po pierwsze, OSINT pozwala poznać historię, manifesty i oświadczenia organizacji, na ich podstawie określić jej strategię, a następnie przygotować odpowiedni sposób postępowania. Po drugie, wykorzystanie źródeł jawnych daje możliwość przeciwdziałania mechanizmom pozyskiwania nowych członków i zwolenników organizacji. Dzięki funkcji naprowadzającej zdobyte informacje mogą być wskazówką do podejmowania działań antyterrorystycznych. Po trzecie, OSINT może stanowić uzupełnienie i/lub weryfikację źródła operacyjnego w celu kompleksowego rozpracowania organizacji. Długotrwała aktywność służb, która prowadzi m.in. do ustalenia

[37] T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*…, s. 85.

[38] RAND Corporation – amerykański think tank i organizacja badawcza non profit, założona 14 maja 1948 r. na potrzeby Sił Zbrojnych Stanów Zjednoczonych. Obecnie RAND zatrudnia ok. 1600 pracowników w sześciu siedzibach w USA oraz w Europie. Prowadzi badania w dziedzinach obronności i terroryzmu, stosunków międzynarodowych, edukacji czy zdrowia publicznego. Za: Wikipedia, https://pl.wikipedia.org/wiki/RAND_Corporation [dostęp: 29 XII 2023].

[39] Za: T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*…, s. 86.

[40] K. Liedel, P. Piasecka, T. Aleksandrowicz, *Analiza informacji*…, s. 25.

[41] Tamże.

[42] T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*…, s. 87.

[43] K. Liedel, P. Piasecka, T. Aleksandrowicz, *Analiza informacji*…, s. 25.

korelacji zjawisk, jest możliwa dzięki wykorzystaniu źródeł otwartych, w tym naukowych, w ramach outsourcingu wywiadowczego[44].

Potencjał OSINT został zauważony także w sferze biznesu, który rozwinął dziedzinę wywiadu gospodarczego. Ocenia się, że wielkie korporacje mogą dysponować dziś większym i bardziej efektywnym aparatem wywiadowczym niż służby wywiadowcze mniej zamożnych państw[45]. Biznes korzysta w tym celu z usług wywiadowni gospodarczych, które cieszą się już międzynarodową popularnością. Mają one charakter przedsiębiorstw wykonujących zadania z zakresu wywiadu gospodarczego, takie jak sporządzanie raportów o podmiotach gospodarczych, opracowywanie rankingów wiarygodności firm, określanie bezpiecznego poziomu finansowania przedsięwzięć gospodarczych. Dodatkowo zajmują się określaniem trendów w sektorach gospodarczych, tworzeniem baz danych i wykazów dłużników, oferują wsparcie przy windykacji i współpracują z bankami i firmami ubezpieczeniowymi w ramach analizy ryzyka[46]. Wywiadownie gospodarcze (również agencje detektywistyczne) bazują na informacjach pozyskanych często ze źródeł otwartych. Wskazują przy tym na etykę i zgodność z prawem swoich działań, a także na zachowanie dyskrecji cenionej w biznesie. Źródła jawne wykorzystywane w wywiadzie gospodarczym to m.in. publiczne wypowiedzi (np. przedstawicieli zarządów), serwisy społecznościowe (w tym branżowe, np. LinkedIn), sondy społeczne, dokumentacje i rejestry z otwartym dostępem czy ogłoszenia sądowe.

Istnieją jednak ograniczenia OSINT. Są to m.in.:

1) **zbyt duża ilość danych** – zdobywanie olbrzymiej liczby informacji wiąże się z pozyskiwaniem również tych nieistotnych z wywiadowczego punktu widzenia. To zjawisko powoduje czasochłonność prowadzenia analizy, a wyselekcjonowanie wiarygodnych informacji wymaga fachowej wiedzy, umiejętności oraz sporego doświadczenia. Innymi słowy, największa zaleta OSINT jest jednocześnie jego wadą;
2) **nieprecyzyjne informacje** – pozyskane dane mogą być nieprecyzyjne, stronnicze albo wprowadzać dezinformację. Informacje w internecie są często wielokrotnie kopiowane, zwykle bez podawania pierwotnego źródła, co komplikuje ocenę ich przydatności, aktualności i rzetelności. Weryfikacja źródeł, choć może ograniczyć problemy, nie wyeliminuje ich całkowicie;

[44] T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*…, s. 88–90.

[45] Tamże, s. 92.

[46] P. Niemczyk, *Wywiadownie gospodarcze jako źródło informacji „białego wywiadu"*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 147.

3) **ograniczenia prawne** – istnieje wiele złożonych kwestii prawnych związanych z pozyskiwaniem, przechowywaniem i niszczeniem danych pochodzących ze źródeł otwartych. W polskim prawie ograniczenia wynikają z praw człowieka (obejmujących prawo do prywatności, wolności słowa, ochrony danych osobowych i własności intelektualnej) oraz aktów prawa międzynarodowego[47];
4) **ograniczenia językowe** – problem bariery językowej zawsze towarzyszy działalności wywiadowczej. Chociaż język angielski dziś jest jednym z najpowszechniej używanych na świecie, to informacje z części globu stanowiących najsilniejsze punkty zapalne nie są publikowane w sieci w tym języku na tyle często, by było możliwe efektywne pozyskiwanie danych. Szacuje się, że nawet 50–80% informacji dotyczących krajów wywiadowczego zainteresowania państw zachodnich nie jest publikowane w języku angielskim[48]. Brak specjalistów posługujących się językami, takimi jak arabski, chiński czy rosyjski, znacznie ogranicza przydatność białego wywiadu, nawet przy wykorzystaniu elektronicznych translatorów. Wskazuje się też na konieczność posiadania wiedzy kulturowej w zakresie rozpatrywanego zagadnienia – znajomość realiów historycznych, społecznych i politycznych pozwala na prawidłową interpretację informacji oraz ocenę wiarygodności źródeł[49];
5) **rozwój technologiczny** – dynamiczny rozwój sprawia, że technologie wykorzystywane do pozyskiwania danych mogą się szybko zdezaktualizować. Duże nadzieje pokłada się w inteligentnych, samouczących się algorytmach, jednak wizja zrobotyzowanego białego wywiadu wydaje się wciąż odległa. Szybkość przyrostu informacji znacznie przewyższa możliwości współczesnych programów przeznaczonych do ich analizy[50]. Dlatego analitycy OSINT muszą ciągle aktualizować swoją wiedzę i podnosić swoje kwalifikacje;
6) **konieczność przestrzegania bezpieczeństwa operacji** (ang. *operations security*, OPSEC) – pozyskiwanie informacji ze źródeł otwartych wymaga

[47] Zob. art. 12 *Powszechnej Deklaracji Praw Człowieka z dnia 10 grudnia 1948 r.*, https://www.bb.po.gov.pl/images/Prawa/PNZ/PDPCZ.pdf [dostęp: 13 XII 2023]; art. 17 *Międzynarodowego Paktu Praw Obywatelskich i Politycznych otwartego do podpisu w Nowym Jorku dnia 19 grudnia 1966 r.*; art. 8 *Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności sporządzonej w Rzymie dnia 4 listopada 1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz uzupełnionej Protokołem nr 2*; art. 7–8 *Karty praw podstawowych Unii Europejskiej*.

[48] B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 36.

[49] T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*…, s. 91.

[50] B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 35.

działania w zgodzie z OPSEC, rozumianym jako (…) *proces zapewniający odpowiedni poziom bezpieczeństwa operacjom lub działaniom* (…) *w celu ukrycia przed przeciwnikiem możliwości i zamiarów sił własnych*[51];

7) **niska przydatność w niektórych obszarach** – biały wywiad nie zawsze będzie uniwersalny i wszechstronny. Terroryści działający w pojedynkę (ang. *lone wolves*) są np. niemożliwi do zlokalizowana i – ze względu na brak podejrzanych powiązań – zapobieganie ich działalności jest trudne[52]. Przywódcy najgroźniejszych grup terrorystycznych wykorzystują internet do celów propagandowych bardzo profesjonalnie i nie zostawiają cyfrowych śladów (ang. *digital footprint*). Przez większość czasu znajdują się w miejscach odciętych zarówno od sieci, jak i od świadków. W takich przypadkach zdobycie danych jest możliwe jedynie dzięki działalności źródeł osobowych (ang. *human intelligence*, HUMINT)[53].

Najpopularniejsza i najbardziej odpowiednia klasyfikacja źródeł białego wywiadu wyodrębnia:

1) wystąpienia publiczne,
2) dokumenty publiczne,
3) programy nadawane publicznie,
4) szarą literaturę,
5) komercyjne bazy danych,
6) internet i media społecznościowe[54].

Wystąpienia publiczne to przekazywanie informacji drogą ustną podczas wydarzeń otwartych i odbywających się w miejscach publicznych. Obejmują one m.in.: dokumentację sądową, wyniki kontroli organów do tego uprawnionych, konferencje prasowe, wiece polityczne, posiedzenia rządu, wykłady, debaty akademickie, kazania religijne, wystawy naukowe i komercyjne. Przyjmuje się, że podczas wystąpień publicznych mówca i słuchacze nie oczekują prywatności[55].

Dokumentami publicznymi są rzeczowe świadectwa danego zjawiska sporządzone w formie właściwej dla danego miejsca i czasu, np.: książki i podręczniki,

[51] *AAP-6 Słownik terminów i definicji NATO*, 2017, https://wcnjik.wp.mil.pl/u/AAP6PL.pdf, s. 336 [dostęp: 24 II 2021].

[52] B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 115.

[53] Taka sytuacja zaistniała podczas ustalania miejsca pobytu Osamy bin-Ladena w 2011 r. Zob. B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 36.

[54] Klasyfikacja na podstawie: *Rozpoznanie ze źródeł otwartych DD-2.9(A)*…, s. 47–50.

[55] Tamże, s. 47.

czasopisma fachowe, ulotki i broszury marketingowe, mapy, fotografie[56], materiały publikowane przez rządy (raporty, dane statystyczne, projekty legislacyjne)[57].

Program nadawany publicznie należy rozumieć jako (…) *jednoczesną transmisję informacji dla użytku ogólnego do odbiorników (przekaźników) w ramach sieci komputerowej, radiowej, telekomunikacyjnej lub telewizyjnej*[58]. Można tu wyszczególnić źródła radiowe i telewizyjne, a z tej klasyfikacji wyodrębnić radiowe rozgłośnie informacyjne, filmy (programy) dokumentalne, materiały filmowe oraz programy radiowe inne niż rozrywkowe[59].

Pod pojęciem szarej literatury kryją się informacje niezastrzeżone, a równocześnie niedostępne komercyjnie. Obejmują one m.in.:

- książki (opracowania) nieobjęte rejestracją bibliograficzną,
- niepublikowane tłumaczenia,
- projekty i rysunki techniczne,
- sprawozdania i raporty naukowe (techniczne, ekonomiczne, społeczne),
- dokumenty dotyczące standardów technicznych (normy, zalecenia, ekspertyzy),
- materiały promocyjne i reklamowe,
- dysertacje magisterskie i doktorskie,
- wewnętrzne materiały metodyczne i szkoleniowe[60].

Źródła szarej literatury są dostępne dzięki specjalistycznym kanałom lub przez bezpośredni kontakt z organizacjami je wytwarzającymi. Przykładami mogą być: agencje rządowe, organizacje pozarządowe, ośrodki akademickie, biblioteki, profesjonalne towarzystwa branżowe oraz ośrodki badawcze statutowo nieprowadzące działalności wydawniczej[61]. Szara literatura jest kolportowana w ograniczonej liczbie egzemplarzy, jednak dostęp do niej jest utrudniony tylko pozornie. W wielu krajach oraz wspólnotach funkcjonują elektroniczne bazy danych, które umożliwiają dotarcie do tego typu dokumentów za pomocą wyszukiwarki. W Europie taką bazą jest OpenGrey (www.opengrey.eu), w Polsce – serwis Nauka Polska (www.nauka-polska.pl), który umożliwia dostęp do baz zawierających raporty i sprawozdania z badań naukowych, informacje o pracach badawczo-rozwojowych, materiały konferencyjne oraz spisy nazwisk osób związanych z danymi dziedzinami nauki[62].

---

[56] Tamże.

[57] K. Liedel, *Zarządzanie informacją*…, s. 65.

[58] *Rozpoznanie ze źródeł otwartych DD-2.9(A)*…, s. 47.

[59] K. Liedel, P. Piasecka, T. Aleksandrowicz, *Analiza informacji*…, s. 58.

[60] Zob. *Rozpoznanie ze źródeł otwartych DD-2.9(A)*…, s. 50; B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 70.

[61] Tamże.

[62] B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 71–72.

Profesjonalne bazy, do których dostęp można uzyskać po opłaceniu abonamentu, takie jak Factiva (www.factiva.com), LexisNexis (www.lexis-nexis.com), Dialog (www.dialog.com), komercyjne bazy fotografii i obrazów (np. z dostępem do zdjęć satelitarnych powierzchni Ziemi), znajdują się na pograniczu otwartości źródeł[63].

Najważniejszym i wymagającym odrębnego omówienia źródłem jest internet. Samą sieć internetową porównuje się do góry lodowej. Jej mały, widoczny wierzchołek stanowi jawna, zindeksowana część, pod powierzchnią wody znajduje się zaś niezmierzona ilość treści o ograniczonym dostępie[64]. Internet dzieli się na trzy poziomy:

1) sieć zindeksowaną (ang. *surface web*), czyli używaną powszechnie, jawną część,
2) sieć głęboką (ang. *deep web*), której treści są niedostępne przy użyciu darmowych i powszechnych wyszukiwarek, obejmującą prywatne strony, na których jest konieczna rejestracja w celu uzyskania dostępu,
3) sieć ciemną (ang. *dark web*), która jest częścią sieci głębokiej, stanowiącą zbiór niewidocznych publicznie stron. Tego typu strony są zakodowane (zaszyfrowane) i dostęp do nich wymaga konkretnej konfiguracji lub autoryzacji albo specjalnego oprogramowania[65].

Szacuje się, że niemal połowa populacji świata ma dostęp do internetu. Co roku do użytkowników sieci dołączają setki milionów nowych. W 2014 r. ogólna liczba stron internetowych przekroczyła 1 mld[66]. Pięć lat później oceniano, że średnio co minutę na portalu Facebook pojawiało się ok. 500 000 nowych komentarzy, 293 000 postów oraz 450 000 zdjęć[67]. Media społecznościowe są ważnym elementem internetu z punktu widzenia białego wywiadu. Przykładami takich mediów są sieci:

- społecznościowe,
- fachowe (branżowe),
- networkingowe,
- do publicznego udostępniania treści wideo (wideoblogi), audio (podcasty) oraz zdjęć (hosting),
- z blogami i mikroblogami.

---

[63] K. Liedel, *Zarządzanie informacją*…, s. 65.

[64] Zawartość sieci zindeksowanej szacuje się na 4%, sieci głębokiej na 90%, a sieci ciemnej na 6% objętości treści w całym internecie. Za: T. Leżoń, *Głęboko pod powierzchnią jest miejsce, o którym wolałbyś nie wiedzieć*, Magazyn TVN24, https://tvn24.pl/magazyn-tvn24/gleboko-pod-powierzchnia-jest-miejsce-o-ktorym-wolalbys-nie-wiedziec,95,1850 [dostęp: 12 III 2021].

[65] *Rozpoznanie ze źródeł otwartych DD-2.9(A)*…, s. 48–49.

[66] P.W. Singer, E.T. Brooking, *Nowy rodzaj wojny. Media społecznościowe jako broń*, Kraków 2019, s. 76.

[67] Tamże, s. 86.

Media społecznościowe zawdzięczają popularność przemianom społeczno-kulturowym oraz technologicznym w zakresie upowszechnienia internetu mobilnego i urządzeń mobilnych[68]. Pozyskiwanie informacji z social mediów przez biały wywiad może być uznane dziś za subdyscyplinę OSINT, która w literaturze anglojęzycznej ma nazwę SOCMINT (ang. *social media intelligence*)[69]. Jej cel to identyfikacja i zrozumienie węzłów sieci oraz relacji między nimi[70]. SOCMINT jest przydatny szczególnie w pracy organów ścigania oraz prokuratury. Portale społecznościowe dostarczają materiałów dowodowych dotyczących popełnienia czynów zabronionych, takich jak zniesławienia, zniewagi, stalking, rozpowszechnianie pornografii, naruszenie prawa wyborczego czy nawet handel ludźmi[71]. Brak autorefleksji podczas publikowania informacji osobistych w sieci albo wyrażanie opinii w sposób widoczny dla wszystkich użytkowników jest ułatwieniem dla służb i organów ścigania.

Zdjęcia publikowane w sieci często zawierają metadane, czyli informacje o pliku, takie jak np. jego wielkość, data wykonania, autor, w przypadku zdjęcia urządzenie, jakim je zrobiono, a nawet dane na temat lokalizacji urządzenia w momencie wykonania fotografii[72]. Amerykańskie rządowe oprogramowanie RIOT (ang. *Rapid Information Overlay Technology*) zaprezentowane w 2010 r. wyszukuje i łączy metadane. Ten system służy do profilowania obywateli na podstawie informacji z serwisów społecznościowych. Potrafi wskazać lokalizacje i przeanalizować aktywność w miejscach, w których dana osoba przebywała, a także stworzyć sieć powiązań z innymi użytkownikami social mediów[73]. Podobne zastosowanie ma oprogramowanie Maltego, które wyszukuje relacje między publicznie dostępnymi treściami oraz pozwala je skonwertować i przedstawić siatkę powiązań za pomocą grafu. Istotnym elementem analizy OSINT przy użyciu metadanych jest wykorzystanie geolokalizacji. Metadane zapisywane automatycznie przez urządzenie, którym wykonuje się fotografię (nagranie), pozwalają zwykle na późniejsze zlokalizowanie użytkownika.

---

[68] Szacuje się, że liczba urządzeń mobilnych już w 2012 r. zrównała się z liczbą ludności świata. Za: M. Nowina-Konopka, *Infomorfoza*…, s. 106.

[69] B. Saramak, *Wykorzystanie otwartych źródeł informacji*…, s. 84.

[70] *Rozpoznanie ze źródeł otwartych DD-2.9(A)*…, s. 49.

[71] B. Stromczyński, P. Waszkiewicz, *Biały wywiad w praktyce*…, s. 162.

[72] Tamże, s. 152.

[73] *RIOT – rządowy system inwigilacji i profilowania przez serwisy społecznościowe*, Niebezpiecznik, 17 II 2013 r. https://niebezpiecznik.pl/post/riot-rzadowy-system-inwigilacji-przez-serwisy-spolecznosciowe/ [dostęp: 16 III 2021].

Możliwości białego wywiadu są zauważane i doceniane przez coraz większą liczbę służb specjalnych[74] i policyjnych. Współcześnie nawet sądy przychylnie patrzą na dowody zgromadzone w ten sposób. Punktem zwrotnym w tym zakresie była sprawa libijskiego zbrodniarza Mahmuda al-Werfallego. W sierpniu 2017 r. Międzynarodowy Trybunał Karny w Hadze wydał nakaz jego aresztowania na podstawie dowodów opartych niemal wyłącznie na informacjach z mediów społecznościowych[75]. Wykorzystanie w procesie sądowym materiałów pochodzących z OSINT jest jednak skomplikowane z uwagi na niezbędną rzetelność informacji i ich źródeł, a także potrzebę utrwalania takich materiałów w specjalnych bazach danych. To kluczowe w kontekście trwałości i równocześnie ulotności treści internetowych. Z jednej strony, informacje raz udostępnione w sieci są niemal niemożliwe do usunięcia, z drugiej strony, w gąszczu informacji trudno odnaleźć taką, która zwróci uwagę odbiorcy.

Tematem OSINT są zainteresowani także dziennikarze śledczy. Narzędzia białego wywiadu umożliwiają im uzyskanie informacji na temat np. konfliktów zbrojnych, wpływowych osób, działalności skrajnych światopoglądowo grup, brutalności resortów siłowych czy degradacji środowiska naturalnego[76]. Pojedynczy obywatele, w tym hobbyści i pasjonaci[77], również korzystają z OSINT, a z roku na rok rośnie liczba otwartych szkoleń, organizowanych głównie przez instytucje związane z cyberbezpieczeństwem[78].

OSINT w zarządzaniu bezpieczeństwem informacji – studium przypadku

Rozwój technologii i mediów społecznościowych doprowadził do tego, co można nazwać złotym wiekiem OSINT[79]. Punktem zwrotnym oraz krokiem w kierunku budowania społeczeństwa odpornego na dezinformację były obserwacje m.in. Eliota

[74] Zob. wykład Agencji Wywiadu pt. *OSINT – nie lekceważ białego wywiadu*, zorganizowany 12 I 2022 r. we współpracy ze studenckimi kołami naukowymi Uniwersytetu Warszawskiego, www.facebook.com/events/1035173887046324/ [dostęp: 16 I 2022].

[75] E. Higgins, *Bellingcat. Ujawniamy prawdę w czasach postprawdy*, Katowice 2021, s. 277.

[76] Tamże, s. 293.

[77] Zob. *OSINT Quest Challenge* organizowany z inicjatywy pasjonatów analizy źródeł otwartych, www.osintquest.pl/category/challenge [dostęp: 16 I 2022].

[78] Zob. m.in. szkolenie *OSINT: zaawansowane pozyskiwanie szczegółowych informacji na temat ludzi i firm* organizowane przez redakcję portalu Niebezpiecznik czy seria „OSINT master" zespołu portalu Sekurak.

[79] *The Golden Age of OSINT is over*, Key Findings, 4 I 2019 r., https://keyfindings.blog/2019/01/04/the-golden-age-of-osint-is-over/ [dostęp: 6 II 2022].

Higginsa, który odkrywał zagrożenia i potencjał źródeł otwartych. Jak stwierdził w swojej książce pt. *Bellingcat. Ujawniamy prawdę w czasach postprawdy*, natrafił na lukę w systemie informacji i postanowił codziennie ją zapełniać[80].

Brytyjczyk Eliot Higgins (ur. w 1979 r.) pierwsze kroki w obywatelskim dziennikarstwie śledczym stawiał w 2012 r. na blogu „Brown Moses", na którym skupiał się na wyjaśnianiu przypadków użycia broni chemicznej w Syrii. Nie znał języka arabskiego, więc po arabskojęzycznej części sieci poruszał się przy użyciu internetowego translatora. Prowadzone śledztwa przysporzyły mu popularności, a wraz z wyjaśnianiem kolejnych spraw zyskiwał coraz większą liczbę fanów, współpracowników i wolontariuszy. W konsekwencji tego powstała grupa Bellingcat. Dziś funkcjonuje ona jako globalna społeczność internetowa, której zadaniem jest prowadzenie śledztw, zwalczanie dezinformacji i tropienie zbrodni wojennych na podstawie danych ze źródeł otwartych.

Bellingcat ma charakter społeczny i egalitarny; funkcjonuje jako (…) *agencja wywiadowcza dla wszystkich*[81]. Motto organizacji opiera się na trzech filarach: odkrywanie (spraw, które pominięto lub które można wyśledzić w internecie), weryfikowanie (dowodów) i nagłaśnianie (uzyskanych informacji)[82]. Zespół składa się z zawodowych dziennikarzy śledczych oraz ze stałych współpracowników i wolontariuszy. Swoją działalność finansuje ze zbiórek publicznych, z grantów i płatnych szkoleń[83]. Unika przy tym finansowania przez rządy państw, co ma zapewnić organizacji niezależność. Uzyskane wyniki prezentuje na stronie internetowej (www.bellingcat.com) w formie raportów, artykułów i podcastów. Wśród sukcesów grupy można wymienić: udowodnienie użycia broni chemicznej w Syrii (2012 r.), zidentyfikowanie sympatyków Państwa Islamskiego w Europie (2016 r.), rozpracowanie neonazistowskiej grupy odpowiedzialnej za zamieszki w Charlottesville w Stanach Zjednoczonych (2017 r.), ujawnienie udziału rosyjskich agentów w otruciu w Anglii Siergieja Skripala (2018 r.), współuczestnictwo w demaskowaniu dezinformacji związanej z pandemią SARS-CoV-2 (od 2019 r.).

W niniejszym artykule przedmiotem analizy przypadku będzie zestrzelenie samolotu Boeing 777-00ER, lot nr MH17 linii lotniczych Malaysia Airlines z Amsterdamu do Kuala Lumpur 17 lipca 2014 r., do którego doszło w przestrzeni powietrznej obwodu donieckiego w Ukrainie kontrolowanego przez prorosyjskich separatystów.

---

[80] E. Higgins, *Bellingcat. Ujawniamy prawdę*…, s. 69.

[81] Tamże, s. 17.

[82] Tamże, s. 91.

[83] B. Biel, *Internet pełen jest dowodów na zbrodnie. Trzeba wiedzieć, gdzie ich szukać*, Magazyn TVN24, https://tvn24.pl/magazyn-tvn24/internet-pelen-jest-dowodow-na-zbrodnie-trzeba-wiedziec-gdzie-ich-szukac,158,2754 [dostęp: 26 I 2022].

Zginęły wszystkie osoby będące na pokładzie – 283 pasażerów i 15-osobowa załoga[84]. Portal Bellingcat zaczął działalność dwa dni przed tym zdarzeniem. Przez kolejne lata grupa pracowała nad wykryciem przyczyn tragedii i osób za nią odpowiedzialnych oraz demaskowaniem manipulacji przekazów dotyczących przebiegu katastrofy. Efektem tego były szczegółowe raporty prezentowane w latach 2014–2019.

W jednym z pierwszych raportów można prześledzić drogę, jaką przebył wojskowy konwój przewożący system kierowanych pocisków Buk M1. Zdjęcie opublikowane 25 lipca 2014 r. przez „Paris Match" przedstawia system transportowany na samochodzie ciężarowym. Analiza fotografii pozwoliła wskazać miejsce oraz czas jej wykonania (określony przez położenie słońca, co ustalono na podstawie cienia rzucanego przez pojazd). Późniejsze posty i nagrania w sieci dostarczały kolejnych informacji dotyczących trasy konwoju. W następnych dniach system Buk był transportowany już nie na samochodzie ciężarowym, lecz poruszał się na gąsienicach.

Kilka dni wcześniej, 17 lipca, miejscowi dziennikarze informowali o wyrzutni z załadowanymi czterema pociskami rakietowymi SA-11. Według lokalnych informacji ok. godziny 16.20 dało się słyszeć huk, po którym zaobserwowano szczątki samolotu spadające z nieba. Kilka godzin później w sieci opublikowano zdjęcie dymu charakterystycznego dla momentu po wystrzeleniu pocisku. Na tej podstawie, a także przy użyciu zdjęć satelitarnych wywiadu Stanów Zjednoczonych oraz fotografii i zeznań świadków, metodą wcięć ustalono dokładne miejsce wystrzelenia pocisku[85]. Ostatni z analizowanych materiałów wideo z 18 lipca ukazywał system Buk podczas ponownego transportu prawdopodobnie tym samym samochodem ciężarowym. Wyrzutnia przewoziła wówczas już tylko trzy pociski[86].

Do przeprowadzenia dalszego śledztwa Bellingcat wykorzystał, oprócz fotografii, nagrań i relacji świadków, posty rosyjskich żołnierzy opublikowane w mediach społecznościowych (VK, Instagram, Odnoklassniki). Niejednokrotnie to oni sami bezrefleksyjnie ogłaszali, gdzie znajdują się w danym momencie, albo wykonywali fotografie, na których detale widoczne w tle zdradzały ich lokalizację[87]. Z uzyskanych dowodów wynikało, że system Buk do strefy walk został dostarczony przez 53 Rakietową Brygadę Przeciwlotniczą z Kurska. Analiza z wykorzystaniem wyszukiwarek,

---

[84] M. Miśko, *Gdyby nie Internet dowodów na tę zbrodnię być może by nie było*, GeekWeb, https://www.geekweb.pl/magazyn-dobrych-tresci/item/1788-proces-o-zestrzelenie-mh17-w-2014-roku [dostęp: 26 I 2022].

[85] *MH17. The Open Source Evidence. A Bellingcat Investigation*, Bellingcat, https://www.bellingcat.com/app/uploads/2015/10/MH17-The-Open-Source-Evidence-EN.pdf [dostęp: 6 II 2022].

[86] *MH17: Source of Separatists' Buk. A Bellingcat Investigation*, Bellingcat, https://www.bellingcat.com/app/uploads/2014/11/Origin-of-the-Separatists-Buk-A-Bellingcat-Investigation1.pdf [dostęp: 6 II 2022].

[87] B. Biel, *Internet pełen jest dowodów na zbrodnie…*

forów i mediów społecznościowych (w tym ponad 200 profili żołnierzy) umożliwiła odtworzenie siatki powiązań oraz zrekonstruowanie całej struktury brygady wraz z jej uzbrojeniem i nazwiskami żołnierzy niemal wszystkich szczebli. W ten sposób ustalono role osób odpowiedzialnych za zestrzelenie malezyjskiego samolotu, w tym tych z kręgów rosyjskiej armii, wywiadu wojskowego oraz prorosyjskich separatystów.

Krótko po zestrzeleniu samolotu strona rosyjska starała się stworzyć narrację, zgodnie z którą odpowiedzialność za katastrofę ponosi Ukraina. Przedstawiano spreparowane dowody, a w kampanię były zaangażowane zarówno rosyjskie Ministerstwo Obrony, jak i portale Russia Insider, Sputnik, RT (dawna Russia Today) oraz pracownicy Agencji Badań Internetowych (potocznie nazywanej fabryką trolli), którzy w ciągu trzech dni od katastrofy tylko na portalu Twitter opublikowali łącznie 111 486 dezinformacyjnych postów[88]. Proces dezinformacji wzmocniono dyskredytowaniem Bellingcat. Ataki były przeprowadzane przez portale i blogi pozornie niezwiązane ze sobą, które jednak mają źródła w rosyjskich ośrodkach wpływu. Przeciwko Higginsowi i jego zespołowi używano też socjotechnik w celu przejęcia ich kont mailowych. Pomimo to zespół Bellingcat sukcesywnie publikował wyniki śledztwa oraz zwalczał manipulacje, dzięki czemu w kolejnych latach wszczęto oficjalne śledztwo.

W 2016 r. Połączony Zespół Śledczy (Joint Investigation Team, JIT) pod przewodnictwem prokuratury holenderskiej ogłosił, że poszukuje informacji o rosyjskich wojskowych i separatystach, których rozmowy telefoniczne przechwyciła Służba Bezpieczeństwa Ukrainy. Bellingcat uznał te osoby za kluczowe dla śledztwa w sprawie lotu MH17 i zidentyfikował je[89]. W maju 2017 r. JIT oficjalnie potwierdził, że system Buk wykorzystany do zestrzelenia samolotu został sprowadzony z Rosji, a jego właścicielem jest brygada z Kurska[90]. W czerwcu 2019 r. ogłoszono, że zarzuty zostaną postawione trzem Rosjanom: Siergiejowi Dubinskiemu, Igorowi Girkinowi i Olegowi Pułatowowi oraz Ukraińcowi Leonidowi Charczence. Na konferencji potwierdzono wszystkie dowody i ustalenia zgromadzone wcześniej przez Bellingcat[91]. Postępowanie karne rozpoczęło się w 2020 r. w Holandii i przebiegło na podstawie lokalnego prawa, ponieważ 193 ofiary katastrofy spośród wszystkich 298 pochodziły właśnie z tego kraju. Oskarżeni byli sądzeni zaocznie. Proces uważany za kulminację (…) *najbardziej skomplikowanego śledztwa w historii prawnej Niderlandów*[92] zakończył się w listopadzie 2022 r. Wyrokiem sądu okręgowego w Hadze Dubinski, Girkin oraz Charczenko zostali skazani na karę dożywotniego pozbawienia wolności oraz

[88] E. Higgins, *Bellingcat. Ujawniamy prawdę*…, s. 114.

[89] B. Biel, *Internet pełen jest dowodów na zbrodnie*…

[90] Tamże.

[91] M. Miśko, *Gdyby nie Internet*…

[92] Tamże.

zobowiązani do wypłacenia krewnym ofiar 16 mln euro odszkodowania. Pułatowa uniewinniono z powodu braku dowodów[93].

Śledztwo grupy Bellingcat udowadnia, że informacje niejawne mogą stać się jawnymi dzięki wykorzystaniu OSINT. Zespołowi udało się odtworzyć drogę rosyjskiego konwoju, a przy okazji także strukturę rosyjskiej brygady, wyłącznie na podstawie danych ze źródeł otwartych. Dziennikarze odkryli dowody, które jednoznacznie wskazywały na zaangażowanie Rosji w konflikt na wschodzie Ukrainy, kilka lat wcześniej niż oficjalne organy państw europejskich[94].

Wnioski

W literaturze przedmiotu podkreśla się, że bezpieczeństwo organizacji nie jest produktem, lecz ciągłym procesem[95]. Myśl tę rozwinął Kavin Mitnick: bezpieczeństwo (…) *nie jest problemem technologicznym, tylko problemem związanym z ludźmi i zarządzaniem*[96]. Zarządzanie bezpieczeństwem informacji opiera się jednak na wszystkich filarach związanych z zarządzaniem ludźmi, odpowiednimi procedurami oraz technologią. Skuteczność ISM zależy od tego, czy środki bezpieczeństwa zostaną odpowiednio wyodrębnione oraz sklasyfikowane. Zgodnie z przyjętym podziałem dzielą się one na: personalne, techniczne, fizyczne oraz organizacyjno-proceduralne.

Personalne środki bezpieczeństwa powinny obejmować wszystkie osoby w organizacji, a szczególnie kierownictwo i tych, którzy mają dostęp do informacji niejawnych[97]. Jak zauważa Mitnick, (…) *firma może dokonać zakupu najlepszych i najdroższych technologii bezpieczeństwa, wyszkolić personel tak, aby każda poufna informacja była trzymana w zamknięciu, wynająć najlepszą firmę chroniącą obiekty i wciąż pozostać niezabezpieczoną.* (…) *Dlaczego? Ponieważ to czynnik ludzki jest piętą achillesową systemów bezpieczeństwa*[98]. Istotne jest szkolenie pracowników na wszystkich szczeblach hierarchii, ze szczególnym uwzględnieniem nowo zatrudnionych. Dodatkowo należy skupić się na budowaniu świadomości na temat tego, jak dużo informacji można uzyskać ze źródeł otwartych, zarówno wśród

[93] *Malezyjski Boeing 777 zestrzelony przez Rosjan w 2014 r. Sąd w Hadze przedstawił stanowisko*, Dziennik Gazeta Prawna, 17 XI 2022 r., https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8590126,holandia-sad-zestrzelenie-2014-malezyjski-boeing-777-ukraina.html [dostęp: 9 X 2023].

[94] *About*, Bellingcat, https://www.bellingcat.com/about/ [dostęp: 2 II 2022].

[95] K. Mitnick, W. Simon, *Sztuka podstępu*…, s. 24.

[96] Tamże.

[97] K. Liedel, *Zarządzanie informacją*…, s. 83.

[98] K. Mitnick, W. Simon, *Sztuka podstępu*…, s. 23–24.

zatrudnionych w organizacji użytkowników sieci, jak i ich rodziny i przyjaciół. Kolejnym środkiem powinno być uniemożliwienie dostępu do informacji niejawnych osobom nieuprawnionym. Należy zapewnić prewencyjne wykrywanie osób, których zatrudnienie może naruszyć bezpieczeństwo informacyjne (postępowanie sprawdzające). Warto przeprowadzać rutynowe kontrole osób mających dostęp do koszy na śmieci i niszczarek dokumentów (ekipy sprzątające lub osoby uprawiające tzw. *dumpster diving*), ponieważ mogą one wejść w posiadanie zdezaktualizowanych informacji niejawnych, jednak wartościowych z punktu widzenia np. konkurencji[99].

W zakresie stosowania **technicznych środków bezpieczeństwa informacyjnego** należy przestrzegać również zasady powszechności. Powinny zostać nią objęte wszystkie nośniki oraz urządzenia służące do przetwarzania informacji. Przechowywanie danych dotyczących organizacji i jej członków w odpowiednio zabezpieczonej bazie danych jest obligatoryjne.

Fizyczne środki bezpieczeństwa powinny obejmować wydzielenie stref bezpieczeństwa poddanych kontroli wejść i wyjść oraz stref administracyjnych służących do kontroli osób i pojazdów[100]. Należy to zastosować wobec wszystkich pomieszczeń, w których informacje niejawne są lub będą przechowywane. Organizacja powinna zapewnić dostęp do sieci intranet z organizacyjnymi środkami komunikacji (własnymi lub zewnętrznymi). Istotne jest certyfikowanie systemów i sieci używanych w organizacji przez uprawnione podmioty. Systemom tym należy zapewnić techniczne wsparcie oraz ochronę fizyczną, kryptograficzną i elektromagnetyczną, a także niezawodność transmisji[101].

W zakresie **proceduralno-organizacyjnym** najważniejszym elementem wydaje się zapewnienie odpowiednich zarobków osobom odpowiedzialnym za bezpieczeństwo organizacji. O ile w dużych przedsiębiorstwach ten problem praktycznie nie występuje, o tyle w tych z mniejszym budżetem rzadko zdarza się możliwość korzystania z profesjonalnej infrastruktury i z bieżącego monitorowania bezpieczeństwa. Podobną barierę napotykają instytucje związane z bezpieczeństwem państwa[102] oraz jego administracją[103]. Powoduje to olbrzymie różnice płacowe niekorzystne dla pracowników sektora publicznego. Organizacja powinna przeprowadzać

[99] Tamże, s. 185.

[100] K. Liedel, *Zarządzanie informacją*…, s. 85.

[101] Tamże, s. 86.

[102] M. Janik, *Wojska Obrony Cyberprzestrzeni stać najwyżej na studentów. „Z płaceniem zawsze był problem"*, INN Poland, 14 II 2019 r., https://innpoland.pl/150265,wojska-obrony-cyberprzestrzeni-place-w-wojsku-roznia-sie-znacznie-od-it [dostęp: 4 IV 2022].

[103] M. Kicka, *Tak zarabiają. Pensja zasadnicza na wybranych stanowiskach urzędników samorządowych*, Serwis Samorządowy PAP, 21 VIII 2019 r., https://samorzad.pap.pl/kategoria/archiwum/tak-zarabiaja-pensja-zasadnicza-na-wybranych-stanowiskach-urzednikow [dostęp: 4 IV 2022].

obowiązkowe szkolenia w zakresie celów polityki bezpieczeństwa informacji oraz postępowania z informacjami niejawnymi. Należy stosować odpowiednie klauzule niejawności oraz wyraźnie określić zakres odpowiedzialności za naruszenie zasad OIN. Po opracowaniu tych procedur i szkoleń kierownictwo powinno dać podwładnym wystarczająco dużo czasu na zapoznanie się z wytycznymi. Planowanie takiego szkolenia w czasie ponadnormatywnym lub wolnym od pracy negatywnie wpływa na przyswajanie informacji. Polityka bezpieczeństwa informacyjnego powinna być regularnie uaktualniana.

Bezpieczeństwo jest procesem, który powinien być stale monitorowany i usprawniany, jeżeli dana organizacja ceni sobie bezpieczeństwo informacyjne. Należy jednak pamiętać, że wszelkie zalecenia dotyczące bezpieczeństwa nie gwarantują całkowitej ochrony przed OSINT. Konieczne jest odpowiednie zarządzanie ryzykiem pozyskania informacji ze źródeł otwartych i zmniejszenie go do akceptowalnego poziomu. Ocena ryzyka powinna pozwolić na określenie, jakie informacje mają podlegać szczególnej ochronie, jakie występują wobec nich zagrożenia oraz jakie szkody może spowodować pozyskanie informacji chronionych (niejawnych). Odpowiednie ISM znacznie przyczyni się do ochrony zasobów w organizacji, a tym samym zostaną zapewnione korzyści wewnętrzne i zewnętrzne, w tym marketingowe, biznesowe oraz dla klientów i innych stron trzecich.

Myśl przytoczona na początku artykułu nie traci na aktualności. Współcześnie są ważne jednak dane nie tylko o nieprzyjacielu, lecz także o potencjalnym partnerze. Techniki i narzędzia OSINT znacznie ułatwiają ich uzyskanie. Dlatego z punktu widzenia organizacji pozyskanie informacji niejawnych działa zawsze na jej niekorzyść. Istotne jest więc wprowadzenie polityki bezpieczeństwa o charakterze prewencyjnym. Nieliczni komentatorzy argumentują, że złoty wiek OSINT, w którym analitycy mogli korzystać z niezliczonej ilości źródeł przy niskiej świadomości użytkowników sieci, dobiegł końca[104]. Jednak zainteresowanie białym wywiadem rośnie i nie przestaje być on zagrożeniem. Problematyka OSINT stwarza możliwość stawiania kolejnych pytań i nowych problemów badawczych. Wyniki tych badań i analiz poprawią bezpieczeństwo informacji będące bardzo ważnym zasobem organizacji. W przyszłości, dzięki zwiększeniu świadomości społecznej oraz poziomu rozwoju technologicznego, może to mieć pozytywny wpływ na działalność organizacji o charakterze społecznym i gospodarczym, jak również na bezpieczeństwo całego państwa.

[104] *The Golden Age of OSINT is over…*

Bibliografia

Aleksandrowicz T., *Biały wywiad w walce z terroryzmem*, w: *Rola mediów w przeciwdziałaniu terroryzmowi*, K. Liedel, P. Piasecka (red.), Warszawa 2009, s. 81–92.

Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki, W. Filipkowski, W. Mądrzejowski (red.),Warszawa 2011.

Higgins E., *Bellingcat. Ujawniamy prawdę w czasach postprawdy*, Katowice 2021.

Krawiec J., *System Zarządzania Bezpieczeństwem Informacji – zabezpieczenia*, „Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie" 2017, nr 1 (38), s. 46–59.

Krztoń W., *Zarządzanie informacją w procesach decyzyjnych organizacji*, „Modern Management Review" 2017, nr 3, s. 83–94.

Liedel K., *Zarządzanie informacją w walce z terroryzmem*, Warszawa 2010.

Liedel K., Piasecka P., Aleksandrowicz T., *Analiza informacji. Teoria i praktyka*, Warszawa 2012.

Łuczak J., Tyburski M., *Systemowe Zarządzanie Bezpieczeństwem Informacji ISO/IEC 27001*, Poznań 2009.

Mitnick K., Simon W., *Sztuka podstępu. Łamałem ludzi, nie hasła*, Gliwice 2016.

Niemczyk P., *Wywiadownie gospodarcze jako źródło informacji „białego wywiadu"*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 147–166.

Nowina-Konopka M., *Infomorfoza. Zarządzanie informacją w nowych mediach*, Kraków 2017.

Nowosad A., *Metody i techniki pozyskiwania i przetwarzania informacji medialnej na potrzeby białego wywiadu*, „Państwo i Społeczeństwo" 2005, nr 2, s. 59–69.

Rozpoznanie ze źródeł otwartych DD-2.9(A), Ministerstwo Obrony Narodowej, Centrum Doktryn i Szkolenia Sił Zbrojnych, Bydgoszcz 2020.

Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015.

Singer P.W., Brooking E.T., *Nowy rodzaj wojny. Media społecznościowe jako broń*, Kraków 2019.

Stanek S., *Podejmowanie decyzji w warunkach zagrożenia bezpieczeństwa informacyjnego organizacji*, Wrocław 2016.

Stromczyński B., Waszkiewicz P., *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo" 2014, nr 5, s. 146–170.

Tzu S., *Sztuka wojny. Traktat*, Gliwice 2012.

Wojciulik A., *Rola „białego wywiadu" w działalności służb specjalnych na przestrzeni wieków,* w: *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipkowski, W. Mądrzejowski (red.),Warszawa 2011, s. 43–55.

Źródła internetowe

AAP-6 Słownik terminów i definicji NATO, 2017, https://wcnjik.wp.mil.pl/u/AAP6PL.pdf [dostęp: 24 II 2021].

About, Bellingcat, https://www.bellingcat.com/about/ [dostęp: 2 II 2022].

Aleksandrowicz T., *„Efekt Snowdena"*, Wszystko Co Najważniejsze, 7 VI 2014 r., https://wszystkoconajwazniejsze.pl/tomasz-aleksandrowicz-efekt-snowdena/ [dostęp: 11 IV 2022].

Biel B., *Internet pełen jest dowodów na zbrodnie. Trzeba wiedzieć, gdzie ich szukać*, Magazyn TVN24, https://tvn24.pl/magazyn-tvn24/internet-pelen-jest-dowodow-na-zbrodnie-trzeba-wiedziec-gdzie-ich-szukac,158,2754 [dostęp: 26 I 2022].

Janik M., *Wojska Obrony Cyberprzestrzeni stać najwyżej na studentów. „Z płaceniem zawsze był problem"*, INN Poland, 14 II 2022 r., https://innpoland.pl/150265,wojska-obrony-cyberprzestrzeni-place-w-wojsku-roznia-sie-znacznie-od-it [dostęp: 4 IV 2022].

Kicka M., *Tak zarabiają. Pensja zasadnicza na wybranych stanowiskach urzędników samorządowych*, Serwis Samorządowy PAP, 21 VIII 2019 r., https://samorzad.pap.pl/kategoria/archiwum/tak-zarabiaja-pensja-zasadnicza-na-wybranych-stanowiskach-urzednikow [dostęp: 4 IV 2022].

Leżoń T., *Głęboko pod powierzchnią jest miejsce, o którym wolałbyś nie wiedzieć*, Magazyn TVN24, https://tvn24.pl/magazyn-tvn24/gleboko-pod-powierzchnia-jest-miejsce-o-ktorym-wolalbys-nie-wiedziec,95,1850 [dostęp: 12 III 2021].

Malezyjski Boeing 777 zestrzelony przez Rosjan w 2014 r. Sąd w Hadze przedstawił stanowisko, Dziennik Gazeta Prawna, 17 XI 2022 r., https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8590126,holandia-sad-zestrzelenie-2014-malezyjski-boeing-777-ukraina.html [dostęp: 9 X 2023].

MH17: Source of Separatists' Buk. A Bellingcat Investigation, Bellingcat, https://www.bellingcat.com/app/uploads/2014/11/Origin-of-the-Separatists-Buk-A-Bellingcat-Investigation1.pdf [dostęp: 6 II 2022].

MH17. The Open Source Evidence. A Bellingcat Investigation, Bellingcat, https://www.bellingcat.com/app/uploads/2015/10/MH17-The-Open-Source-Evidence-EN.pdf [dostęp: 6 II 2022].

Miśko M., *Gdyby nie Internet dowodów na tę zbrodnię być może by nie było*, GeekWeb, https://www.geekweb.pl/magazyn-dobrych-tresci/item/1788-proces-o-zestrzelenie-mh17-w-2014-roku [dostęp: 26 I 2022].

RIOT – rządowy system inwigilacji i profilowania przez serwisy społecznościowe, Niebezpiecznik, 17 II 2013 r. https://niebezpiecznik.pl/post/riot-rzadowy-system-inwigilacji-przez-serwisy-spolecznosciowe/ [dostęp: 16 III 2021].

The Golden Age of OSINT is over, Key Findings, 4 I 2019 r., https://keyfindings.blog/2019/01/04/the-golden-age-of-osint-is-over/ [dostęp: 6 II 2022].

www.bezpiecznymiesiac.pl [dostęp: 29 XII 2023].

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (t.j. DzU z 1997 r. nr 78 poz. 483, ze zm.).

Powszechna deklaracja praw człowieka (Rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) przyjęta i proklamowana 10 grudnia 1948 r.).

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (DzU z 1993 r. nr 61 poz. 284).

Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (DzU z 1977 r. nr 38 poz. 167).

Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 303/1 z 14 XII 2007 r.).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2023 r. poz. 913, ze zm.).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. DzU z 201 r. poz. 1781).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. DzU z 2023 r. poz. 756, ze zm.).

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. DzU z 2024 r. poz. 34).

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. DzU z 2020 r. poz. 344).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. DzU z 2022 r. poz. 902).

Ustawa z dnia 29 września 1994 r. o rachunkowości (t.j. DzU z 2023 r. poz. 120, ze zm.).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. DzU z 2022 r. poz. 2509).

Inne dokumenty

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [dostęp: 19 XII 2023].

Maciej Witczak

Absolwent Akademii Wojsk Lądowych im. gen. Tadeusza Kościuszki we Wrocławiu.

Kontakt: maciejwitczak1995@gmail.com

VARIA

Seminarium „25 lat Polski w Sojuszu. Pierwszy polski oficer w NATO”

Centralny Ośrodek Szkolenia i Edukacji
Agencji Bezpieczeństwa Wewnętrznego
im. gen. dyw. Stefana Roweckiego „Grota",
18 marca 2024 r.

IWONA OSŁOWSKA

Autorka niezależna
https://orcid.org/0000-0002-8625-0072

Przegląd Bezpieczeństwa Wewnętrznego, 2024, nr 30: 243–250

https://doi.org/10.4467/20801335PBW.24.010.19612

VARIA

Dnia 12 marca 1999 r. polski minister spraw zagranicznych Bronisław Geremek przekazał sekretarz stanu USA Madeleine Albright akt przystąpienia Polski do Organizacji Traktatu Północnoatlantyckiego. Proces akcesji zakończył się sukcesem dzięki solidarnemu działaniu liderów polskiej sceny politycznej, dyplomatów oraz wsparciu przyjaciół z zagranicy, w tym działaczy polonijnych, którzy wywierali wpływ na decyzje podejmowane w Waszyngtonie. W 2024 r. obchodzimy 25. rocznicę tego wydarzenia oraz 20. rocznicę śmierci gen. Ryszarda Kuklińskiego, bohatera zimnej wojny. Jego raporty i informacje ujawniły, jak armie Układu Warszawskiego mogłyby zareagować w przypadku ewentualnych operacji wojskowych, a także pomogły USA właściwie odpowiedzieć na manewry Układu w okresach napięć międzynarodowych.

Z okazji tych rocznic 18 marca 2024 r. w Centralnym Ośrodku Szkolenia i Edukacji Agencji Bezpieczeństwa Wewnętrznego im. gen. dyw. Stefana Roweckiego „Grota” odbyło się seminarium pt. „25 lat Polski w Sojuszu. Pierwszy polski oficer w NATO”. Spotkanie miało na celu przypomnienie, jak wyglądała polska droga

do NATO. Stanowiło również przyczynek do refleksji nad historią Rzeczpospolitej i bezpieczeństwem w Europie po 24 lutego 2022 r.

Zdjęcie 1. Historia i współczesność – problematyka poruszana podczas seminarium obejmowała zagadnienia związane z wejściem Polski w struktury NATO oraz wyzwaniami, z którymi obecnie mierzy się Sojusz Północnoatlantycki.

Źródło: materiały własne.

Podczas seminarium zaprezentowano pięć referatów. Pierwszy z nich pt. *Rola wschodniej flanki NATO* wygłosił moderator spotkania, dyrektor Muzeum Zimnej Wojny w Warszawie Filip Frąckowiak. Rozpoczął wystąpienie od zarysowania sytuacji geopolitycznej na początku XX w. Wskazał na imperialne plany Rosji i rewolucję bolszewicką, które pokrzyżowała zwycięska dla Polski Bitwa Warszawska w 1920 r., a także na skutki paktu Ribbentrop–Mołotow z 23 sierpnia 1939 r. Zakończenie II wojny światowej nie przyniosło spokoju podzielonej Europie. W 1947 r. ponownie przystąpiła ona do rywalizacji, tym razem na tle ideologicznym, politycznym, wojskowym i gospodarczym, określanej mianem zimnej wojny między blokiem wschodnim i jego państwami satelickimi a blokiem zachodnim, zrzeszonym od 1949 r. w Organizacji Traktatu Północnoatlantyckiego. Dyrektor Frąckowiak przedstawił kremlowskie plany podboju Europy, których potwierdzenie znajduje się w materiałach przekazanych CIA przez Kuklińskiego. Zwrócił uwagę także na przebieg transformacji systemowej, jaka dokonała się po 1989 r. w krajach satelickich Związku Radzieckiego. Byłaby ona niemożliwa bez wielu osób, których

aktywność przyczyniła się do powstania silnego bloku demokratycznego. Wskazał tu na pontyfikat Jana Pawła II oraz na Ryszarda Kuklińskiego.

Dyrektor Muzeum zasygnalizował, że rezygnacja USA z umieszczenia w Polsce elementów tarczy antyrakietowej (wrzesień 2009 r.) otworzyła Rosji drogę do aneksji Krymu w 2014 r. *Patrząc w przeszłość, powinniśmy tworzyć przyszłość, która będzie bezpieczna m.in. za sprawą silnej wschodniej flanki NATO, jeszcze bardziej potrzebnej po rosyjskiej agresji na Ukrainę w 2022 r.* – stwierdził Frąckowiak. Jednym ze sposobów wzmocnienia tej granicy Sojuszu jest zapowiedź udzielenia Polsce kredytu w wysokości 2 mld dolarów w ramach programu „Foreign Military Financing" na zakup amerykańskiego uzbrojenia, w tym 96 śmigłowców AH-64E Apache[1]. W trakcie prelekcji zebrani usłyszeli również o działaniach Unii Europejskiej, których celem jest rozwój europejskich sił zbrojnych, w tym o projekcie utworzenia do 2025 r. wspólnej armii (do 5000 żołnierzy). Jej zadaniem byłoby interweniowanie w sytuacjach kryzysowych[2]. W ocenie Frąckowiaka Polska ma silną pozycję w strukturze NATO, a agresja Rosji na Ukrainę spowodowała, że należy położyć większy nacisk na zapewnienie Europie bezpieczeństwa.

Zdjęcie 2. Spotkanie poprowadził Filip Frąckowiak, dyrektor Muzeum Zimnej Wojny.

Źródło: materiały własne.

[1] Zob. M. Bruszewski, *Biały Dom podał wysokość pożyczki dla Polski. Co ze śmigłowcami Apache?*, Defence24, 12 III 2024 r., https://defence24.pl/geopolityka/bialy-dom-podal-wysokosc-pozyczki--dla-polski-co-ze-smiglowcami-apache [dostęp: 8 IV 2024].

[2] *UE do 2025 chce stworzyć własne siły wojskowe*, Rzeczpospolita, 16 XI 2021 r., https://www.rp.pl/konflikty-zbrojne/art19109351-ue-do-2025-chce-stworzyc-wlasne-sily-wojskowe [dostęp 8 IV 2024].

Następną prelekcję, zatytułowaną *Polska droga do NATO*, wygłosił dr Krzysztof Zielke z ABW. Omówił następujące zagadnienia: cele i koncepcje rozszerzenia Sojuszu Północnoatlantyckiego, program „Partnerstwo dla Pokoju" jako polska droga do NATO, udział sił Sojuszu w operacji w Kosowie w 1999 r., której celem było zakończenie tam czystek etnicznych. Wskazał sukcesy i porażki polityki międzynarodowej w tamtym okresie. Warto pamiętać, że po 1989 r. wydarzenia na europejskiej scenie politycznej miały bardzo dynamiczny przebieg. Istniało ryzyko, że Polska pozostanie w szarej strefie i tzw. próżni bezpieczeństwa, dlatego jednym z celów strategicznych w latach 90. XX w. było przystąpienie naszego państwa do NATO. Doktor Zielke przybliżył koncepcje rozszerzenia Sojuszu i stanowiska w tej kwestii zarówno polskich, jak i zagranicznych polityków, m.in. sekretarza generalnego NATO Manfreda Wörnera, który w 1992 r. stwierdził, że drzwi do NATO są otwarte. Polska zdecydowała się skorzystać z tego nieformalnego zaproszenia. Jej staraniom sprzyjała dodatkowo transformacja polityki wschodniej Sojuszu i stworzenie programu „Partnerstwo dla Pokoju" (10 stycznia 1994 r.), który był odpowiedzią na dążenie państw Europy Środkowo-Wschodniej do członkostwa. Wprawdzie uczestnictwo w tym programie nie dawało formalnych przesłanek do przyjęcia w struktury NATO, ale – jak pokazuje przykład Polski, Czech i Węgier – znacznie ułatwiało dalsze starania. Polska miała, poza głosami orędowników na jej rzecz, silne karty przetargowe. Utorowała drogę do wolności innym narodom, była ustabilizowaną demokracją, miała za sobą udaną realizację programu gospodarczego, prowadziła rozsądną politykę zagraniczną. Doktor Zielke opisał kolejne etapy prowadzące do akcesji Rzeczpospolitej do NATO. Jednym z nich było spotkanie prezydentów Billa Clintona, Lecha Wałęsy i Václava Havla w Pradze (1994 r.), po którym rozpoczęto prace koncepcyjne nad rozszerzeniem Sojuszu. Prezydent Clinton złożył wtedy deklarację, że rozszerzenie NATO nie jest kwestią „czy?", ale „kiedy?" i „jak?". Istotną rolę w tym procesie odegrali ambasador Stanów Zjednoczonych w Polsce Daniel Fried i ambasador Stanów Zjednoczonych przy ONZ Richard Holbrook. Warunkami wstąpienia Polski do Sojuszu było rozwiązanie wewnętrznych problemów: lustracji i wyroku ciążącego na Kuklińskim. Prelegent zwrócił uwagę, że oczekiwanie Polski na przyjęcie do Sojuszu, wbrew pozorom, nie trwało długo. W 1996 r. prezydent Clinton ogłosił, że w następnym roku kolejne kraje zostaną zaproszone do rozmów akcesyjnych. Warto podkreślić, że Rosjanie do końca próbowali osłabić wojskowe i polityczne skutki rozszerzenia. Z tego wynikały ich żądania dotyczące infrastruktury, stacjonowania wojsk sojuszniczych, a także wstrzymania dalszego powiększania Sojuszu, zwłaszcza o państwa bałtyckie. Po wstąpieniu do NATO Polska podjęła starania o przyjęcie do Unii Europejskiej, a w kolejnych latach podobnie postąpiły inne państwa Europy Środkowo-Wschodniej. Doktor Zielke przedstawił też historyczne i polityczne uwarunkowania operacji „Allied Force" (1999 r.) w Jugosławii, która rozpoczęła nowy rozdział w historii

Sojuszu. Podczas tej interwencji odbył się – już z udziałem Polski – szczyt NATO w Waszyngtonie (23–25 kwietnia 1999 r.). Przyjęto na nim wiele ważnych deklaracji, m.in. *Oświadczenie w sprawie Kosowa*, w którym potępiono działania prezydenta Słobodana Miloševicia i wezwano go do zakończenia represji. Prelegent zwrócił uwagę na istotną rolę Rumunii w trakcie konfliktu w Kosowie, która udostępniła swoją przestrzeń powietrzną dla samolotów NATO i od tego momentu popierała natowskie i amerykańskie inicjatywy militarne na świecie. Do politycznych sukcesów na przełomie wieków dr Zielke zaliczył m.in. utworzenie wschodniej flanki Sojuszu, wejście kolejnych krajów w jego struktury, a także awans Polski z trzeciego do pierwszego świata. Jednocześnie wskazał, że kryzysy, które wpłynęły na sytuację w Europie, zaczęły się w kwietniu 2008 r., kiedy wstrzymano rozszerzenia Sojuszu.

Trzecim prelegentem był płk dr Marek Świerczek z ABW, który zaprezentował referat pt. *Zmiana roli i zadań polskich służb specjalnych po 1990 r. Utworzenie kierunku wschodniego UOP*. Celem wystąpienia było zwrócenie uwagi na trudności i wyzwania, jakie stały przed służbami specjalnymi tworzonymi po zmianach ustrojowych, w tym na trudną sytuację kontrwywiadowczą III RP. Zaczął od problemów, z jakimi borykała się Służba Bezpieczeństwa pod koniec swojego istnienia, takich jak: całkowity zanik ideologii, wakaty, upadek autorytetu kadry kierowniczej, masowe odejścia funkcjonariuszy, szczególnie z pionu techniki MSW. Następnie przedstawił działania Centralnej Komisji Kwalifikacyjnej oraz Komisji Kwalifikacyjnej do Spraw Kadr Centralnych i wojewódzkich komisji kwalifikacyjnych powołanych *Uchwałą nr 69 Rady Ministrów z dnia 21 maja 1990 r. w sprawie trybu i warunków przyjmowania byłych funkcjonariuszy Służby Bezpieczeństwa do służby w Urzędzie Ochrony Państwa i w innych jednostkach organizacyjnych podległych Ministrowi Spraw Wewnętrznych oraz zatrudniania ich w Ministerstwie Spraw Wewnętrznych*. Komisje te miały przeprowadzić postępowania kwalifikacyjne byłych funkcjonariuszy SB przyjmowanych do służby w Urzędzie Ochrony Państwa. Podkreślił, że kroki podjęte przez te komisje nie przyczyniły się do rozwiązania problemów. Rezygnacja z „opcji zero" na rzecz weryfikacji spowodowała, że lustracja była procesem iluzorycznym. W nowo utworzonej służbie 95% funkcjonariuszy wywodziło się z SB. Niskie pensje i niedofinansowanie jednostki nie przyciągały kandydatów, co sprawiło, że 1/3 etatów pozostała nieobsadzona. Doktor Świerczek zwrócił uwagę, że najistotniejszą kwestią było w tamtym czasie przeorientowanie działań kontrwywiadowczych. Od lat 70. XX w. Rosjanie postrzegali PRL jako istotny czynnik ryzyka strategicznego ze względu na polityczną niestabilność państwa, które było jednocześnie zwornikiem systemu satelickiego. Dlatego zdecydowali się na systematyczne zwiększanie liczby nielegałów, a rozbudowa ich siatki szpiegowskiej nakładała się na kolejne kryzysy w Polsce (w latach 1970, 1976, 1980, 1988–1990). Nowa służba miała być odpowiedzią na główne zagrożenia tamtego okresu. Wydział Wschodni

Zarządu Kontrwywiadu UOP czekała trudna droga do osiągnięcia pełnej zdolności operacyjnej, ponieważ od zakończenia II wojny światowej nie prowadzono w Polsce działań rozpoznawczych wobec wywiadu radzieckiego i brakowało kadry doświadczonej w tym zakresie. Urząd Ochrony Państwa był służbą o charakterze operacyjno-rozpoznawczym, a nie administracyjnym, która przez kolejne lata tworzyła coraz większą sieć naprowadzeń kontrwywiadowczych. Zagrożenie ze strony FR było priorytetowym zagadnieniem, dlatego kontrolą operacyjną objęto wszystkie elementy o wysokim poziomie ryzyka kontrwywiadowczego. Zapewnienie osłony kontrwywiadowczej kraju przez UOP również miało wpływ na ostateczną decyzję NATO w sprawie włączenia Polski do swoich struktur, co prelegent podkreślił na zakończenie wystąpienia.

Kolejny referat pt. *Od teorii do praktyki współczesnej. Kwatera Główna NATO w Brukseli po 24 lutego 2022 r.* wygłosił kpt. Krystian Szymański z ABW. Rozpoczął od spraw związanych z nazewnictwem i symboliką, a na dalszych slajdach pokazał budynek Kwatery Głównej NATO i jego otoczenie z kilkoma pomnikami, takimi jak replika muru berlińskiego, fragment 107 piętra World Trade Center czy logo NSZZ „Solidarność". Następnie omówił artykuły 4 i 5 traktatu północnoatlantyckiego i przedstawił strukturę organizacyjną Sojuszu. Szymański opisał, jak rozszerzały się wpływy NATO w Europie, wskazując na istotę wojskowej obecności zarówno NATO, jak i USA na obszarze Rzeczpospolitej. Podkreślił fakt, że Polska jest obecnie liderem na wschodniej flance Sojuszu i pełni funkcję frontową, a wydatki naszego państwa na armię wzrosły do niemal 4% PKB. Po 24 lutego 2022 r. Zachód musiał zmienić swoje podejście i przekierować uwagę w kwestiach bezpieczeństwa, przynajmniej częściowo, z Chin na Europę. W tym kontekście fundamentalne znaczenie ma przyjęcie w ostatnim czasie Finlandii i Szwecji do Sojuszu i rozciągnięcie w ten sposób północnej flanki. Prelegent zwrócił uwagę, że świat jest obecnie wielobiegunowy, a nie jak w czasach zimnej wojny – dwubiegunowy. NATO musi więc się dozbrajać, poszerzać swoje wpływy i pozostawać przeciwwagą dla Rosji. Na politykę Sojuszu ma wpływ zarówno zmieniająca się sytuacja na Dalekim Wschodzie, gdzie Chiny budują potęgę gospodarczą i militarną, jak i rozszerzenie BRICS[3] o nowe państwa. Jedno z ostatnich zagadnień zasygnalizowanych przez kpt. Szymańskiego dotyczyło nowych zagrożeń bezpieczeństwa cybernetycznego i kosmicznego, których wystąpienie może prowadzić w ostateczności do uruchomienia

[3] BRICS – akronim od anglojęzycznych nazw państw: Brazylii, Rosji, Indii, Chin i Republiki Południowej Afryki (Brazil, Russia, India, China, South Africa), które zrzeszyły się w 2009 r. w ramach współpracy polityczno-gospodarczej (RPA dołączyła w 2011 r.). Od 2024 r. członkami BRICS są także Egipt, Etiopia, Iran i Zjednoczone Emiraty Arabskie (przyp. red.).

art. 5 traktatu. Na zakończenie prelegent poruszył kwestie związane z obsadą kadrową w Kwaterze Głównej NATO.

Zdjęcie 3. Seminarium towarzyszyła wystawa dotycząca powstania i misji NATO oraz obecności Polski w Sojuszu Północnoatlantyckim.

Źródło: materiały własne.

Podczas ostatniego wystąpienia Filip Frąckowiak w referacie pt. *Generał Ryszard Kukliński – pierwszy polski oficer w NATO* zaprezentował biografię człowieka, który miał realny wpływ na historię świata. Dzięki Kuklińskiemu Amerykanie poznali strategiczne plany ofensywy Związku Sowieckiego na zachód Europy z wykorzystaniem państw Układu Warszawskiego. W czasie 11 lat współpracy Kukliński dostarczył ok. 40 000 stron dokumentów, z których większość wciąż pozostaje tajna. Były wśród nich m.in. plany strategiczne na wypadek wybuchu III wojny światowej, rozmieszczenie radzieckich sił w krajach Układu Warszawskiego, techniczne dane uzbrojenia, plan wprowadzenia w Polsce stanu wojennego. Frąckowiak nakreślił sytuację geopolityczną w czasach działalności Jacka Stronga (pseudonim nadany Kuklińskiemu przez Amerykanów) i na jej tle przedstawił jego sylwetkę. Pomogło to zebranym zrozumieć motywy, dla których Kukliński zdecydował się postawić na szali życie swoje i rodziny oraz dobrze rokującą karierę. Kiedy rozpoczynał współpracę z obcym wywiadem – choć początkowo sądził, że ze swoimi odpowiednikami w amerykańskiej armii – był postrzegany jako utalentowany oficer młodego pokolenia. W tamtym okresie pełnił funkcję szefa Oddziału Planowania Obronno-

-Strategicznego w Sztabie Generalnym Ludowego Wojska Polskiego. Był także oficerem łącznikowym między Sztabem a dowództwem Układu Warszawskiego, dzięki czemu miał pełną wiedzę o sowieckich planach. Prelegent opisał, jak wyglądało nawiązanie współpracy z CIA i jak ona przebiegała aż do momentu ewakuacji, która nastąpiła przed ogłoszeniem stanu wojennego w Polsce. Przedstawił też tragiczne losy rodziny Kuklińskiego po przyjeździe do Stanów Zjednoczonych. Ten oficer WP był dla CIA najważniejszym źródłem informacji w czasie zimnej wojny. Frąckowiak kilkakrotnie podkreślał patriotyczne pobudki doświadczonego wojskowego, który doskonale zdawał sobie sprawę z tego, co dzieje się z państwem „w kleszczach mocarstw". Po 1989 r. Kukliński lobbował na rzecz przyjęcia Polski do NATO. Zatarcie wyroku sądu PRL, skazującego go na karę śmierci zamienioną w 1990 r. na karę 25 lat pozbawienia wolności, było jednym z warunków akcesji postawionym przez Amerykanów. Profesor Zbigniew Brzeziński nazwał Kuklińskiego pierwszym polskim oficerem w NATO. Określenie to stało się mottem przewodnim wystąpienia dyrektora Muzeum Zimnej Wojny, który zabrał uczestników spotkania na wirtualny spacer po placówce, zaprezentował zbiory i zaprosił do jej odwiedzenia.

Po wygłoszeniu wszystkich referatów rozpoczęła się dyskusja, w trakcie której uczestnicy mieli możliwość zadania pytań prelegentom oraz podzielenia się swoimi spostrzeżeniami. Wydarzeniu towarzyszyła okolicznościowa wystawa poświęcona omawianej problematyce.

Seminarium wpisało się w cykl spotkań i publikacji związanych z jubileuszem. Przedstawione referaty pozwoliły na nowo spojrzeć na wyzwania, przed jakimi stanęła Polska, podejmując starania o akcesję do Sojuszu, i na rolę, jaką w tym procesie odegrał Ryszard Kukliński. Uwidoczniły, jak trudna i skomplikowana to była droga. Obecnie członkostwo naszego kraju w NATO to nie tylko gwarancja bezpieczeństwa, lecz także wiele zobowiązań. To międzynarodowa solidarność i troska o wspólne bezpieczeństwo.

Dr Iwona Osłowska

Kontakt: i.oslowska@wp.pl

Debata „Rola służb specjalnych we współczesnej Polsce”

Wydział Nauk Politycznych i Stosunków Międzynarodowych
Uniwersytetu Warszawskiego, 26 stycznia 2024 r.

LESZEK WOJCIESZAK

Agencja Bezpieczeństwa Wewnętrznego
https://orcid.org/0009-0003-7080-6069

Przegląd Bezpieczeństwa Wewnętrznego, 2024, nr 30: 251–263

https://doi.org/10.4467/20801335PBW.24.011.19613

VARIA

Polskie służby specjalne w XXI w. Jakie są ich zadania w dobie dynamicznych zmian geopolitycznych, społecznych i technologicznych zachodzących we współczesnym świecie? Z jakimi problemami i wyzwaniami się mierzą? Jakie działania należałoby podjąć, aby usprawnić ich funkcjonowanie? Tym zagadnieniom została poświęcona debata ekspercka, która odbyła się 26 stycznia 2024 r. na Wydziale Nauk Politycznych i Stosunków Międzynarodowych Uniwersytetu Warszawskiego. W dyskusji moderowanej przez prof. Aleksandrę Gasztold z Katedry Bezpieczeństwa Wewnętrznego UW wzięli udział: gen. Krzysztof Bondaryk – szef Agencji Bezpieczeństwa Wewnętrznego w latach 2008–2013, prof. Zbigniew Siemiątkowski – szef Agencji Wywiadu w latach 2002–2004, adiunkt w Katedrze Bezpieczeństwa Wewnętrznego UW, płk Grzegorz Małecki – szef Agencji Wywiadu w latach 2015–2016, prof. Andrzej Zybertowicz – doradca Prezydenta RP oraz dr Arkadiusz Nyzio – adiunkt w Katedrze Bezpieczeństwa Narodowego UJ.

Aktualne priorytety polskich służb specjalnych

Tematem przewodnim debaty były priorytety polskich służb specjalnych na 2024 r. Jednym z nich, zdaniem prof. Zybertowicza, powinno być monitorowanie rozwoju nowych technologii, takich jak sztuczna inteligencja czy biologia syntetyczna, które mogą skokowo zmienić układ sił i zostać wykorzystane w szkodliwych celach. Według niego (…) *rewolucja cyfrowa przyniosła ze sobą głęboką penetrację technologiczną tkanek społecznych,* (…) *łącznie do warstw podświadomości w wyobraźni zbiorowej*. Problemem jest to, że Polska, podobnie jak większość państw, nie ma instrumentów służących do precyzyjnego monitorowania sterowanych przez algorytmy strumieni bodźców badających kondycję społeczną i subtelnie manipulujących zachowaniami społecznymi. To jest bardzo ważne zadanie. Aby polskie służby mogły je skutecznie realizować, muszą, zdaniem prof. Zybertowicza, zostać znacznie lepiej dofinansowane.

W opinii prof. Siemiątkowskiego priorytetem służb, nie tylko w Polsce, jest obecnie odtworzenie zasobów i aktywów na kierunku wschodnim. Do 1990 r., czyli do roku, kiedy istniał podział na dwa bloki ideologiczne, polityczne i militarne, sytuacja była prosta. Po zmianie układu sił wiele służb miało problem z odpowiedzią na pytanie, jaka jest ich rola. W odniesieniu do bloku wschodniego zaczęła obowiązywać koncepcja końca historii. Wspólnoty służb wywiadowczych trudno było przekonać do istnienia w historii Rosji „teorii zbierania ziem ruskich" czy „smuty" i do tego, że prędzej czy później nacjonalizm i szowinizm wielkoruski dojdą w tym kraju do głosu. Zdaniem prof. Siemiątkowskiego stale aktualnym problemem służb na świecie pozostaje ich akcyjność. W sytuacji zaistnienia przełomowych wydarzeń, np. takich jak zamach z 11 września 2001 r., przerzucają one całą swoją aktywność na powstałe zagrożenie. Należy z tym skończyć i podjąć systematyczne, długofalowe działania oraz w prawidłowy sposób zdefiniować skalę i mapę zagrożeń we współczesnym świecie, w tym w Polsce.

Do tego postulatu przychylił się płk Małecki, który stwierdził, że właściwe zidentyfikowanie zagrożeń to klucz do sukcesu służb specjalnych. W jego opinii aktualna prognoza dotycząca zagrożeń uznawanych za najbardziej istotne powinna być

jedna i powstawać w najważniejszym miejscu, jakim jest Kancelaria Prezesa Rady Ministrów. Dopiero na tej podstawie powinny być przydzielane priorytetowe zadania dla poszczególnych służb. W praktyce bowiem każda z nich przedstawia mapę zagrożeń tworzoną z własnej perspektywy, co czasami prowadzi do powstawania obszarów niepokrytych zadaniami. Służbom nierzadko umyka potrzeba rozpoznawania zjawisk nie tylko w ujęciu defensywnym, lecz także w kontekście szans, których identyfikacja pozwoliłaby lepiej wykorzystać możliwości rozwojowe, chociażby gospodarcze, oraz efektywniej budować pozycję państwa. Najważniejsze jest oczywiście rozpoznawanie celów i działań Rosji, ale należy też oceniać rozwój sytuacji w Ukrainie, również w perspektywie poprawy sytuacji polityczno-gospodarczej Polski po zakończeniu wojny. Nie wolno jednocześnie zapominać o monitorowaniu Bliskiego Wschodu pod kątem zjawisk mogących negatywnie oddziaływać na sytuację w Unii Europejskiej, np. nielegalnej imigracji czy zmiany zagrożeń terrorystycznych. Bezpieczeństwo Polski wymaga ponadto śledzenia tzw. wielkiej gry mocarstw i jej negatywnego wpływu na nasz kraj, gdyż pole rywalizacji pomiędzy głównymi graczami (Chinami, Rosją) może momentami przenosić się na terytorium RP.

Wysuwane przez przedmówców sugestie na temat kierunku wschodniego i sztucznej inteligencji poparł dr Nyzio. Postulował jednocześnie zwiększenie aktywności polskich służb w zakresie zagrożeń wewnętrznych, polegającej na monitorowaniu i operacyjnym zwalczaniu organizacji, stowarzyszeń, grup, jednostek prowadzących działalność o charakterze skrajnym, wywrotowym, radykalnym, ekstremistycznym. W Europie aktywność nazywaną *foreign influence* (pol. obce wpływy) odnotowano ostatnio w Niemczech, a Federalny Urząd Ochrony Konstytucji przyznał, że był niewystarczająco czujny w tej kwestii. Zdaniem dr. Nyzia służby powinny również mieć pogłębione rozpoznanie zjawisk określanych jako *democratic sliding* (pol. zanikanie demokracji), gdyż (…) *po prostu zjeżdżamy w dół, jeśli chodzi o standardy demokratyczne, i trzeba bardzo intensywnie monitorować wszystkie grupy, które na tym odcinku działają i do tego zjawiska się przyczyniają*. Drugim zgłoszonym postulatem była transparentność. Komunikację społeczną prowadzoną przez polskie służby ocenił on jako zdecydowanie niewystarczającą, jednostronną. Brakuje konferencji prasowych, dialogu ze społeczeństwem. Jako przykład odmiennego podejścia dr Nyzio wskazał wystąpienia publiczne szefa MI5, porównując je z medialną absencją szefa polskiego odpowiednika Security Service. Jego zdaniem służby specjalne powinny zacząć aktywniej działać w tym obszarze – wyjaśniać, czym się zajmują, dlaczego podejmują takie, a nie inne działania, edukować na temat zagrożeń.

Zgłoszone podczas debaty oczekiwania wobec polskich służb specjalnych gen. Bondaryk określił jako oderwane od ich stanu. To spojrzenie na służby przez pryzmat oczekiwań społecznych, a nie oczekiwań ich nadzorców politycznych. Jego zdaniem służby są przede wszystkim urzędami centralnymi czy też biurokracjami

specjalnymi posługującymi się kodeksem postępowania administracyjnego, więc jest w nich dużo transparentności. Przyznał jednak rację przedmówcy, że nie dotyczy to komunikacji społecznej. Kiedyś służby specjalne miały rzeczników prasowych, organizowały konferencje prasowe i zamieszczały informacje na stronach internetowych. Potem nastąpił regres. Były szef ABW stwierdził, że służby te ogólnie zostały zdewastowane. Zaszkodzono im czystkami kadrowymi, przeglądami genealogicznymi, usuwaniem z szeregów profesjonalistów. Z tego względu trudno się spodziewać, aby mogły one spełniać oczekiwania, o których mówiono podczas debaty. Jak stwierdził, (…) *mając charakter bardziej fasadowy niż realny, służby milczą. Wiedzą, co robią*. Wszystkie kraje, zarówno te demokratyczne, jak i autorytarne, mają służby. W państwach demokratycznych są one atrybutem demokracji, niepodległości, bezpieczeństwa państwowego i publicznego. Problemem w tych państwach jest określenie granic transparentności, sprawczości czy uprawnień służb. Te dylematy wymagają rozstrzygnięć konstytucyjno-ustawowych. W Polsce nastąpił podział służb, zarówno tych cywilnych, jak i wojskowych. Zdaniem gen. Bondaryka to rozproszenie daje siłę, gdyż najważniejsza jest specjalizacja.

Blaski i cienie reformy instytucji wywiadowczych i kontrwywiadowczych. Postulaty zmian

Kolejnym punktem dyskusji było spojrzenie na ostatnie dwie dekady funkcjonowania służb i pytanie o to, jakie błędy popełniono podczas reformowania instytucji wywiadowczych i kontrwywiadowczych, oraz o konieczne zmiany.

Według prof. Siemiątkowskiego raczej nie popełniono błędu przy reformie z lat 2001–2002, tylko zabrakło czasu na jej dokończenie, m.in. z powodu kalendarza wyborczego. Stwierdził on, że w Polsce istnieją tylko cztery służby specjalne, gdyż nie wszystkie te, które mają uprawnienia operacyjno-rozpoznawcze, są tak naprawdę służbami specjalnymi. Tę kwestię należałoby, jego zdaniem, uporządkować. Określenie „specjalne" powinno być zarezerwowane dla służb wykonujących zadania wywiadowcze i kontrwywiadowcze, dzielone na cywilne i wojskowe. Zgodnie z tym kryterium w Polsce jest ich właśnie cztery. Należałoby także dokładnie przyjrzeć się zakresowi kompetencji ABW. Według projektu ustawy miała to być przede wszystkim służba kontrwywiadowcza, zajmująca się również ochroną informacji niejawnych. Pod wpływem ówczesnej argumentacji, że (…) *jeżeli ABW zostanie pozbawiona atrybutu śledczego, to będzie to pies, którego szczekania nikt nie będzie się obawiał*, Agencji pozostawiono uprawnienia dochodzeniowo-śledcze. Zdaniem prof. Siemiątkowskiego proporcja potencjału organizacyjnego i kadrowego ABW

przeznaczonego do prowadzenia działalności kontrszpiegowskiej w stosunku do potencjału przeznaczanego na realizację innych zadań jest mocno zachwiana.

Innym pomysłem z czasów reformy było stworzenie narodowego wywiadu, który jednoczyłby wywiady wojskowy i cywilny. Stało się jednak tak, że w Polsce istnieją dwie służby wojskowe, które działają zgodnie z ustawą będącą lustrzanym odbiciem ustawy o ABW oraz AW. Polska, o czym prof. Siemiątkowski przypomniał, jako jeden z nielicznych krajów nie ma czwartego ogniwa cyklu wywiadowczego. Brakuje miejsca, w którym powstawałaby ujednolicona informacja wywiadowcza dla jej dysponentów i formułowano by na bieżąco, cyklicznie perspektywiczne zadania dla służb specjalnych. Służby bowiem (…) *są od analizy, od zbierania informacji, a nie od ścigania się na newsy i dostarczania haków*. Profesor zwrócił uwagę także na relacje służb wywiadowczych i kontrwywiadowczych z użytkownikami. Zauważył, że bardzo duże kompetencje w sprawach służb ma premier, ale brakuje mu czasu na te zadania. Więcej ma go prezydent, ale nie ma kompetencji. Remedium mógłby być sprawdzony, jego zdaniem, patent amerykański. Tam w Radzie Bezpieczeństwa Narodowego jest usytuowana komórka – Narodowa Rada ds. Wywiadu kierowana przez dyrektora Narodowego Wywiadu, gdzie przedstawiciele wszystkich wspólnot wywiadowczych Stanów Zjednoczonych spotykają się z administracją. W Polsce musimy budować system, w którym za służby specjalne byłyby odpowiedzialne różne ogniwa władzy wykonawczej i ustawodawczej, z rotacyjnym szefem komisji do spraw służb specjalnych, aby opozycja co sześć miesięcy miała wpływ na to, co dzieje się w służbach.

Zdjęcie 1. Spotkanie dotyczące służb specjalnych było drugim z cyklu debat organizowanych przez Katedrę Bezpieczeństwa Wewnętrznego WNPiSM UW. Jego uczestnicy dyskutowali m.in. o stanie polskich służb i systemie kontroli nad nimi oraz o potrzebnych zmianach w tym zakresie.

Źródło: materiały własne.

Z większością tez prof. Siemiątkowskiego zgodził się płk Małecki, według którego (…) *problem polega na tym, że zostaliśmy z tymi służbami właśnie w tym 2002 r*. Są one w tej chwili (…) *skoncentrowane nie na rozwoju, nie na poszukiwaniu impulsów rozwojowych, nowych obszarów, nowych mediów, nowych form, tylko na kultywowaniu tradycji modelu utworzonego w 2002 r*. Przyznał, że nadal brakuje ogniwa, które scalałoby te cztery formacje specjalne, i ogniwa planistyczno-koordynująco-nadzorczego, w którym ulokowany byłby m.in. czwarty element cyklu wywiadowczego. Efektywna koordynacja działalności tych służb to najważniejszy brak. Koordynacja nie jest jednak tożsama z nadzorem, a większość polityków uważa, że główne zadanie polityki wobec służb to tworzenie aparatu nadzoru, de facto prowadzącego do paraliżu ich działalności. Są one pozbawiane autorytetu, traktowane instrumentalnie, a rezultaty ich pracy – niedoceniane. Służby muszą korzystać z zaufania społecznego, dlatego konieczne jest stworzenie skutecznego systemu realnej kontroli demokratycznej nad nimi, systemu wielopoziomowego i komplementarnego, badającego efektywność służb i ich przydatność w kontekście wyzwań współczesności.

Wątek nadzoru kontynuował gen. Bondaryk, mówiąc o systemie kontroli sądowej w kwestii kontroli operacyjnej. Uznał, że ten system ma wymiar formalny i korespondencyjny, a nie faktyczny. Argumentując, opisał „przeładowanie" sądów okręgowych wnioskami (ok. 20–30 dziennie). Dyżurny sędzia w kancelarii tajnej albo wyraża zgodę i zarządza kontrolę operacyjną, albo się nie zgadza i pisze uzasadnienie, a to wymaga czasu. Nie zawsze jest go wystarczająco dużo. W związku z tym należy wprowadzić system realnej kontroli sądowej. Większość problemów dotyczy nie pracy śledczej, gdyż ona jest bardziej transparentna, lecz pracy operacyjnej. Zdaniem gen. Bondaryka procedury operacyjne nie są weryfikowane. Regulujące je instrukcje wewnętrzne nie stanowią powszechnie obowiązującego prawa. To prowadzi do pytania: co to są czynności operacyjno-rozpoznawcze? Ich definicji nie ma bowiem w żadnej ustawie, a czynności te (ich liczba jest podobna) znajdują się w uprawnieniach poszczególnych służb. Jego postulatem jest stworzenie jawnej, dostępnej dla wszystkich ustawy o pracy operacyjnej, definiującej sferę, która tak mocno ingeruje w prawa i wolności obywatelskie. Skoro naczelną zasadą jest praworządność, to brak takiego aktu prawnego oznacza jednocześnie brak odpowiedzi na nieprawidłowości. Spuentował stwierdzeniem: (…) *odpowiedź instytucjonalna, że powstanie specjalny urząd, który będzie strzegł praworządności, to jest żadna odpowiedź, to jest złudzenie*.

Doktor Nyzio, odnosząc się do zagadnienia kontroli operacyjnej, dopełnił je statystyką z badań prowadzonych w Katedrze Bezpieczeństwa Narodowego UJ. Zgodnie z wynikami z 2022 r. za 80% takich kontroli odpowiadała Policja. *Zwykliśmy mówić o służbach specjalnych właśnie à propos czynności operacyjno-*

-rozpoznawczych, a one w ogóle nie są wyznacznikiem tego rodzaju instytucji. Tym, co odróżnia służby specjalne, które powinniśmy nazywać wywiadowczymi, od innych instytucji bezpieczeństwa, jest realizowanie przez nie czynności analityczno-informacyjnych, czyli wyposażanie naszych decydentów politycznych w wartościową wiedzę na temat tego, co się dzieje – stwierdził. Służby wywiadowcze to instrument optymalizacji procesu decyzyjnego w państwie, a praca operacyjna ma służyć realizacji tego celu. Dlatego często polemizuje on z twierdzeniem o apolityczności służb. Jego zdaniem służby są instrumentem polityki, ale powinny być apartyjne, czyli (…) *nie mają służyć interesom partii rządzącej, tylko interesom bezprzymiotnikowego państwa*. Ustosunkowując się do kwestii kontroli i wypowiedzi płk. Małeckiego, dr Nyzio wyraził większą wiarę w sądy niż w „zewnętrzne ciała" mające uzdrowić wszystko. Warunkiem koniecznym jest właściwe wymodelowanie odpowiednich komórek w sądach. Godnym rozważenia pomysłem byłaby rozproszona kontrola sądowa realizowana z udziałem przeszkolonych sędziów. Doktor Nyzio zaznaczył przy okazji, że w Polsce mówi się o funkcji ministra koordynatora, a tak naprawdę mamy ministra bez teki, który podejmuje działania w imieniu premiera, na podstawie imiennych aktów wykonawczych. Na zakończenie przyznał, że (...) *brakuje nam takiego serca, jeśli chodzi o koordynację przedsięwzięć z zakresu służb specjalnych, a także jeśli chodzi o współdziałanie pomiędzy służbami specjalnymi a innymi ogniwami systemu bezpieczeństwa*.

Pytania i dyskusja

Kolejna część debaty została przeznaczona na pytania z sali i dyskusję. Pierwsze z nich dotyczyło oceny wpływu pracowników byłych tajnych służb oraz ich współpracowników na dzisiejsze życie społeczno-polityczno-kulturalne w Polsce. W odpowiedzi prof. Zybertowicz stwierdził, że obecnie o wiele większą niż tajne służby wiedzę o pojedynczym człowieku i społeczeństwie mają giganci technologiczni, a bardziej znaczący jest wpływ potężnych biznesmenów, ludzi mediów niż pozostałości systemu postesbeckiego.

Z pytaniem na temat potrzeby stworzenia w Polsce kolejnej służby na wzór brytyjskiej Government Communications Headquarters (GCHQ) zmierzył się dr Nyzio. W jego ocenie powołanie samodzielnej instytucji zajmującej się rozpoznaniem elektromagnetycznym i mającej charakter integrujący byłoby pożądane. Należałoby tylko zadbać o to, by powstanie polskiej służby będącej odpowiednikiem GCHQ czy amerykańskiej National Security Agency nie spowodowało nałożenia się właściwości, czyli zadań, jak to się stało w przypadku CBA, które zdublowało pewne kwestie mieszczące się w zakresie zainteresowań ABW.

Kolejne zagadnienie dotyczyło zmian w szkoleniu kadr służb specjalnych. Okazało się ono bliskie płk. Małeckiemu, który jest zaangażowany w projekt na ten temat realizowany na UJ. Przedstawił on pomysł tzw. kuźni kadr. To rozwiązanie, istniejące już w innych państwach, miałoby polegać na stworzeniu katedry czy akademii wywiadowczej, która byłaby swoistym hubem – miejscem styku służb specjalnych, świata nauki i polityki, a także biznesu, zwłaszcza tego strategicznego. Jego celem byłoby wzajemne poznawanie potrzeb i opinii, inspirowanie wspólnych badań adekwatnych do realnych potrzeb, m.in. służb, prowadzenie debat i wypracowywanie optymalnych rozwiązań dla państwa. Ta współpraca odbywałaby się w warunkach w pełni bezpiecznych, dających gwarancję zachowania dyskrecji i konspiracji. Akademia mogłaby stanowić przestrzeń do organizowania specjalistycznych szkoleń oferowanych zarówno przez nią, jak i niektóre think tanki. W ofercie kuźni kadr byłyby ponadto kursy podstawowe dla wszystkich adeptów służb specjalnych w celu unifikacji bazy pojęciowej i metodologicznej oraz stworzenia systemu uwspólnionych wartości, ułatwiającego dialog pomiędzy służbami. Wartością dodaną byłaby wymiana kadr, gdyż w pewnym stopniu są one potencjałem całego systemu wywiadowczego i w interesie państwa jest jego efektywne wykorzystanie. Pułkownik Małecki zaznaczył, że nie oznacza to braku konieczności rozwijania przez każdą ze służb swoich ośrodków i systemów szkoleniowych, uwzględniających specyfikę potrzeb danej formacji. Taka instytucja pod auspicjami ministra koordynatora byłaby miejscem, gdzie dochodziłoby do styku impulsów rozwojowych ze strony centrum zarządzania bezpieczeństwem państwa. Proponowane w niej modele szkolenia muszą uwzględniać współczesne możliwości, narzędzia, formy i być otwarte na najnowsze trendy. Jego zdaniem systemy szkoleniowe polskich służb są anachroniczne, stanowiąc nierzadko kontynuację modelu wypracowanego jeszcze w latach 70. i 80. XX w.

Taka wizja kuźni kadr nie spotkała się z aprobatą prof. Siemiątkowskiego, który w pomyśle przedmówcy doszukiwał się analogii do Instytutu im. Andropowa w Moskwie. Wątpił, czy w sytuacji, kiedy na wielu uczelniach w Polsce powstają kierunki związane z bezpieczeństwem, a osób na nich się kształcących są tysiące, jest to najbardziej potrzebne. Istotą rzeczy jest – jego zdaniem – ekskluzywność i elitarność służb specjalnych, a przez to ich efektywność. Ekskluzywność kryje w sobie ograniczony dostęp do wiedzy wytworzonej przez służby, przeznaczonej tylko dla nielicznych. Elitarność natomiast to zaszczyt znalezienia się w szeregach służby. Na realną wymierność tych znaczeń służby muszą sobie jednak zasłużyć i dopiero wtedy będą w stanie przyciągać najlepszych. Należy przyjąć założenie, że służby państwowe nigdy nie wygrają z rekrutacją wielkich korporacji, ponieważ nie są w stanie zaoferować porównywalnych wynagrodzeń. Za to mogą dać kandydatowi poczucie satysfakcji, że (…) *będzie robił rzeczy, o których inni mogą tylko śnić,*

będzie w miejscach, które nie istnieją, będzie znał ludzi, których nie ma. Niestety jednocześnie oznacza to pogodzenie się z myślą o byciu anonimowym i z przypisywaniem zasług innym.

Do uwag prof. Siemiątkowskiego na temat kuźni kadr odniósł się płk Małecki przy okazji odpowiedzi na inne pytanie. Przekonywał, że akademia nie dubluje działań uczelni i nie ma niczego zastępować. Ma stanowić element uzupełniający system, z którym mamy dzisiaj do czynienia, i umożliwiać odpowiednią komunikację i synergię działań służb, skutkującą ich lepszą, gdyż zarządzaną systemowo, działalnością.

W kontekście szkolenia kadr padło również pytanie o ewentualny udział w nim obcokrajowców, ale z polskim obywatelstwem. Odniósł się do tego płk Małecki. Przypomniał, że cudzoziemcy z oczywistych powodów są wykorzystywani przez służby wywiadowcze. Włączenie osób mieszkających w Polsce i mających rzadkie kompetencje związane z krajami pozostającymi w zainteresowaniu polskich służb specjalnych jest perspektywicznym kierunkiem. Na potwierdzenie płk Małecki przywołał Stany Zjednoczone, które od lat rozwiązują problem współpracy z obywatelami amerykańskimi pochodzącymi z krajów „produkujących" terrorystów. Obywatele ci są niezbędni do tego, aby profesjonalnie przeciwdziałać zagrożeniom, których źródła znajdują się na terytoriach tych państw. Przypomniał o nowelizacji ustawy o służbach specjalnych w 2016 r. Dzięki niemu została wprowadzona zmiana umożliwiająca zatrudnianie w AW osób, które mają obywatelstwo polskie i jednocześnie obywatelstwo innych krajów.

Kolejny poruszony wątek dotyczył braku w przestrzeni publicznej dyskusji na temat wymogów związanych z profesjonalizmem i odpowiednim doświadczeniem przy nominacji na szefa służby oraz ewentualnej zmiany przepisów w tym zakresie. W odpowiedzi prof. Siemiątkowski zacytował słowa teoretyka wojny Carla von Clausewitza, że (…) *wojna jest zbyt skomplikowanym przedsięwzięciem, aby jej prowadzenie powierzyć generałom*. Parafrazując je, stwierdził, że (…) *służby specjalne są zbyt skomplikowanym narzędziem, które musi funkcjonować w sferze politycznej, aby kierowanie nimi powierzyć funkcjonariuszom*. Profesor bronił tej opinii, gdyż jak przypomniał, sam został szefem, nie będąc funkcjonariuszem. Na poparcie swojego zdania przywołał precedensy – cywilnego szefa CIA George'a Teneta, jego następcę Leona Panettę oraz byłego szefa BND Klausa Kinkela. Wskazał również model brytyjski, w którym funkcję kontrolera pełni ktoś pochodzący ze służb. Jego zdaniem w urzędzie centralnym szefem musi być osoba (…) *bardzo dobrze obeznana w funkcjonowaniu w świecie administracji państwa*, (…) *znająca ludzi w parlamencie, łatwo poruszająca się po korytarzach Rady Ministrów*. W przypadku cywilnego szefa służb ważne jest, jakich dobiera sobie współpracowników. Delegowanie funkcjonariusza do roli szefa wymaga przyjęcia zastrzeżenia, aby miał on

odpowiednią pozycję. Za przykład podał byłego szefa ABW gen. Bondaryka, którego „niejednowymiarowa" droga uplasowała nie tylko w gronie specjalistów z zakresu służb. „Jednowymiarowa" droga, oznaczająca wąską specjalizację, pozwala się sprawdzić na stanowisku szefa służby, ale może uczynić bezradnym w kontaktach z ministrami i politykami. Reasumując, prof. Siemiątkowski stwierdził, że istnieją różne modele i w zależności od kontekstu sytuacji trzeba to wykorzystywać.

Generał Bondaryk jako przykład szefa wywodzącego się „jednolicie" ze służb podał gen. Dariusza Łuczaka, który przeszedł całą ścieżkę kariery – od szeregowego funkcjonariusza w UOP do generała i szefa ABW. Jak stwierdził, profesjonalizmu i zdolności do pełnienia tej funkcji nabywa się z czasem, gdyż każda służba ma swoją właściwość. Istotą kształcenia zarówno szefa, jak i personelu i oficerów jest budowanie zdolności. Muszą oni mieć poczucie, że w służbie nabywają kompetencji, że wykonują zawód, który ich rozwija.

W swojej wypowiedzi gen. Bondaryk nawiązał ponadto do technologii, o których wspomniał prof. Zybertowicz. Uznał je za niezwykle istotne nie tylko dla przyszłości służb specjalnych i administracji w Polsce, lecz także dla niepodległości kraju. Zaznaczył, że w świecie wirtualnym jest się albo użytkownikiem, albo administratorem. Inne role nie istnieją. Użytkownikami są też państwa, tak jak Polska, która niestety nie jest administratorem systemów globalnych czy nawet części ogólnoświatowego internetu. Bardzo ważną rolę odgrywają więc kompetencje. *Naszym wyzwaniem jest nabywanie zdolności, do pewnych działań, do pewnych umiejętności indywidualnych i zbiorowych* – stwierdził. Jeżeli państwo polskie nie będzie miało kompetencji poruszania się w obecnym świecie technologicznym, których efektem będą krajowe produkty bądź rozwiązania, to nasza suwerenność i nasza niepodległość mogą być iluzoryczne i stanowić element gry wielkich producentów i dostawców.

Do kwestii bycia szefem służby specjalnej odniósł się również płk Małecki. Zwrócił uwagę na konieczność posiadania przez taką osobę autorytetu oraz doświadczenia w zarządzaniu instytucjami, ponieważ kompetencja szefowska to przede wszystkim umiejętność zarządzania procesami i organizacjami. Jeśli miałby to być szef wywodzący się ze służby, to – jego zdaniem – najlepiej gdyby to była osoba z doświadczeniem na różnych stanowiskach kierowniczych, rozwijająca swoje umiejętności na tzw. ścieżce poziomej. Jako idealny przykład przywołał wspomnianego już gen. Łuczaka.

Generał Bondaryk został zapytany o szanse na przeprocedowanie projektu kodeksu pracy operacyjnej. Były szef ABW stwierdził, że nie wie, czy wygrają dobre rozwiązania, ale ma nadzieję, że Ministerstwo Spraw Wewnętrznych i Administracji się tym zajmie i w najbliższym czasie projekt ustawy będzie oficjalnym projektem konsultowanym w resortach rządowych. Bez wątpienia ma on

ogromne znaczenie dla praworządności oraz bezpieczeństwa funkcjonariuszy, przede wszystkim służb specjalnych, wykonujących tę pracę. Według niego na pracy operacyjnej w dzisiejszej Polsce ciąży niewdzięczna przeszłość – wspomnienie lustracji, dekomunizacji, likwidacji Wojskowych Służb Informacyjnych, ujawnienia zasobów operacyjnych. Żadne służby specjalne czy policje na świecie nie ujawniają swoich aktywów operacyjnych – nieważne, z jakich epok one pochodzą – oraz zasobów, jeśli wiąże się to z korzyściami dla państwa. Szeroko rozumiana agentura jest chroniona. Zdolności służb specjalnych do zapewnienia bezpieczeństwa polegają na zaufaniu obywateli do tajnej współpracy z państwem polskim. W jego imieniu formacje te muszą oferować obywatelowi jakieś gwarancje. Permanentne łamanie tych gwarancji poprzez publikowanie newsów czy sensacji o osobowych źródłach informacji czyni takie służby niewiarygodnymi, niezdolnymi do wypełniania zadań wobec państwa.

Wypowiedź dr. Nyzia na temat obecności szefa MI5 w mediach stała się źródłem pytania odnoszącego się do jego przekonania o tym, że brytyjskie służby specjalne pokazują swojego prawdziwego szefa, co może się wiązać z dużym ryzykiem. W odpowiedzi potwierdził on, że Ken McCallum stojący na czele MI5 faktycznie bierze udział w wystąpieniach publicznych. Nawiązał przy tej okazji do wypowiedzi gen. Bondaryka i w tym kontekście powrócił do problemu transparentności. Politykę informacyjną służb nazwał ciągłą flautą przerywaną niekontrolowanymi eksplozjami. Ponownie podkreślił brak w Polsce uporządkowanej polityki w tym zakresie – takiej, która rozbrajałaby domysły i teorie spiskowe i zwiększała zaufanie do służb.

Kolejne pytanie z sali dotyczyło wypowiedzi gen. Bondaryka i podało w wątpliwość sprawczość polskich służb wobec podmiotów, które od kilkunastu lat mają olbrzymi dostęp do danych i są daleko przed nimi, co czyni naszą niezależność fantomową. Były szef ABW jako zagrożenie wskazał możliwość braku świadomości i kompetencji służb specjalnych we współczesnym świecie technologii big data. Te kompetencje należy kształtować, w większości służb specjalnych, w wymiarze interdyscyplinarnym, gdyż bez tego nie da się obecnie funkcjonować. Z drugiej strony należy jednak pamiętać, że najważniejszy jest człowiek, stanowiący najsłabsze, a zarazem najsilniejsze ogniwo, bo (…) *albo mamy kogoś w środku, jak to się mówi, i patrzy na te kremlowskie kuranty, albo nie mamy. I to jest siła wywiadu.*

Ostatnią kwestią, poruszoną przez prof. Gasztold, było finansowanie służb specjalnych. Generał Bondaryk stwierdził, że bez pieniędzy nie ma nic, gdyż nie ma mowy o właściwych wynagrodzeniach, nabywaniu sprzętu, technologii oraz umiejętności. Niestety od 30 lat podział budżetu służb jest dokonywany w ten sam sposób. Tak było zawsze i we wszystkich służbach, tylko że wojsko i policja cieszą się większą akceptacją społeczną i domniemaniem potrzeby istnienia niż służby

specjalne. Nigdy więc nie było funduszu modernizacji tych ostatnich. Pieniądze zawsze są niewystarczające, ale trzeba się liczyć z potrzebami budżetu, a służby specjalne znajdują się raczej na końcu kolejki.

Profesor Zybertowicz wyraził pogląd, że fundusz operacyjny powinien służyć do zakupu informacji, które ktoś chce ukryć przed służbami. Zdumiewające jest dla niego to, że większość tych środków przeznacza się na inwestycje. Stwierdził, że służby mają pieniądze i nie potrafią kupować informacji. Zgodził się jednak, że systemowo służby wywiadowcze powinny dostawać wielokrotnie więcej funduszy. Uzasadnił to np. potrzebą zdobycia pozycji operacyjnej w big techach poprzez podkupienie kogoś, kto będzie partnerem dla twórcy systemów sztucznej inteligencji, a także wyszkolenie go do operacji pod fałszywą flagą. Takie działania wymagają bardzo dużych nakładów, ale zyski dla bezpieczeństwa mogą być ogromne. Natomiast dr Nyzio zasygnalizował problem skali wydatków przeznaczanych w Polsce na służby specjalne w relacji do całości wydatków państwa. Wskazał, że nastąpił regres, ponieważ obecnie na AW i ABW razem stosunkowo wydaje się mniej niż kiedyś na UOP.

Powyższe poparł płk Małecki, porównując AW do bliźniaczej służby niemieckiej – BND, która w 2021 r. miała budżet dwudziestotrzykrotnie większy niż AW, mimo że jest liczniejsza tylko sześciokrotnie. Nie może to być budżet przetrwania – stwierdził. Konieczne jest wypracowanie modelu wieloletniego planowania finansowania służb specjalnych, ponieważ budowa infrastruktury wywiadowczej jest obliczona na lata. System przygotowywania takiego budżetu powinien być elastyczny i dopasowywać się do sytuacji i wyzwań, które pojawiają się ad hoc.

Profesor Siemiątkowski zauważył, że problem nie tkwi tylko w pieniądzach. Najważniejsi są ludzie, czyli HUMINT. Inna kwestia to zróżnicowanie wynagrodzeń wewnątrz każdej struktury. Przy funkcjonowaniu czterech podstawowych pionów w każdej służbie specjalnej nie powinno być tak, że oficer operacyjny zarabia tyle samo co logistyk. W jego opinii w ramach służb musi być jasny podział wynagradzania – elitarna grupa operatorów i najlepsi z najlepszych analitycy oraz ci wszyscy, którzy w jakimś sensie nie mieszczą się w tych dwóch kategoriach. Oczywiście jest to bardzo trudne do przeprowadzenia ze względu na pragmatykę służbową czy grupy zaszeregowania. Jednak konkurencyjność służb w stosunku do tych sfer, które dzisiaj stanowią ogromne wyzwanie, musi polegać na wystawianiu osób lepszych od przeciwników, czyli też lepiej opłacanych. Podsumowując, nawet fundusze i nakłady, które aktualnie są do dyspozycji, można inaczej rozdzielić. Trzeba tylko mieć pomysł, odwagę i siłę przebicia u zwierzchników, żeby to zaakceptowali. Odwagę szefowie muszą mieć również w relacjach ze swoim zespołem. W tym kontekście prof. Siemiątkowski wskazał osobę, która nie wywodzi się

ze służb i ma świadomość, że jest „kadencyjnym przechodniem”. Nie będąc uwikłana w układy koleżeńskie, będzie miała ona większe pole manewru.

Leszek Wojcieszak

Funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Kontakt: l.wojcieszak@abw.gov.pl

Dear readers!

In the 30th issue of the Internal Security Review, we are pleased to present you with some interesting articles that - for geostrategic reasons - focus on the threat to the security of the Republic of Poland from the east. Among other things, we offer an interesting analysis on the so-called Prigozhin's rebellion, which is one of the biggest mysteries of the war in Ukraine, the characteristics of the Russian Federation information activity, a description of its methods of circumventing EU financial sanctions, as well as an attempt to explain one of the most Machiavellian operation in the history of intelligence in the form of the takeover of almost the entire Crimean Security Service staff of Ukraine by the Russian internal service. The subject of external threats - indirectly - is included in the text devoted to legal aspects of the amendment of the Polish Criminal Code with regard to the crime of espionage.

It is worth recalling that the Internal Security Review is celebrating its 15th anniversary. For more than a decade, our semi-annual journal has been striving to be a platform for the exchange of ideas between the secret services community and the academic world. We are the only professional journal dealing with the activities of these service sensu largo and we have - as a periodical published by the largest secret service of the Republic of Poland - the potential to moderate the public discourse in this area, combining scientific achievements with practical experience. Indeed, the Internal Security Agency is a source of knowledge about actual threats to state security. However, without superimposing scientific theories on this data, it is difficult to draw broader conclusions and formulate forecasts. In contrast, scientific research devoid of factual basis and source knowledge takes on a speculative and academic character, detaching itself from reality. Combining these two perspectives creates complementarity and

synergy. This is why we are guided by the idea of being a hub integrating different communities interested in issues of state security and promoting knowledge in this area. We are convinced that the worst thing for secret service is to remain stuck in the old ways - to be a reactive, uncreative and stiffened by bureaucratic procedures part of the public administration. The Internal Security Review is - in our view - one of the necessary elements of the ongoing development of these services and the evolution of their operation paradigm instead of the unreflective reproduction of operational, analytical and organisational dogmas. In order to achieve such an ambitious aim, we strive to maximise the range of topics covered in our pages by inviting specialists from many fields, not just narrowly conceived security sciences. We start from the premise that issues related to the secret services ex definitione are multidisciplinary. In 15 years, we have managed to gather around the journal a group of people who try to implement new theoretical approaches in the activities of secret services, as well as to feed the academic world with the knowledge drawn from the experience of operational and analytical officers. We hope that this group will continue to expand and develop a platform to intensify interaction between secret services and expert as well as scientific communities.

We would like to thank all the people who have contributed to our journal over the years - editors-in-chief, members of the Academic Editorial Board, editorial secretaries, reviewers, authors and members of the editorial team. Without you, your work and enormous commitment, there would not be the Internal Security Review. You were the architects of its heritage and the guarantors of its quality. We would also like to thank our Readers, some of whom have accompanied us almost from the beginning. We believe that our magazine will continue to be an important and necessary voice in the discussion of the secret services of the democratic Republic of Poland.

Editor-in-Chief
Marek Świerczek, PhD

ARTICLES

Prigozhin's mutiny - causes, course and consequences of the Wagner Group rebellion

FILIP BRYJKA

Institute of Political Sciences of the Polish Academy of Sciences
The Polish Institute of International Affairs
https://orcid.org/0000-0002-8613-1030

Internal Security Review, 2024, no. 30: 269–304

https://doi.org/10.4467/20801335PBW.24.012.19614

ARTICLE

Abstract

The author seeks answers to the question of how the Prighozin's mutiny affected the position of the Wagner Group in Russia. He mainly takes into account the events that took place on 23-24 June 2023, when the mercenaries led by Yevgeny Prigozhin carried out the so-called "march of justice" against the Russian Defense Ministry. The aim of the article is to answer three specific research questions: 1) what factors led to the Wagner Group's rebellion? 2) what was the reaction of the Russian government to these events? 3) what are the consequences of Prigozhin's rebellion for the stability of Putin's regime, the Wagner Group leadership and the organisation as a whole? In seeking answers to these questions, the author focuses on Prigozhin's relations with the Russian military elite. He then presents the course of the rebellion and the Kremlin's reaction to these events. The author further discusses the consequences of the rebellion both within Russia and internationally.

Keywords

Wagner Group, mercenaries, hybrid threats, Russian secret services

On the night of 23-24 June 2023, the head of the Wagner Group, Yevgeny Prigozhin, carried out a rebellion against the Russian Ministry of Defence (Министерство обороны Российской Федерации). The failed attempt by a mercenary group[1] to take control of the ministry was the culmination of a personnel conflict that had been building up since mid-2022 between Prigozhin and Defence Minister Gen. Sergei Shoygu as well as the Chief of the General Staff of the Russian Federation Armed Forces (Генеральный штаб Вооружённых сил Российской Федерации) Gen. Valery Gerasimov[2]. These actions can be seen as a manifestation of Prigozhin's exorbitant political ambitions, a misjudgement of his own position in the power structures and an attempt to maintain the independence of the paramilitary group he leads from the military. On 10 June 2023, General Shoygu announced that from 1 July, all irregular armed formations fighting in Ukraine, i.e. volunteer battalions and so-called private military companies, PMCs (Частная Военная Компания, ЧВК)[3] will be placed under the direct control of the Ministry of Defence. The head

[1] The author deliberately refers to members of the Wagner Group as mercenaries to emphasise their financial motivation. From the point of view of international law, Wagnerists generally (especially in Syria and Africa) meet the criteria to be considered as mercenaries according to Article 47 of the First Additional Protocol to the Geneva Conventions (*Protocols Additional to the Geneva Conventions of 12 August 1949, Relating to the Protection of Victims of International Armed Conflicts (Protocol I) and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), adopted in Geneva on 8 June 1977*), and are therefore not entitled to the status of combatants. In the case of the war in Ukraine, citizens of Russia (a party to the conflict) from the Wagner Group may be qualified as a "militia or other volunteer formation belonging to a party to the conflict" under Article 4 of the Geneva Convention III (*Conventions for the Protection of Victims of War, signed in Geneva on 12 August 1949*). Considering the numerous human rights violations and war crimes (e.g. the murder of prisoners of war in Olenivka, complicity in the Bucza massacre and ethnic cleansing in the occupied territories), however, they do not meet the condition of "respecting in their actions the laws and customs of war". In this case, the Ukrainian side may consider them as so-called unlawful combatants, which does not give them the privileges of combatant status.

[2] A. Legucka, F. Bryjka, *Rywalizacja między rosyjską armią a Grupą Wagnera* (Eng. Rivalry between the Russian army and the Wagner Group), PISM, 6 VI 2023, https://www.pism.pl/publikacje/rywalizacja-miedzy-rosyjska-armia-a-grupa-wagnera [accessed: 6 VI 2023].

[3] In the case of Russia, such formations most often do not meet the criteria to qualify as PMCs, which are illegal under the Russian Constitution (Articles 13 § 5 and 71) and the Criminal Code (Articles 208 and 359). Russia is also not a signatory to the Montreux Document, an attempt to regulate the operation of PMCs. The definition formulated therein speaks of the defensive nature of such entities. According to it, the scope of tasks carried out by contractors should include 'protection of persons and facilities (…), maintenance and operation of weapons systems; detention of prisoners; advice and training of local security forces'. The tasks carried out by the Wagner Group often go beyond this catalogue and are offensive in nature - involving, among other things, destabilising other states, conducting covert combat, paramilitary, intelligence, sabotage and diversionary operations, etc. The Wagner Group cannot be regarded as a PMC also because it employs persons with criminal records. See in more detail: F. Bryjka, *Grupa Wagnera – paramilitarne narzędzie rosyjskich operacji hybrydowych*

of the Wagner Group consistently opposed the subordination of their army and tried unsuccessfully to negotiate an agreement allowing them to retain some operational autonomy.

President Vladimir Putin's administration, with the mediation of Alexander Lukashenko, has managed to defuse the most serious internal crisis in Russia since the Yanayev putsch. The disobedience of Prigozhin - Putin's long-time protégé - highlighted the deepening divisions within Russia's power structures. Although the Wagner rebellion targeted part of the military elite, it had serious image consequences for the president himself and the system of power he had established. The rebellion also signals that the increasing costs of the Russian invasion of Ukraine are beginning to have a negative impact on the stability of the regime, which is tightening its internal mechanisms of control and repression to avoid showing weakness.

Contrary to the frequent opinions of columnists and commentators[4] the putsch and the redeployment of the Wagner Group to Belarus was not operational game by the Russian secret services, but an ad hoc measure to reduce the image costs of the rebellion. It also allowed the Kremlin authorities to sort out the seizure of Prigozhin's assets in Russia, Syria and Africa. The death of the head of the Wagner Group in a plane crash exactly two months after the so-called march of justice was most likely not accidental. Treason and disloyalty in Russian strategic culture are accounted for by means of liquidation operations conducted by the special services[5]. According to The Wall Street Journal, the order to get rid of the putschist leader (with Putin's knowledge and consent) was given by the Secretary of the Security Council of the Russian Federation (RF) Nikolai Patrushev[6].

The deaths of Prigozhin and Wagner's main commander Dmitry Utkin, aka Wagner, began a process of deep reorganisation of the group. The deployment of Russian mercenaries in Belarus may also have important consequences for

(Eng. The Wagner Group - a paramilitary tool of Russian hybrid operations), "Sprawy Międzynarodowe" 2022, vol. 75, no. 2, pp. 68–91. https://doi.org/10.35757/SM.2022.75.2.05.

4 A review of mutually exclusive hypotheses suggesting that Prigozhin's rebellion may have been a special operation by Russian intelligence was presented by Adam Jawor. See the same: *Rosyjskie służby po buncie Prigożyna. Putin wyrównuje szeregi w kremlowskich wieżach* (Eng. Russian services after Prigozhin's revolt. Putin aligns ranks in Kremlin towers), InfoSecurity24, 31 VII 2023, https://infosecurity24.pl/za-granica/rosyjskie-sluzby-po-buncie-prigozyna-putin-wyrownuje-szeregi-w-kremlowskich-wiezach [accessed: 31 VII 2023].

5 M.R. Gordon et al., *Early Intelligence Suggests Prigozhin Was Assassinated, U.S. Officials Say*, The Wall Street Journal, 24 VIII 2023, https://www.wsj.com/world/russia/wagner-prigozhin-russia-assassinated-intelligence-3e456fab [accessed: 24 VIII 2023].

6 T. Grove, A. Cullison, B. Pancevski, *How Putin's Right-Hand Man Took Out Prigozhin*, The Wall Street Journal, 22 XII 2023, https://www.wsj.com/world/russia/putin-patrushev-plan-prigozhin-assassination-428d5ed8?mod=hp_lead_pos7 [accessed: 26 I 2024].

Poland's security. For through them, Russia may intensify its hybrid actions against the countries on NATO's eastern flank.

Reasons for Prigozhin's mutiny

The immediate reason for Prigozhin's decision to march on Moscow was a missile attack on Wagnerists positions in eastern Ukraine. The mercenary chief accused Gen. Shoygu of planning it, and attributed the execution to the Russian armed forces. Although the published footage from the scene does not make it clear that the mercenaries' camp was the target of the attack and that the strike was carried out by the Russian army, it provided the pretext to justify the rebellion[7]. These actions were accompanied by Prigozhin's tirades targeting the military elite, whom he accused of launching a full-scale invasion of Ukraine for the purpose of self-promotion, obtaining advancements and material benefits[8]. In doing so, Prigozhin challenged the Kremlin's propaganda justification for the war in Ukraine, undermining the claim that (…) *NATO and Ukraine pose a threat to Russia*[9].

The dispute between the head of the Wagner Group and the leadership of the Ministry of Defence had been growing since mid-2022. Prigozhin used the military failures of the Russian aggression against Ukraine to openly criticise the ministry and military commanders loyal to Gen. Shoygu. He pointed out, among other things, the mistakes of the command in the conduct of the war operation, the bad situation of poorly trained and inadequately equipped units. He used, among other things, his troll farms and paid military bloggers to launch information attacks. Prigozhin's statements were tolerated by Putin for a long time, which may indicate that the president saw them as criticism of the Russian army's lack of success and pressure on the Ministry of Defence[10].

The personal conflict between Prigozhin and Gen. Shoygu dates back to Russia's intervention in Syria (2015-2019), during which the Wagner Group played the role of the main land component. Problems between the mercenaries and

---

7 Y. Prigozhin, post on Telegram channel, https://t.me/Prigozhin_hat/3797 [accessed: 23 VI 2023].

8 Y. Prigozhin, post on Telegram channel, https://t.me/prigozhin_2023_tg/1844 [accessed: 23 VI 2023].

9 See in more detail: *Sprawa Prigożyna a tuszowanie słabości Rosji i rys na jej wizerunku militarnej potęgi* (Eng. The Prigozhin case and the cover-up of Russia's weaknesses and cracks in its image of military power), EUvsDisinfo, 29 VI 2023, https://euvsdisinfo.eu/pl/sprawa-prigozyna-a-tuszowanie-slabosci-rosji-i-rys-na-jej-wizerunku-militarnej-potegi/ [accessed: 29 VI 2023].

10 A.M. Dyner, *Znaczenie buntu Prigożyna dla rosyjskiej polityki bezpieczeństwa* (Eng. The significance of Prigozhin's revolt for Russian security policy), PISM, 26 VI 2023, https://www.pism.pl/publikacje/znaczenie-buntu-prigozyna-dla-rosyjskiej-polityki-bezpieczenstwa [accessed: 26 VI 2023].

the army included supply issues, a general reluctance to work together and competition for oil production profits[11]. In Prigozhin's view, the Wagnerists were not sufficiently rewarded for their participation in the operation (e.g. for recapturing Palmyra from the hands of the jihadists). The events of 2018, when the Russian military command failed to stop a US attack on a column of Wagner Group mercenaries storming the Conoco refinery, controlled by the Syrian Democratic Forces, were also a flashpoint. An estimated 200-300 Wagnerists were killed at the time[12]. The US attack was not met with retaliatory action by the Russian authorities, who denied links with the mercenaries. At the time, Gen. Shoygu also deprived Prigozhin's companies of numerous contracts for the military, which earned him USD 2 billion in revenue between 2011 and 2018. The defence minister created his own military company Patriot in 2018, which competed with Wagner Group for contracts in Syria and Africa[13].

The conflict between this organisation and the Ministry of Defence escalated in mid-2022 as mercenaries became increasingly involved in the war in Ukraine. Initially, the invasion was supported by around 400 mercenaries tasked with assassinating President Volodymyr Zelensky in order to form a puppet government in Kiev[14]. However, according to Russian investigative journalists from the portals Meduza and The Insider, these were former Wagnerists, who had joined the rival military company Redut founded by the Deputy Chief Intelligence Directorate of the General Staff of the Russian Armed Forces (Главное разведывательное управление Генерального штаба Вооружённых сил Российской Федерации, GRU) Gen. Vladimir Alekseev. From August 2021, Redut began to intensively acquire Wagner personnel resources for the war in Ukraine, which led to a dispute between Prigozhin and Gen. Alekseev[15]. The head of the Wagner Group was not to be informed about preparations for the invasion, nor was his formation

---

[11] See in more detail: M. Gabidullin, *Wagnerowiec. Spowiedź byłego dowódcy tajnej armii Putina* (Eng. Wagnerist. Confession of a former commander of Putin's secret army), Kraków 2022.

[12] R. Blakely, *Russian mercenaries killed by US troops in Syria gun battle*, The Times, 14 II 2018, https://www.thetimes.co.uk/article/russia-mercenaries-killed-by-us-troops-in-syria-gun-battle-g5zswflfg [accessed: 19 I 2024].

[13] S. Sukhankin, *Russia's New PMC Patriot: The Kremlin's Bid for a Greater Role in Africa?*, The Jamestown Foundation, 1 VIII 2018, https://jamestown.org/program/russias-new-pmc-patriot-the-kremlins-bid-for-a-greater-role-in-africa/ [accessed: 12 V 2023].

[14] M. Rana, *Volodymyr Zelensky: Russian mercenaries ordered to kill Ukraine's president*, The Times, 28 II 2022, https://www.thetimes.co.uk/article/volodymyr-zelensky-russian-mercenaries-ordered-to-kill-ukraine-president-cvcksh79d [accessed: 19 I 2024].

[15] *Жаба и Минобороны. Как поссорились Евгений Викторович с Сергеем Кужугетовичем*, The Insider, 12 V 2023, https://theins.ru/politika/261683 [accessed: 12 V 2023].

initially expected to take part in the war effort[16]. However, the situation changed already in the first month of the war, when, due to high losses in men and equipment, as well as numerous desertions, some Russian troops lost their ability to conduct offensive operations. When it became apparent in April 2022 that the Russian army was unable to break through the Ukrainian defensive lines in the Donbass, the Wagner Group's participation amounted to around 1,500 mercenaries, and as many as 7,000 a month later. They were recruited, among others, through veterans' associations (e.g. the League for the Protection of the Interests of Veterans of Local Wars and Armed Conflicts - the so-called League, Лига защиты интересов ветеранов локальных войн и военных конфликтов or the Volunteer Organisation for the Support of the Army, Air Force and Navy - DOSAAF, Добровольное общество содействия армии, авиации и флоту, ДОСААФ), sports clubs, as well as more than 60 regional recruitment centres[17]. In September 2022, with the approval of the Russian authorities, the Wagnerists began mass recruitment in prisons and penal colonies (so-called Project K). In addition to financial benefits, convicts were promised - upon completion of a six-month contract[18] – a pardon (regardless of sentence) by President Putin. In this way, the Wagner Group acquired nearly 40,000 war crime offenders (including those committing rape, torture and murder of civilians). Due to the shortage of artillery ammunition, the command of this organisation treated criminals like cannon fodder. The tactic adopted of continuous assaults by small groups of infantry on selected sections of the front caused losses among the convicts of up to 90 per cent and had little effect[19].

---

[16] *Грубо говоря, мы начали войну Как отправка ЧВК Вагнера на фронт помогла Пригожину наладить отношения с Путиным - и что такое «собянинский полк». Расследование «Медузы» о наемниках на войне в Украине*, Meduza, 13 VII 2022, https://meduza.io/feature/2022/07/13/grubo-govorya-my-nachali-voynu [accessed: 13 VII 2022].

[17] K. Hird et al., *Russian Offensive Campaign Assessment, March 10, 2023*, Institute for the Study of War, 10 III 2023, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-march-10-2023 [accessed: 10 III 2023].

[18] Those who were pardoned by Putin and returned to Russia often committed further crimes, especially murder and rape. See: *Против двоих боевиков ЧВК «Вагнер» в разных регионах России возбудили дела об изнасиловании 13-летних девочек*, Важные истории, 30 VIII 2023, https://storage.googleapis.com/istories/news/2023/08/30/protiv-dvoikh-boevikov-chvk-vagner-v-raznikh-regionakh-rossii-vozbudili-dela-ob-iznasilovanii-13-letnikh-devochek/index.html [accessed: 30 VIII 2023].

[19] J. Ber, *Od Popasnej do Bachmutu. Grupa Wagnera w wojnie rosyjsko-ukraińskiej* (Eng. From Popasna to Bachmut. Wagner's Group in the Russian-Ukrainian war), OSW, 28 IV 2023, https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2023-04-28/od-popasnej-do-bachmutu-grupa-wagnera-w-wojnie-rosyjsko [accessed: 28 IV 2023]; Y. Chornogor, P. Rad, A. Chernysh, *Anatomy of "Wagner PMC": creation, war in Ukraine and ways of countering the group*, Ukrainian PRISM, April 2023, https://prismua.org/wp-content/uploads/2023/05/PMC_Wagner_eng.pdf, p. 9 [accessed: 28 IV 2023].

The Wagnerists initially fought mainly in the Luhansk region, where they played an important role in the seizure of Popasna, Severodonetsk and Lysychansk in the summer of 2022. They were then redeployed to the Donetsk region, where they announced the seizure of Soledar on 10 January 2023[20]. Putin publicly hailed this as a success (…) *for all forces involved in the war in Ukraine*[21], rather than for the Wagner Group alone, which could be interpreted as a warning signal for Prigozhin's growing political ambitions. The head of the Wagner Group planned to run for mayor of Saint Petersburg on behalf of Fair Russia's Sergei Mironov, thus taking the office away from Aleksandr Beglov - a long-time trusted Putin associate. After winning the 2019 elections Beglov prevented Prigozhin from implementing his infrastructure investments on the outskirts of the city and in the Gulf of Finland. In retaliation, Prigozhin attempted to force the Federal Security Service of the Russian Federation (Федеральная служба безопасности Российской Федерации, FSB) and the prosecutor's office to initiate proceedings against the mayor of Saint Petersburg for embezzlement of public money, treason and destruction of cultural sites[22]. During the invasion of Ukraine, Beglov obstructed the Wagner Group's ability to recruit in the region, which contributed to exacerbating the dispute between them.

The role the Wagnerists played on the frontline in Ukraine led to a change in the Kremlin's narrative about the organisation. Until 2021, its existence and any links to the Russian state apparatus were denied. The successes of the Wagnerists led the Kremlin-controlled RT station to produce propaganda videos revealing, among other things, the Wagner Group's previously kept secret involvement in the 2014 aggression against Ukraine, and behind-the-scenes operations in the Middle East and Africa. The Russian authorities also agreed to partially institutionalise Wagnerists activities[23]. In November 2022, the Wagner Group Centre and the Wagnerenok (Вагнеренок) youth club were established in Saint Petersburg. In January 2023, the Wagner Group was registered as a business entity providing 'consultancy services'. However, Prigozhin failed to get the PMC legalised in Russia, which he tried

[20] S. Walker, P. Beaumont, D. Sabbagh, *Head of Russia's Wagner group says his troops have taken control of Soledar*, The Guardian, 11 I 2023, https://www.theguardian.com/world/2023/jan/10/head-of-wagner-group-says-his-troops-have-taken-control-of-soledar [accessed: 1 I 2024].

[21] K. Stepanenko et al., *Russian offensive campaign assessment, January 16, 2023*, Institute for the Study of War, 16 I 2023, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-january-16-2023 [accessed: 19 I 2024].

[22] Y. Chornogor, P. Rad, A. Chernysh, *Anatomy of "Wagner PMC"*…, pp. 20–21.

[23] K.P. Larsen, *From mercenary to legitimate actor? Russian discourses on private military companies*, "Post-Soviet Affairs" 2023, vol. 39, no. 6, pp. 420–439. https://doi.org/10.1080/1060586X.2023.2247782.

to do through the lobbying of the Fair Russia party[24]. As a result of the mercenaries' involvement in the invasion of Ukraine, the Russian government lost all plausible deniability of the state's links to the organisation, which had previously had limited effectiveness anyway[25].

The Kremlin's policy towards the Wagner Group reinforced the organisation's head's belief in his growing position in the power system and encouraged him to further confront the military. A warning signal for Prigozhin's growing ambitions was the assassination of Russian blogger Maksim Fomin (aka Vladlen Tatarsky, who was one of many war propagandists and critics of the Ministry of Defence linked to the Wagner Group. The bombing occurred on 2 April 2023 during Tatarsky's author meeting in central Saint Petersburg in a bar owned by Prigozhin. The venue also served as a discussion club for the Cyber Front Z group[26]. Ukraine was officially accused of carrying out the bombing, but given the context of the relationship between the mercenary chief and the Ministry of Defence at the time, it can be assumed that this was a liquidation operation by the Russian special services.

The rivalry between the Wagnerists and the military intensified on 11 January 2023, when Putin put Gen. Gerasimov in charge of the occupation troops in Ukraine directly. He replaced Gen. Sergei Surovikin, who had been cooperating with the Wagner Group. The Ministry of Defence attempted to weaken Prigozhin and the Wagnerists fighting at Bakhmut by restricting the supply of ammunition and taking control of the recruitment process in the penal colonies (by May 2023, the army had recruited 10,000 people in this way). In retaliation, Prigozhin was said to have offered Ukrainian military intelligence (Головне управління розвідки Міністерства Оборони України) information on the position of Russian troops in the Donbass in exchange for the surrender of Bakhmut[27]. The Ukrainian side did not accept this offer, fearing deception. The head of the mercenaries blamed

[24] F. Bryjka, *Transformacja Grupy Wagnera w związku z wojną na Ukrainie* (Eng. Transformation of the Wagner Group in the wake of the war in Ukraine), PISM, 7 III 2023, https://www.pism.pl/publikacje/transformacja-grupy-wagnera-w-zwiazku-z-wojna-na-ukrainie [accessed: 7 III 2023].

[25] P. Stronski, *Implausible Deniability: Russia's Private Military Companies*, Carnegie Endowment for International Peace, 2 VI 2020, https://carnegieendowment.org/2020/06/02/implausible-deniability-russia-sprivate-military-companies-pub-81954 [accessed: 2 VI 2020].

[26] *В кафе Петербурга на «творческом вечере» «военкора» Владлена Татарского (у него полмиллиона подписчиков в телеграме) произошел взрыв. Блогер погиб*, Meduza, 2 IV 2023, https://meduza.io/feature/2023/04/02/v-peterburge-v-kafe-evgeniya-prigozhina-proizoshel-vzryv-vo-vremya-tvorcheskogo-vechera-voenkora-vladlena-tatarskogo-po-predvaritelnym-dannym-on-pogib [accessed: 2 IV 2023].

[27] S. Harris, I. Khurshudyan, *Wagner chief offered to give Russian troop locations to Ukraine*, The Washington Post, 15 V 2023, https://www.washingtonpost.com/national-security/2023/05/14/prigozhin-wagner-ukraine-leaked-documents/ [accessed: 15 V 2023].

the Ministry of Defence and the General Staff for the high losses (estimated at 20,000-30,000 people) in the fighting for Bakhmut[28], and threatened to surrender the occupied positions to Ukraine. The issue of the 'ammunition famine' was resolved with the participation of General Surovikin, who acted as an intermediary between the Wagnerists and the army. Although Putin congratulated the Wagner Group on the seizure of Bakhmut on 20 May 2023, he pointed out that units of the regular army were also involved in the operation[29]. Prigozhin downplayed this fact and attributed the success solely to his mercenaries. He then announced that by the end of May, the Wagner Group would hand over all seized positions to the Russian armed forces, withdraw from Ukraine and rebuild combat capability for two months[30]. The Ministry of Defence used this moment to subdue all irregular armed formations fighting in Ukraine. The head of the Wagnerists unsuccessfully tried to prevent them from losing their operational autonomy and subordinating themselves to the military, leading to the so-called march of justice.

The course of the Wagner Group rebellion

On the night of 23-24 June 2023, Prigozhin declared that the Wagner Group had crossed the Ukrainian-Russian border in the Rostov region and was heading for Moscow. The mercenary chief stressed that the operation he was conducting was not a coup against Putin, but a so-called march of justice against Defence Minister Gen. Shoygu. The Wagnerists arrived without resistance at the headquarters of the Southern Military District (SMD) in Rostov-on-Don, which also acts as the command of the "special military operation" in Ukraine. On site, they were met with a positive response from the local community[31]. Prigozhin held talks with Deputy Defence Minister Gen. Yunus Bek Yevkurov and first deputy GRU chief Gen. Alexeyev. The putschist leader's demands to talk to Gen. Shoygu and Gen. Gerasimov were rejected, which influenced the decision to continue the march. Prigozhin called

[28] On the role of the Wagner Group in the battles for Bachmut see in more detail: K. Stepanenko, *The Kremlin's Pyrrhic Victory in Bakhmut: A Retrospective on the Battle for Bakhmut*, Institute for the Study of War, 24 V 2023, https://www.understandingwar.org/backgrounder/kremlin%E2%80%99s-pyrrhic-victory-bakhmut-retrospective-battle-bakhmut [accessed: 24 V 2023].

[29] *Путин поздравил российских военных с освобождением Артемовска*, Tacc, 20 V 2023, https://tass.ru/politika/17804025 [accessed: 19 I 2024].

[30] Y. Prigozhin, post on Telegram channel, https://t.me/concordgroup_official/1002 [accessed: 20 V 2023].

[31] P. Ivanova, A. Stognei, M. Seddon, *Russian insurrection: Prigozhin's failed mutiny and the fallout*, Financial Times, 23 VI 2023, https://www.ft.com/content/34f3a349-a05f-4672-b059-6980ecc27adf [accessed: 23 VI 2023].

on the entire Russian army to join the rebels. However, this did not meet with the response he expected from the military. Even Gen. Surovikin, who had contributed to the rise of the Wagner Group's position during his time as commander of the military operation in Ukraine, condemned the putsch and called on the Wagnerists not to follow Prigozhin's orders. The rebels were also not supported by the federal and regional authorities, the power structures or the business elite.

The mercenary columns heading towards Moscow consisted of around 1,000 units of military equipment and vehicles (including Tigr armoured vehicles and infantry fighting vehicles, T-80 and T-90 tanks, BM-21 Grad rocket launchers, and Pancyr S-1 surface-to-air systems)[32]. Prigozhin declared that the force he was leading consisted of 25,000 mercenaries. It is possible that he meant all Wagner Group personnel - including those conducting operations in Africa and receiving medical treatment in Russia. In all likelihood, 5,000-10,000 Wagnerists participated in the rebellion[33]. In response to the rebellion, the FSB Investigative Committee opened criminal proceedings against Prigozhin under Article 279 of the Russian Criminal Code, which states the organisation of a rebellion, punishable by 20 years in prison. Security measures have been stepped up in Moscow. Federal Military Service of the RF National Guard (Федеральная служба войск национальной гвардии Российской Федерации, Rosgwardia), The Special Mobile Unit (Отряд мобильный особого назначения, OMON) and the Special Rapid Response Unit (Специальный Отряд Быстрого Реагирования, SOBR) have been placed on high alert[34]. Military personnel and law enforcement agencies set up military posts and checkpoints near the SMD headquarters in Rostov-on-Don. The Federal Security Service and SOBR units also prepared roadblocks along the Moscow--Voronezh-Rostov route[35]. The Wagnerists generally encountered no resistance from the military or security services, but a few clashes resulted in the downing of six helicopters and an Il-22M aircraft. Thirteen pilots were killed[36].

---

[32] M. Galeotti, *Russia's coup d'état – Nature and Implications*, In Moscow's Shadows, 27 VI 2023, https://inmoscowsshadows.wordpress.com/2023/06/27/scss10-26-june-2023-russias-coup-detat-nature-and-implications/ [accessed: 27 VI 2023].

[33] Ibid.

[34] *В Москве усилили меры безопасности*, Tacc, 23 VII 2023, https://tass.ru/proisshestviya/18103225 [accessed: 23 VII 2023].

[35] *В Ростове-на-Дону рядом со штабом ЮВО выставили посты*, Tacc, 23 VII 2023, https://tass.ru/bezopasnost/18103205 [accessed: 23 VII 2023].

[36] S. Mitzer, J. Janovsky, *Chef's Special – Documenting Equipment Losses During The 2023 Wagner Group Mutiny*, Oryx, 24 VI 2023, https://www.oryxspioenkop.com/2023/06/chefs-special-documenting-equipment.html [accessed: 24 VI 2023].

Negotiations with Prigozhin were undertaken by Lukashenko, who urged the Wagnerists leader to cease hostilities to avoid further bloodshed. According to the official message[37], he conducted them in consultation with Putin, who rejected the offer of a phone call or meeting with Prigozhin. General Yevkurov and FSB chief Aleksandr Bortnikov also played an important mediating role. During the negotiations, Prigozhin abandoned his planned raid on the Defence Ministry. The Wagner Group's columns stopped about 200 km outside Moscow and turned back towards the Donbass. In return, the Russian authorities abandoned the pursuit of the putschists, and the Russian president gave Prigozhin unspecified security guarantees on the condition that he would move to Belarus with the rebels[38].

The Russian government admitted that on 29 June 2023 Putin met with Prigozhin and 35 commanders of the Wagner Group[39]. During the three-hour meeting in the Kremlin, the Russian president assessed the role of mercenaries in the war in Ukraine so far, gave his assessment of the armed rebellion, and listened to the explanations and assurances of the Wagnerists about their loyalty to the state and its president. The mercenaries were offered three options:

1) signing a contract with the Russian Ministry of Defence and continuing to fight in Ukraine,
2) following their leader to Belarus,
3) terminating the contract and returning to Russia without legal consequences for participation in the mutiny[40].

At the same time, Putin stated that such an entity as the Wagner Group does not exist, as PMC's activities in Russia are prohibited by law[41].

Although Prigozhin's rebellion targeted Gen. Shoygu, and the head of the Wagnerists repeatedly stressed his loyalty to Putin, the fact that the so-called march of justice took place caused serious (negative) consequences for the Russian president. First of all, it undermined his authority as a strong and capable leader, as he was forced to negotiate with a rebel. It weakened the president's image among

---

37 Y. Preiherman, *What Does Lukashenka's Role as Mediator in Russian Crisis Imply? – Analysis*, Eurasia Review, 29 VI 2023, https://www.eurasiareview.com/29062023-what-does-lukashenkas-role-as-mediator-in-russian-crisis-imply-analysis/ [accessed: 29 VI 2023].

38 *Вручение генеральских погон высшему офицерскому составу*, Президент Республики Беларусь, 27 VII 2023, https://president.gov.by/ru/events/vruchenie-pogon-vysshemu-oficerskomu-sostavu [accessed: 27 VII 2023].

39 Ibid.

40 *Песков подтвердил встречу Путина с Пригожиным и командирами «Вагнера» 29 июня*, Интерфакс, 10 VII 2023, https://www.interfax.ru/russia/910904 [accessed: 10 VII 2023].

41 *Putin says Wagner Group doesn't legally exist*, Meduza, 14 VII 2023, https://meduza.io/en/news/2023/07/14/putin-says-wagner-group-no-longer-legally-exists [accessed: 14 VII 2023].

the power elite[42]. Putin described Prigozhin's rebellion as "treason" and a "stab in the back". He called the mercenary chief a corrupt liar who destroyed the reputation of the Wagner Group. He described the march on Moscow as (…) *a mortal threat to the state* and assured that (…) *all those who participated in the preparation of the rebellion would suffer severe punishment*[43]. According to The Washington Post, the Russian president was said to have received intelligence on preparations for the rebellion 2-3 days before the mutiny[44]. These reports seem to be confirmed by the deployment of FSB 'Alpha' special units to protect the Lubianka headquarters[45]. Despite this, Putin was said to have not given a single order and to have left the decision on how to respond to the so-called march of justice to the regional military and security services. The rebellion of the Wagnerists revealed the failure of the services to effectively neutralise such actions. In doing so, their inaction was due to the lack of specific orders and the belief that the head of the Wagner Group was under the Kremlin's tutelage and that the activities of his mercenaries were controlled by the authorities. The president was to be assisted in resolving the crisis by the governor of the Tula region, an FSB and GRU officer responsible in the past for, among other things, Putin's security - Colonel General Alexei Diumin[46]. He has been touted by many commentators as a potential successor to Gen. Shoygu.

---

[42] A. Legucka, *Konsekwencje buntu Prigożyna dla systemu putinowskiego w Rosji* (Eng. Consequences of Prigozhin's revolt for the Putinist system in Russia), PISM, 26 VI 2023, https://www.pism.pl/publikacje/konsekwencje-buntu-prigozyna-dla-systemu-putinowskiego-w-rosji [accessed: 26 VI 2023]; M. Komin, *"Fighting spirit": Russia's technocrat elite after the Wagner mutiny*, European Council on Foreign Relations, 24 VII 2023, https://ecfr.eu/article/fighting-spirit-russias-technocrat-elite-after-the-wagner-mutiny/ [accessed: 24 VII 2023].

[43] *Обращение к гражданам России*, Kremlin.ru, 24 VI 2023, https://web.archive.org/web/20230628083145/https://kremlin.ru/events/president/news/71496 [accessed: 24 VI 2023].

[44] C. Belton, S. Harris, G. Miller, *Putin appeared paralyzed and unable to act in first hours of rebellion*, The Washington Post, 25 VII 2023, https://www.washingtonpost.com/world/2023/07/25/putin-prigozhin-rebellion-kremlin-disarray/ [accessed: 25 VII 2023].

[45] M. Weiss, *Russia's Spies Say Putin Faces More Coups*, The Insider, 20 VII 2023, https://theins.ru/en/politics/263596 [accessed: 20 VII 2023].

[46] Colonel-General Alexei Diumin (born 28 August 1972 in Kursk) - graduated from the Higher Military School of Radioelectronic Engineering in Voronezh in 1994. He then worked as an engineer at the Central Centre for Integrated Technical Control of the Russian Air Force until 1996. From 1996 to 2013, he served in the FSB, where he was responsible for, among other things, presidential security. In 2009, he graduated with honours from the Russian Academy of Public Administration (Civil Service) under the President of the Russian Federation, and in 2013 from the Military Academy of the General Staff of the Russian Armed Forces. From 2013 to 2016, he was Deputy Chief of the GRU, Chief of the General Staff and First Deputy Commander-in-Chief of the Land Forces, and then Deputy Minister of Defence of the Russian Federation. Since 2016, he has served as governor of the Tula region. See: Д. Дурова, *В России уже нашли нового министра обороны для*

To stabilise the regime and consolidate his own position, Putin decided to strengthen the National Guard in charge of internal security and commanded by General Viktor Zolotov, who is loyal to the president[47]. On 19 July 2023, the State Duma of the Russian Federation passed a law allowing this formation to possess heavy military equipment for the recovery of hostages, protection of citizens, officials and military personnel, providing security during riots and emergencies, combating unmanned aircrafts, as well as the activities of illegal armed groups[48]. In all likelihood, specialised military equipment has gone to the Oplot (Eng. Fortress) regiment. The elite Grom unit, which had previously been part of the Federal Drug Control Service (FSKN, Федеральная служба Российской Федерации по контролю за оборотом наркотиков)[49] was subordinated to the Rosgvardia. The strengthening of the Rosgvardia, which is a kind of security cordon for the president, shows that Putin fears further attacks of which he may be a target.

The Wagner rebellion has also resulted in purges in the Russian army. More than a dozen generals have been arrested, including former Deputy Defence Minister for Logistics Gen. Mikhail Mizintsev, who was first removed from his post at the Defence Ministry for supplying the Wagnerists with ammunition and then signed a contract with the Wagner Group. Another is Gen. Surovikin, who made the Wagnerists a key assault force in the urban fighting in the Donbass. On the day of Prigozhin's death, Gen. Surovikin was removed from his position as commander of the Russian air and space forces[50]. In time, however, he was released from house arrest and took up the post of head of the Coordinating Committee for Air

Пригожина: в сети назвали имя, Oboz.ua, 25 VI 2023, https://news.obozrevatel.com/russia/v-rossii-uzhe-nashli-novogo-ministra-oboronyi-dlya-prigozhina-v-seti-nazvali-imya.htm [accessed: 25 VI 2023].

47 J. Darczewska, *Rosgwardia. Siły specjalnego przeznaczenia* (Eng. Rosgvardia. Special purpose forces), "Punkt Widzenia OSW" 2020, no. 78, p. 5.

48 *State Duma passes bill allowing Russia's National Guard troops to use heavy military equipment*, Meduza, 19 VII 2023, https://meduza.io/en/news/2023/07/19/state-duma-passes-bill-allowing-russia-s-national-guard-troops-to-use-heavy-military-equipment [accessed: 19 VII 2023].

49 М. Солопов, *Силовые ведомства прорабатывают вопрос о переподчинении полицейского спецназа «Гром» Росгвардии*, Ведомости, 4 VII 2023, https://www.vedomosti.ru/politics/articles/2023/07/04/983567-vedomstva-prorabativayut-vopros-o-perepodchinenii-politseiskogo-spetsnaza-rosgvardii [accessed: 4 VII 2023].

50 He was replaced by Colonel-General Viktor Afzalov, who had served as Chief of Staff of the Russian Air Force since August 2018. See: *Источник: врио главкома ВКС назначили генерала Афзалова*, Риа Новости, 23 VIII 2023, https://ria.ru/20230823/afzalova-1891645152.html [accessed: 23 VIII 2023].

Defence within the Council of Defence Ministers of the Commonwealth of Independent States[51].

The authorities in the Kremlin have also taken steps to silence critics. Igor Girkin aka Strelkov - a former FSB Spetsnaz colonel and self-proclaimed defence minister of the Donetsk People's Republic (DNR, Донецкая Народная Республика) - was arrested. His social media activity has pushed the boundaries of criticism acceptable to the Kremlin. He even founded the Angry Patriots Club of nationalists openly expressing their dissatisfaction with the way the war in Ukraine is being conducted[52]. The Russian Investigative Committee has charged him, as well as Pavel Gubarev (in the past self-proclaimed leader of the DNR and chairman of the Angry Patriots Club), with extremist activities[53]. The main reason for Girkin's detention was his political ambitions. He planned to capitalise on his popularity among nationalist circles by running in the presidential elections in spring 2024[54]. On 25 January 2024, a court in Moscow sentenced him to four years' imprisonment on charges of inciting extremism[55].

The Wagner Group in Belarus

As a result of Lukashenko's mediation, Putin gave Prigozhin and his mercenaries unspecified security guarantees on the condition that the members of the Wagner Group would be relocated to Belarus. The process of deploying the Wagnerists

---

[51] *Генерал Суровикин возглавил координационный комитет СНГ по вопросам ПВО Подробнее*, EurAsia Daily, 10 X 2023, https://eadaily.com/ru/news/2023/09/10/general-surovikin-vozglavil-koordinacionnyy-komitet-sng-po-voprosam-pvo [accessed: 10 X 2023].

[52] In addition to Girkin, former FSB colonel Mikhail Polyakov and former GRU colonel Vladimir Kvachkov were taken into custody. They all ran channels on Telegram used to openly criticise the Kremlin, the Ministry of Defence and the General Staff of the Russian Armed Forces. See: K. Kirillova, *Propaganda and Repression Turn Against Their Creators in Russia*, The Jamestown Foundation, 25 VII 2023, https://jamestown.org/program/propaganda-and-repression-turn-against-their-creators-in-russia/ [accessed: 25 VII 2023].

[53] *Pavel Gubarev, associate of Igor Strelkov, reportedly investigated for extremism*, Meduza, 23 VII 2023, https://meduza.io/en/news/2023/07/23/pavel-gubarev-associate-of-igor-strelkov-reportedly-investigated-for-extremism [accessed: 23 VII 2023].

[54] *Jailed former 'Donetsk People's Republic' militia leader to run for president*, Novaya Gazeta Europe, 31 VIII 2023, https://novayagazeta.eu/articles/2023/08/31/jailed-former-donetsk-peoples-republic-militia-leader-to-run-for-president-en-news [accessed: 31 VIII 2023].

[55] *Russia sentences former separatist commander and pro-war blogger Igor Strelkov to four years in prison*, Meduza, 25 I 2024, https://meduza.io/en/news/2024/01/25/russia-sentences-former-separatist-commander-and-pro-war-blogger-igor-strelkov-to-four-years-in-prison [accessed: 25 I 2024].

began during the NATO summit in Vilnius on 11 July 2023. Belarusian authorities provided them with military infrastructure in the village of Tsel near Osipovich in the Mogilev region, where the main Wagnerists' camp was established on the site of a former missile army base (military unit no. 61732). On 27 June, tents capable of accommodating a total of around 8,000 people began to be erected there[56]. At the end of July, the Wagner Group's previous base in Molkino, Russia, which was located at the GRU's 10th Special Purpose Brigade, was dismantled[57].

On 18 July, Prigozhin and Utkin appeared in the Wagner camp. In their speeches, they emphasised the start of a new chapter in the organisation's history. Its main task in Belarus is to train soldiers and units of the Ministry of Internal Affairs[58]. The new location allowed for the organisation of a logistical base for Wagner Group operations in Africa. At the same time, Prigozhin did not rule out the possibility of the mercenaries returning to Ukraine[59]. The following day, the Wagner chief registered a subsidiary company in Belarus, Concord Management and Consulting, which was officially to deal with property management[60]. Sergei Chubko aka Pioneer - a veteran of operations in Syria, the Central African Republic (CAR), Sudan, Mali and Libya, decorated with five Medals for Courage - became the commander of the Wagner Group in Belarus[61].

---

[56] In addition to the base in Tsel village, the Wagnerists are also expected to have smaller facilities in the village of Sosnovi near Osipovich and the town of Narovla (Gomel region). See: *Вагнерівці продовжують прибувати у білорусь*, Центр Національного спротиву, 22 VII 2023, https://sprotyv.mod.gov.ua/vagnerivtsi-prodovzhuyut-prybuvaty-u-bilorus/ [accessed: 22 VII 2023].

[57] *Наемники ЧВК Вагнера объявили, что закрывают свою главную базу в краснодарском Молькино*, Meduza, 17 VII 2023, https://meduza.io/news/2023/07/17/naemniki-chvk-vagnera-ob-yavili-chto-zakryvayut-svoyu-glavnuyu-bazu-v-krasnodarskom-molkino [accessed: 17 VII 2023].

[58] The Wagner Group mainly trains special operations forces, defence troops against weapons of mass destruction, mechanised troops, engineering and communications troops, as well as territorial defence. Training takes place, among others, at the Brest training ground located near the Polish border. See: A.M. Dyner, *Grupa Wagnera na Białorusi – potencjalne zagrożenia dla Polski* (Eng. The significance of Prigozhin's revolt for Russian security policy), PISM, 27 VII 2023, https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-potencjalne-zagrozenia-dla-polski [accessed: 27 VII 2023].

[59] *'Welcome to hell' Prigozhin reappears in Belarus, rallying Wagner Group mercenaries for future work in Africa (but not yet in Ukraine)*, Meduza, 19 VII 2023, https://meduza.io/en/feature/2023/07/19/welcome-to-hell [accessed: 19 VII 2023].

[60] *Евгений Пригожин зарегистрировал компанию в Осиповичском районе*, Reformation, 22 VII 2023, https://reform-by.cdn.ampproject.org/c/s/reform.by/evgenij-prigozhin-zaregistriroval-kompaniju-v-osipovichskom-rajone/amp [accessed: 22 VII 2023].

[61] Sergei Chubko (born 27 X 1976 in Chernivtsi, Ukraine, then USSR) - comes from a family with military traditions. His father fought in Afghanistan during the Soviet invasion. After the collapse of the USSR, the family moved to Novorossiysk. From 1994 to 2002, Chubko served in the Russian army (including the airborne troops) and took part in the Chechen wars. After leaving the service, he moved to the private sector. In 2003, despite his lack of higher education, he unexpectedly became

According to activists from the Hajun Project, 14 convoys (a total of about 930 vehicles) of mercenaries, estimated to number between 4,000 and 5,000, had entered Belarus by 1 August. However, the Wagnerists ended up there without any heavy military equipment, as more than 2,000 pieces (including tanks, armoured vehicles, artillery and missile systems), 2,500 tonnes of ammunition and about 20,000 small arms had been seized by the Russian army on 12 July[62]. Therefore, the Wagner Group as an independent armed formation with only small arms did not pose a military threat to the NATO border states. However, the Wagner Group's unclear legal status, combat experience and international recognition gave Belarus and Russia an additional instrument of hybrid influence in the so-called grey zone, in which it is difficult to assess the nature of the threat and assign clear responsibility for various forms of aggression. Poland and the Baltic States feared that Belarus and Russia would use the Wagnerists to attack the services protecting the border and the infrastructure located there, increase migration pressure[63], place their agents among the migrants, infiltrate the territory through sabotage and reconnaissance groups, identify critical infrastructure and prepare acts of sabotage[64].

head of the Novorossiysk municipal administration (2003 - chairman of the Youth Commission in the Novorossiysk administration; 2005 - deputy head of the Myschak Rural District administration). He then became a security guard again in a private company. In 2011, they wanted to strip him of his Russian citizenship due to suspicions of Ukrainian citizenship. In 2014, he helped to establish a Cossack association in Novorossiysk, which may indicate his involvement in the annexation of Crimea or the fighting in the Donbass (but there is no confirmation of this). He joined the Wagner Group in 2017 and took part in operations in Syria. After a year of service, he became commander of the group's operations in eastern Syria. In 2020, he was transferred to Libya, where he headed the Wagner Group's staff. See: *Journalists identify head of Wagner Group forces in Belarus as 46-year-old Ukraine native*, Meduza, 26 VII 2023, https://meduza.io/en/news/2023/07/26/journalists-identify-head-of-wagner-forces-in-belarus-as-46-year-old-ukraine-native [accessed: 26 VII 2023]; *Кто такой Сергей «Пионер» – глава «Вагнера» в Беларуси?*, Reformation, 19 VII 2023, https://reform.by/kto-takoj-sergej-pioner-glava-vagnera-belarusi [accessed: 19 VII 2023].

62 *Wagner Group reportedly hands over military equipment and ammunition to Russia's Defense Ministry*, Meduza, 12 VII 2023, https://meduza.io/en/news/2023/07/12/wagner-group-reportedly-hands-over-military-equipment-and-ammunition-to-russia-s-defense-ministry [accessed: 12 VII 2023].

63 A. Sari, *Hybrid CoE Paper 17: Instrumentalized migration and the Belarus crisis: Strategies of legal coercion*, Hybrid CoE, 25 IV 2023, https://www.hybridcoe.fi/publications/hybrid-coe-paper-17-instrumentalized-migration-and-the-belarus-crisis-strategies-of-legal-coercion/ [accessed: 25 IV 2023]. On Russia's use of coercive engineered migration, see: M. Wojnowski, *The genesis, theory, and practice of Russian coercive migration engineering. A contribution to the study of the migration crisis on NATO's eastern flank*, "Internal Security Review" 2022, no. 26, pp. 263–300. https://doi.org/doi: 10.4467/20801335PBW.21.042.15702.

64 A.M. Dyner, W. Lorenz, F. Bryjka, *Grupa Wagnera na Białorusi – konsekwencje dla NATO i UE* (Eng. The Wagner Group in Belarus - implications for NATO and the EU), PISM, 7 IX 2023, https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-konsekwencje-dla-nato-i-ue [accessed: 7 IX 2023].

The presence of Russian mercenaries in Belarus has been used in Russia's psychological and disinformation operations. The chairman of the Defence Affairs Committee of the Russian State Duma, Andrei Kartapolov, suggested that the deployment of the Wagnerists signifies Russia's preparations to occupy the so-called Suwałki Gap separating Belarus from the Russian exclave (Königsberg region)[65]. Lukashenko warned that the Wagnerists would like to enter Polish territory in order to carry out military actions in Warsaw and in Rzeszów, where the main logistics hub for supplying Ukraine with military aid provided by Western countries is located. Putin, on the other hand, stated that Poland has aggressive plans against Ukraine and Belarus, and Russia is ready to respond to them "with all available means"[66]. Coordinated actions in the information sphere were intended to intimidate Polish society and influence the Polish authorities to change their policy towards Belarus and Russia to a less confrontational one and to stop supporting Ukraine. These actions were also a clear warning that the Wagnerists could be used for a provocation that would force a disproportionate response from NATO and EU border states. In this way, Russia and Belarus created a sense of threat and increased tension within NATO and hoped that this would exacerbate political divisions among the allies over the assessment of the threat nature and its possible consequences, and thus make it more difficult for them to respond effectively[67].

In order to discourage Belarus and Russia from escalating provocations and to strengthen its sense of security, Poland increased support to the Border Guard by several hundred police officers (including counter-terrorists), deployed additional military troops (up to 4,000 soldiers) on the border and created a task force in the operation codenamed 'RENGAW' (6,000 soldiers) kept in reserve[68]. Lithuania has closed four of its six border crossings with Belarus due to the risk of infiltration of the territory by Wagnerists using Belarusian passports. Countries in the region warned that they could close their borders with Belarus completely, which would

---

[65] *Celem wagnerowców na Białorusi będzie "przejęcie Przesmyku Suwalskiego" – rosyjski deputowany* (Eng. Wagnerists' goal in Belarus will be to 'take over the Suwałki Gap' - Russian MP), Belsat, 16 VII 2023, https://belsat.eu/pl/news/16-07-2023-celem-wagnerowcow-na-bialorusi-bedzie-przejecie-przesmyku-suwalskiego-rosyjski-deputowany [accessed: 16 VII 2023].

[66] P. Żochowski, *Rosja i Białoruś oskarżają Polskę o plany agresji* (Eng. Russia and Belarus accuse Poland of aggression plans), OSW, 24 VII 2023, https://www.osw.waw.pl/pl/publikacje/analizy/2023-07-24/rosja-i-bialorus-oskarzaja-polske-o-plany-agresji [accessed: 24 VII 2023].

[67] A.M. Dyner, W. Lorenz, F. Bryjka, *Grupa Wagnera na Białorusi – konsekwencje dla NATO i UE…*

[68] *Operacja RENGAW. Na granicy polsko-białoruskiej rozpoczyna działanie wojskowe zgrupowanie zadaniowe* (Eng. Operation RENGAW. A military task force is launched on the Polish-Belarusian border), gov.pl, 12 VIII 2023, https://www.gov.pl/web/obrona-narodowa/operacja-rengaw-na-granicy-polsko--bialoruskiej-rozpoczyna-dzianie-wojskowe-zgrupowanie-zadaniowe [accessed: 26 I 2024].

cut it off from trade opportunities with the EU, which - despite the sanctions imposed on the country - remains its second largest trading partner (after Russia). They also called on the Belarusian authorities to immediately remove the Wagner Group from the territory of the country, as well as to withdraw migrants used by Belarusian services to destabilise the border from the border areas[69].

An important element of Russian-Belarusian psychological operations using the Wagner Group was the impact on Polish society. According to a survey by the Institute for Market and Social Research, more than half of Poles (50.6% of respondents) perceived the presence of Wagnerists in Belarus as a threat to Poland's security[70]. The disinformation-propaganda apparatus of Russia and Belarus tried to sustain these sentiments by, among other things, disseminating a graphic depicting a mercenary holding a knife and fork and embracing Polish soldiers against a background of a border post and the inscription 'Keep the fork in your left hand, the knife in your right, and the Poles in fear'. A reworked photo of a Polish soldier with the Wagner Group insignia and a Russian flag glued on also appeared online. Other graphics showed Polish and Belarusian border posts with the hand of a mercenary with a Wagner Group patch glued on, which was supposed to suggest that members of this organisation were infiltrating Polish territory. However, analysis of the images clearly showed that they had been manipulated. Similar activities were carried out against Lithuania and Latvia. On 11 August 2023, the Internal Security Agency detained two Russians who, on the orders of Russian intelligence, were distributing propaganda materials of the Wagner Group in Cracow and Warsaw[71].

Disintegration of the Prigozhin Empire

Russian investigative journalists have identified more than 400 companies linked to Prigozhin[72]. These assets are being seized by oligarchs loyal to Putin, but the details of this process are not fully known. The play focuses on two segments of Prigozhin's criminal and business activities:

---

[69] A.M. Dyner, W. Lorenz, F. Bryjka, *Grupa Wagnera na Białorusi – konsekwencje dla NATO i UE…*

[70] I. Kacprzak, *Wagnerowcy sieją zamęt na granicy. Ponad połowa Polaków uważa, że stanowią zagrożenie* (Eng. Wagnerists sow confusion at the border. More than half of Poles consider them a threat), Rzeczpospolita, 1 VIII 2023, https://www.rp.pl/spoleczenstwo/art38884031-wagnerowcy-sieja-zamet-na-granicy-ponad-polowa-polakow-uwaza-ze-stanowia-zagrozenie [accessed: 1 VIII 2023].

[71] *ABW zatrzymała 2 obywateli Rosji* (Eng. ISA detained 2 Russian citizens), gov.pl, 14 VIII 2023, https://www.gov.pl/web/sluzby-specjalne/abw-zatrzymala-2-obywateli-rosji [accessed: 14 VIII 2023].

[72] *Прошлое и будущее Пригожина. Как владелец ЧВК «Вагнер» создал свою армию - и что будет делать после мятежа*, Досье, 6 VII 2023, https://dossier.center/wagner-fall/ [accessed: 6 VII 2023].

1) a media empire used to conduct influence operations, spread propaganda and disinformation as well as interfere in the political processes of Western countries,
2) companies used to exploit natural resources in Africa and Syria, where in exchange for the Wagner Group's military services, Prigozhin's companies were awarded contracts for the extraction of oil, gold, diamonds or logging, among others.

According to The New York Times, the first sector was seized by the Foreign Intelligence Service of RF (Служба Внешней Разведки Российской Федерации, SVR), and the other is under the control of the GRU and the Ministry of Defence[73].

Even during the so-called march of justice on Moscow, the Federal Service for Supervision in the Sphere of Communications, Information Technologies and Mass Communications, Roskomnadzor (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, Роскомнадзор) blocked communications from the Russian media organisation Patriot Media Group, which was subsequently dissolved[74]. This included the RIA FAN agency, where Prigozhin served as head of the supervisory board. In addition, Prigozhin's media assets from 2013 included troll and bot farms, channels on Telegram and bloggers involved in Russian disinformation operations. Prigozhin's media assets were most likely taken over by state-owned corporations, led by Yuri Kovalchuk's holding company or one of the directors of state-owned Rostech Vasily Brovka, among others[75].

During the seizure of Prigozhin's media assets, Russian government representatives (including Sergei Lavrov and Dmitry Peskov) assured that the Wagner Group would continue its operations in Africa, where 4,000-5,000 mercenaries are based[76]. In reality, however, the GRU and the Ministry of Defence were taking

---

[73] A. Troianovski et al., *After Prigozhin's Death, a High-Stakes Scramble for His Empire*, The New York Times, 8 IX 2023, https://www.nytimes.com/2023/09/08/world/europe/prigozhin-wagner-russia-africa.html [accessed: 8 IX 2023].

[74] *Yevgeny Prigozhin reportedly dissolving Patriot Media Group, home of his 'troll factory'*, Meduza, 30 VI 2023, https://meduza.io/en/news/2023/06/30/prigozhin-reportedly-dissolving-patriot-media-group-home-of-his-troll-factory [accessed: 30 VI 2023].

[75] J. Czerep, A. Legucka, *Przyszłość "imperium" Prigożyna* (Eng. The future of Prigozhin's "empire"), PISM, 17 VII 2023, https://www.pism.pl/publikacje/przyszlosc-imperium-prigozyna [accessed: 17 VII 2023]; A. Stognei, M. Seddon, *Yevgeny Prigozhin's 'toxic' media empire left in Kremlin limbo*, Financial Times, 14 VII 2023, https://www.ft.com/content/723a967f-213b-45b4-8ca6-792aa8e10ba0?shareType=nongift [accessed: 14 VII 2023].

[76] See in more detail: J. Stanyard, T. Vircoulon, J. Rademeyer, *The Grey Zone: Russia's military, mercenary and criminal engagement in Africa*, Global Initiative Against Transnational Organized Crime, 16 II 2023, https://globalinitiative.net/analysis/russia-in-africa/ [accessed: 16 II 2023]; *Guns for gold:*

steps to prepare the ground for the takeover of this sphere of the Prigozhin empire. In Syria, members of the Wagner Group were coerced into signing contracts with the Ministry of Defence[77]. They were then denied access to the Hmeimim military airbase, used to supply operations in Syria and the CAR, where 1,900 mercenaries are deployed[78].

In mid-August, at the Armia-2023 arms fair near Moscow, Gen. Shoygu urged representatives of African states not to use the services of the Wagner Group, but to cooperate only with companies subordinate to the Ministry of Defence. In doing so, he threatened to break off military-technical cooperation and withdraw Russia's diplomatic support at the UN[79]. On the eve of his death, the head of the Wagnerists published videos recorded in one of the countries in Africa (most likely the CAR or Mali), in which he assured the continuation of operations on the continent[80]. At the same time, however, Gen. Yevkurov embarked on a series of diplomatic visits to Africa and the Middle East (by mid-September he had been to Libya, Syria, Burkina Faso, Mali, Algeria, Sudan and Niger, among others), where he discussed new rules of military cooperation with Russia. These most likely included the issue

the Wagner Network exposed, House of Commons Foreign Affairs Committee, 26 VII 2023, https://committees.parliament.uk/publications/41073/documents/200048/default/ [accessed: 26 VII 2023]; E. Pokalova, *The Wagner Group in Africa: Russia's Quasi-State Agent of Influence*, "Studies in Conflict & Terrorism", https://doi.org/10.1080/1057610X.2023.2231642; M. Weiss, P. Vaux, *The Company You Keep: Yevgeny Prigozhin's Influence Operations in Africa*, Free Russia Foundation, Washington 2020, https://www.4freerussia.org/wp-content/uploads/sites/3/2020/09/The-Company-You-Keep-Yevgeny-Prigozhins-Influence-Operations-in-Africa.pdf [accessed: 16 II 2023]; L. Serwat, H. Nsaibia, N. Gurcov, *Moving Out of the Shadows: Shifts in Wagner Group Operations Around the World*, The Armed Conflict Location & Event Data Project (ACLED), 2 VIII 2023, https://acleddata.com/2023/08/02/moving-out-of-the-shadows-shifts-in-wagner-group-operations-around-the-world/#exec [accessed: 2 VIII 2023]; G. Kuczyński, *Wagnerowcy. Psy wojny Putina* (Eng. Wagnerists. Putin's dogs of war), Warszawa 2022.

77 S. Al-Khalidi, M. Gebeily, *Syria brought Wagner fighters to heel as mutiny unfolded in Russia*, Reuters, 7 VII 2023, https://www.reuters.com/world/syria-brought-wagner-group-fighters-heel-mutiny-unfolded-russia-2023-07-07/ [accessed: 7 VII 2023].

78 By the beginning of July, it is likely that around one-quarter (500-600) of the mercenaries had been withdrawn from CAR. See: J. Yongo, *Central African Republic says Wagner troop movement is rotation not departure*, Reuters, 8 VII 2023, https://www.reuters.com/world/africa/central-african-republic-says-wagner-troop-movement-is-rotation-not-departure-2023-07-08/ [accessed: 8 VII 2023].

79 G. De Vries, *The Russian Ministry of Defense forces the countries at the Army 2023 forum to refuse to cooperate with PMC Wagner*, Savanna News, 15 VI 2023, https://savannanews.com/the-russian-ministry-of-defense-forces-the-countries-at-the-army-2023-forum-to-refuse-to-cooperate-with-pmc-wagner/ [accessed: 15 VI 2023].

80 *Russia's Prigozhin posts first video since mutiny, hints he is in Africa*, Reuters, 22 VIII 2023, https://www.reuters.com/world/africa/russias-prigozhin-posts-first-video-since-mutiny-hints-hes-africa-2023-08-21/ [accessed: 22 VIII 2023].

of the provision of military services by companies supervised by the Ministry of Defence[81].

These meetings were often attended by the GRU's deputy head of military intelligence, General Andrei Averjanov - commander of the GRU's Special Action Service (unit no. 29155), responsible for, among other things, the attempted poisoning of Sergei Skripal in the UK, interference in the US elections, and subversive activities in Europe (including the Czech Republic, Bulgaria, Moldova and Montenegro)[82]. According to media reports, it was Gen. Averjanov who devised the plan for the complete takeover of Prigozhin's African assets. This plan included, among other things, the concept of creating a Russian Expeditionary Corps of 20,000 mercenaries, with Spetsnaz soldiers at its core[83]. Arms dealer Viktor But, who is linked to the GRU and has extensive experience in military-business activities in Africa, was also to be involved in this process. Prigozhin opposed these plans, and his increased activity on the continent was an attempt to maintain contracts in progress.

The process of disintegration of the Prigozhin empire was sealed by his death in a plane crash on 23 August 2023 in the Tver region. According to the Federal Air Transport Agency, seven executives of the Wagner Group, including mercenary chief Prigozhin, military commander-in-chief Utkin and security chief Valery Chekalov, were on board the private jet Embraer Legacy 600 No RA-02795 flying from Moscow to Saint Petersburg. All passengers and a crew of three were killed. On 27 August, the Russian Investigative Committee said that genetic tests had confirmed the presence of Prigozhin and Utkin among the victims[84].

The elimination of the Wagner Group's leadership is linked to the failed mutiny carried out on the night of 23/24 June 2023 and was beneficial to the Russian army and Putin himself. By taking personal revenge, the president strengthened his position, stabilised a system of power based on fear, and sent a clear message to

---

[81] *ЧВК «Вагнер» предложила бойцам найти другую работу из-за конкуренции с Минобороны и Росгвардией в Африке и на Ближнем Востоке*, Важные истории, 30 VIII 2023, https://storage.googleapis.com/istories/news/2023/08/30/chvk-vagner-predlozhila-boitsam-naiti-druguyu-rabotu-iz-za-konkurentsii-s-minoboroni-i-rosgvardiei-v-afrike-i-na-blizhnem-vostoke/index.html [accessed: 30 VIII 2023].

[82] M. Schwirtz, *Top Secret Russian Unit Seeks to Destabilize Europe*, The New York Times, 8 X 2019, https://www.nytimes.com/2019/10/08/world/europe/unit-29155-russia-gru.html [accessed: 8 X 2019].

[83] *Putin Moves to Seize Control of Wagner's Mercenary Empire*, Bloomberg, 31 VIII 2023, https://www.bloomberg.com/news/articles/2023-08-31/russia-moves-to-seize-control-of-wagner-empire-after-yevgeny-prigozhin-s-death#xj4y7vzkg [accessed: 31 VIII 2023].

[84] *Russia says genetic tests confirm Prigozhin died in plane crash*, Reuters, 27 VIII 2023, https://www.reuters.com/world/europe/russias-investigators-confirm-wagner-mercenary-chief-prigozhin-died-plane-crash-2023-08-27/ [accessed: 27 VIII 2023].

potential rebels. Strengthening his authority was important in the face of the lack of progress on the Ukrainian front, the fall in the value of the rouble and the prospect of presidential elections in 2024 Prigozhin's rebellion, whatever its fate, highlighted to the Russian power elite the weakness of Putin's system, which does not guarantee their security and revenues[85].

Prigozhin's funeral was a closed one. It took place on 29 August at the Porokhov cemetery in Saint Petersburg without military ceremonies. Putin did not attend the ceremony, but only publicly referred to an acquaintance with Prigozhin dating back to the 1990s. He characterised his protégé as a person who had a "difficult fate" and "made serious mistakes". However, he emphasised Prigozhin's "loyalty, right up to his death" and "merits for the common cause"[86]. The authorities kept it a secret until the last minute when and where the mercenary chief would be buried. The protocol for the event was agreed between the Kremlin and the FSB. It was decided that the funeral would not be open so as not to create the myth of Prigozhin as a martyr. One FSB official was said to have stated that (…) *Prigozhin was a hero of the people, and we don't need heroes who marched on Moscow*[87].

In order to mask the Kremlin's probable involvement in the elimination of the rebel, Russian disinformation channels spread lies suggesting that Western and Ukrainian special services were responsible for Prigozhin's death and that they had carried out a 'terrorist attack'[88]. However, even the Russians themselves do not believe this. According to a poll conducted by the Levada Centre[89], only 14% of Russians agree with the Kremlin's official narrative line. The majority of respondents (26%) called the incident in the Tver region a tragic accident, and 20% outright believe that Prigozhin was murdered by the authorities for his so-called march of justice on Moscow. These reports were denied by Kremlin spokesman Peskov,

---

[85] A. Legucka, F. Bryjka, *Konsekwencje śmierci Jewgienija Prigożyna* (Eng. Consequences of the death of Yevgeny Prigozhin), PISM, 24 VIII 2023, https://www.pism.pl/publikacje/konsekwencje-smierci-jewgienija-prigozyna [accessed: 24 VIII 2023].

[86] *Putin breaks silence over Prigozhin's reported death*, BBC, 24 VIII 2023, https://www.bbc.com/news/world-europe-66609678 [accessed: 26 I 2024].

[87] '*We don't need heroes who marched on Moscow': Kremlin and FSB decided to bury Yevgeny Prigozhin secretly, without military honors*, Meduza, 30 VIII 2023, https://meduza.io/en/news/2023/08/30/we-don-t-need-heroes-who-marched-on-moscow-kremlin-and-fsb-decided-to-bury-yevgeny-prigozhin-secretly-without-military-honors [accessed: 30 VIII 2023].

[88] *DISINFO: The West is behind the terrorist attack on Prigozhin*, EUvsDisinfo, 29 VIII 2023, https://euvsdisinfo.eu/report/the-west-is-behind-the-terrorist-attack-on-prigozhin [accessed: 29 VIII 2023].

[89] *Запомнившиеся события августа, смерть Пригожина*, Левада Центр, 1 IX 2023, https://www.levada.ru/2023/09/01/zapomnivshiesya-sobytiya-avgusta-smert-prigozhina/ [accessed: 1 IX 2023].

describing them as "absolute lies"[90]. In contrast, 16% of respondents are supporters of conspiracy theories (spread, among others, on Telegram by channels linked to the Wagner Group) suggesting that Prigozhin "lives somewhere in Africa" and that the plane crash was staged. Almost one-quarter of respondents (22%) found it difficult to respond. One factor contributing to the resistance to Kremlin disinformation in this particular case may be the high support for Prigozhin's actions, which stood at 39% in August 2023[91].

The death of the head of the mercenaries and their commander led to profound changes in the leadership of the Wagner Group and put the future of this armed formation in question. According to channels linked to the Wagnerists, after Prigozhin's death, the command was taken over by Anton Yelizarov aka Lotos - the Spetsnaz officer under whose command the Wagnerists had captured Soledar[92]. He was dismissed from the army for falsifying documents. Potential successors to Prigozhin and Utkin included those in charge of military, business and political operations in Africa (Vitaly Perfilyev, Dmitry Sytyi, Maksim Shugaley), as well as from the top command, such as Alexander Kuznetsov aka Ratibor or Andrei Bogatov aka Brodyaga. Other sources indicated that the Wagner Group's assets were managed by Prigozhin's son Pavel[93].

After Prigozhin's death, about a third of the Wagner camp in Osipovichi, Belarus, was liquidated[94]. Part of the Belarusian contingent was redeployed to Africa and the rest returned to Russia. According to Ukrainian military intelligence, at most 1,000 Wagnerists remain in Belarus, 200-500 of them as instructors[95]. It cannot be ruled out that they will eventually be officially recruited into the Belarusian army as trainers. At the end of December 2023, unconfirmed information also emerged indicating that the Wagnerists had been placed in a new special forces unit

---

[90] *Песков опроверг утверждения о причастности Кремля к крушению самолета Пригожина*, Интерфакс, 25 VIII 2023, https://www.interfax.ru/russia/917796 [accessed: 25 VIII 2023].

[91] *Запомнившиеся события августа, смерть Пригожина…*

[92] *Anton Yelizarov from "Wagner". He commanded the offensive on Soledar, killing many of Ukrainian soldiers*, Molfar, https://molfar.com/en/blog/komanduvav-nastupom-na-soledar-vbiv-bagato-nashih-deanon-ielizarova-z-vagnera [accessed: 26 I 2024].

[93] M. Droin, T. Dolbaia, *Post-Prigozhin Russia in Africa. Regaining or Losing Control?*, Center for Strategic and International Studies, 20 IX 2023, https://www.csis.org/analysis/post-prigozhin-russia-africa-regaining-or-losing-control [accessed: 20 IX 2023].

[94] *Satellite Images Show Wagner Camp In Belarus Being Dismantled*, Radio Free Europe/Radio Liberty, 24 VIII 2023, https://www.rferl.org/a/belarus-satellite-images-wagner-camp-dismantled/32563104.html [accessed: 24 VIII 2023].

[95] *В Білорусі лишилось менше 1000 терористів з «пвк «вагнер»*, Центр Національного спротиву, 18 IX 2023, https://sprotyv.mod.gov.ua/v-bilorusi-lyshylos-menshe-1000-terorystiv-z-pvk-vagner/ [accessed: 18 IX 2023].

of the internal army, 'Tarnada' (English: Tornado), which was created to combat sabotage and reconnaissance groups and illegal armed groups[96]. Some of them may also be offered jobs in Africa by the Belarusian military company Guard Service, which is linked to Lukashenko's close associate Viktor Sheyman[97].

At the beginning of November 2023 Kartapolov stated that the Wagner Group had been fully dissolved[98]. Its assets are being taken over by companies controlled by the Ministry of Defence (mainly Redut and Africa Corps). However, their operational activity in Africa is based (at least in part) on the Wagner Group's infrastructure and human resources. Former Wagnerists are also returning to the Ukrainian front, where they are fighting, among others, in the Avdiyivka and Bakhmut areas[99] in the structures of the DNR's International Brigade (the so-called Fifteen) and the Rosgvardia, including the Chechen specnaz "Akhmat" (Kamerton unit)[100]. Supervision of the 'volunteer formations' - as the Russian authorities euphemistically refer to the semi-private military companies fighting in Ukraine - is exercised by Andrei Troshev aka Sedoy (English: grey-haired), who for years was Utkin's deputy and chief of staff of the Wagner Group[101]. He had previously served as a liaison officer between the Wagnerists and the Kremlin and the Russian army. He also managed the Liga association of veterans, which was one of the channels for recruitment. Troshev did not support Prigozhin's rebellion and, together with a group of ten Wagner Group commanders, signed a contract with the Ministry of Defence[102] and the military company Redut co-financed by Gennady Timchenko and Oleg Deripaska.

---

[96] *Najemnicy z Grupy Wagnera zasilili białoruski specnaz* (Eng. Wagner Group mercenaries reinforced Belarusian specnaz), Belsat, 16 XII 2023, https://belsat.eu/pl/news/16-12-2023-najemnicy-z-grupy-wagnera-zasilili-bialoruski-specnaz [accessed: 26 I 2024].

[97] *Вагнерівці, які підписали контракт з білоруською ПВК, відправляють в Африку*, Центр Національного спротиву, 12 IX 2023, https://sprotyv.mod.gov.ua/vagnerivtsi-yaki-pidpysaly-kontrakt-z-biloruskoyu-pvk-vidpravlyayut-v-afryku/ [accessed: 12 IX 2023].

[98] *Картаполов заявил об окончательном расформировании ЧВК «Вагнер»*, РБК, 2 XI 2023, https://www.rbc.ru/politics/02/11/2023/6543d4389a794741e8fa258e [accessed: 3 XI 2023].

[99] А. Степура, *Колишні бійці «Вагнера» справді перебувають на Бахмутському напрямку, це психологічна операція*, Суспільне Новини, 27 IX 2023, https://suspilne.media/581703-kolisni-bijci-vagnera-spravdi-perebuvaut-na-bahmutskomu-napramku-ce-psihologicna-operacia-evlas/ [accessed: 27 IX 2023].

[100] *В «Ахмате» рассказали о массовом пополнении из экс-бойцов «Вагнера»*, Риа Новости, 28 X 2023, https://ria.ru/20231028/akhmat-1905834455.html [accessed: 28 X 2023].

[101] *Встреча с Юнус-Беком Евкуровым и Андреем Трошевым*, Kremlin.ru, 29 IX 2023, https://kremlin.ru/events/president/news/72391 [accessed: 29 IX 2023].

[102] *Wagner's second-in-command Troshev sided against Prigozhin during the coup – report*, The New Voice of Ukraine, 18 VII 2023, https://news.yahoo.com/wagner-second-command-troshev-sided-015200321.html [accessed: 18 VII 2023].

Summary

Prigozhin's mutiny was the most serious manifestation of the Putin regime's instability to date. The failure of this rebellion is primarily due to the fact that it was not supported by the political elite, the power structures or part of the army. Left to their own devices, the Wagnerists were also not determined enough to achieve their goals. Although the main cause of the Wagner Group's rebellion was the conflict between the mercenary chief and the military elite, the armed march of the Wagnerists on Moscow weakened the image of the president, who had maintained close relations with Prigozhin since the 1990s. The disloyalty of a protégé who dared to form a conspiracy against the Russian state was not forgiven, and the security guarantees given to the rebel proved completely unreliable. In the two months between the mutiny and Prigozhin's death, the Russian government carried out spot purges in the army, but did not carry out a thorough personnel reshuffle. In order to stabilise the internal situation, the Rosgvardia was strengthened and some ultranationalist critics of the Kremlin and the Ministry of Defence were removed from the information space. Despite the temporary crisis, Putin's regime is strengthening and tightening the mechanisms of control and repression against opponents. It should therefore not be assumed that there will be any significant splits in the Russian power elite in the near future.

For the Wagner Group, Prigozhin's rebellion in turn proved to be the beginning of the end of its activities. The efficient takeover of Wagnerists' assets by rival military companies controlled by the Ministry of Defence and the GRU can be seen as a success allowing the government to rebuild its image after the rebellion. The division of Prigozhin's assets between several entities is most likely to prevent one company from monopolising the military services sector. Subordinating them to the Ministry of Defence will make it easier to exercise operational control over them, but will weaken Russia's ability to plausibly deny links with them. Despite the Wagnerist rebellion, according to the author, Russia will not abandon its use of semi-private armed companies in Ukraine, the Middle East or Africa. From the Polish perspective, the most important issue is the presence of Russian mercenaries in Belarus, where they may be involved in destabilising the situation on the border. Therefore, it is in Poland's interest to strengthen NATO's strategic communication on this issue. The Alliance should send a clear signal that any provocation involving the Wagner Group and their followers could be considered aggression. NATO should prepare a flexible concept of response to various forms of their actions destabilising its eastern flank and the countries of the Global South.

Bibliography

Bryjka F., *Grupa Wagnera – paramilitarne narzędzie rosyjskich operacji hybrydowych* (Eng. The Wagner Group - a paramilitary tool of Russian hybrid operations), "Sprawy Międzynarodowe" 2022, vol. 75, no. 2, pp. 68–91. https://doi.org/10.35757/SM.2022.75.2.05.

Darczewska J., *Rosgwardia. Siły specjalnego przeznaczenia* (Eng. Rosgvardia. Special purpose forces), "Punkt Widzenia OSW" 2020, no. 78.

Gabidullin M., *Wagnerowiec. Spowiedź byłego dowódcy tajnej armii Putina* (Eng. Wagnerist. Confession of a former commander of Putin's secret army), Kraków 2022.

Kuczyński G., *Wagnerowcy. Psy wojny Putina* (Eng. Wagnerists. Putin's dogs of war), Warszawa 2022.

Larsen K.P., *From mercenary to legitimate actor? Russian discourses on private military companies*, "Post-Soviet Affairs" 2023, vol. 39, no. 6, pp. 420–439. https://doi.org/10.1080/1060586X.2023.2247782.

Pokalova E., *The Wagner Group in Africa: Russia's Quasi-State Agent of Influence*, "Studies in Conflict & Terrorism", https://doi.org/10.1080/1057610X.2023.2231642.

Wojnowski M., *The genesis, theory, and practice of Russian coercive migration engineering. A contribution to the study of the migration crisis on NATO's eastern flank*, "Internal Security Review" 2022, no. 26, pp. 263–300. https://doi.org/doi:10.4467/20801335PBW.21.042.15702.

Internet sources

ABW zatrzymała 2 obywateli Rosji (Eng. ISA detained 2 Russian citizens), gov.pl, 14 VIII 2023, https://www.gov.pl/web/sluzby-specjalne/abw-zatrzymala-2-obywateli-rosji [accessed: 14 VIII 2023].

Al-Khalidi S., Gebeily M., *Syria brought Wagner fighters to heel as mutiny unfolded in Russia*, Reuters, 7 VII 2023, https://www.reuters.com/world/syria-brought-wagner-group-fighters-heel-mutiny-unfolded-russia-2023-07-07/ [accessed: 7 VII 2023].

Anton Yelizarov from "Wagner". He commanded the offensive on Soledar, killing many of Ukrainian soldiers, Molfar, https://molfar.com/en/blog/komanduvav-nastupom-na-soledar-vbiv-bagato-nashih-deanon-ielizarova-z-vagnera [accessed: 26 I 2024].

Belton C., Harris S., Miller G., *Putin appeared paralyzed and unable to act in first hours of rebellion*, The Washington Post, 25 VII 2023, https://www.washingtonpost.com/world/2023/07/25/putin-prigozhin-rebellion-kremlin-disarray/ [accessed: 25 VII 2023].

Ber J., *Od Popasnej do Bachmutu. Grupa Wagnera w wojnie rosyjsko-ukraińskiej* (Eng. From Popasna to Bachmut. Wagner's group in the Russian-Ukrainian war), OSW, 28 IV 2023, https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2023-04-28/od-popasnej-do-bachmutu-grupa-wagnera-w-wojnie-rosyjsko [accessed: 28 IV 2023].

Blakely R., *Russian mercenaries killed by US troops in Syria gun battle*, The Times, 14 II 2018, https://www.thetimes.co.uk/article/russia-mercenaries-killed-by-us-troops-in-syria-gun-battle-g5zswflfg [accessed: 19 I 2024].

Bryjka F., *Transformacja Grupy Wagnera w związku z wojną na Ukrainie* (Eng. Transformation of the Wagner Group in the wake of the war in Ukraine), PISM, 7 III 2023, https://www.pism.pl/publikacje/transformacja-grupy-wagnera-w-zwiazku-z-wojna-na-ukrainie [accessed: 7 III 2023].

Celem wagnerowców na Białorusi będzie "przejęcie Przesmyku Suwalskiego" – rosyjski deputowany (Eng. Wagnerists' goal in Belarus will be to 'take over the Suwałki Gap' - Russian MP), Belsat, 16 VII 2023, https://belsat.eu/pl/news/16-07-2023-celem-wagnerowcow-na-bialorusi-bedzie-przejecie-przesmyku-suwalskiego-rosyjski-deputowany [accessed: 16 VII 2023].

Chornogor Y., Rad P., Chernysh A., *Anatomy of "Wagner PMC": creation, war in Ukraine and ways of countering the group*, Ukrainian PRISM, April 2023, https://prismua.org/wp-content/uploads/2023/05/PMC_Wagner_eng.pdf [accessed: 28 IV 2023].

Czerep J., Legucka A., *Przyszłość "imperium" Prigożyna* (Eng. The future of Prigozhin's "empire"), PISM, 17 VII 2023, https://www.pism.pl/publikacje/przyszlosc-imperium-prigozyna [accessed: 17 VII 2023].

De Vries G., *The Russian Ministry of Defense forces the countries at the Army 2023 forum to refuse to cooperate with PMC Wagner*, Savanna News, 15 VI 2023, https://savannanews.com/the-russian-ministry-of-defense-forces-the-countries-at-the-army-2023-forum-to-refuse-to-cooperate-with-pmc-wagner/ [accessed: 15 VI 2023].

DISINFO: The West is behind the terrorist attack on Prigozhin, EUvsDisinfo, 29 VIII 2023, https://euvsdisinfo.eu/report/the-west-is-behind-the-terrorist-attack-on-prigozhin [accessed: 29 VIII 2023].

Droin M., Dolbaia T., *Post-Prigozhin Russia in Africa. Regaining or Losing Control?*, Center for Strategic and International Studies, 20 IX 2023, https://www.csis.org/analysis/post-prigozhin-russia-africa-regaining-or-losing-control [accessed: 20 IX 2023].

Dyner A.M., *Znaczenie buntu Prigożyna dla rosyjskiej polityki bezpieczeństwa* (Eng. The significance of Prigozhin's revolt for Russian security policy), PISM, 26 VI 2023, https://www.pism.pl/publikacje/znaczenie-buntu-prigozyna-dla-rosyjskiej-polityki-bezpieczenstwa [accessed: 26 VI 2023].

Dyner A.M., *Grupa Wagnera na Białorusi – potencjalne zagrożenia dla Polski* (Eng. The Wagner Group in Belarus - potential threats to Poland), PISM, 27 VII 2023, https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-potencjalne-zagrozenia-dla-polski [accessed: 27 VII 2023].

Dyner A.M., Lorenz W., Bryjka F., *Grupa Wagnera na Białorusi – konsekwencje dla NATO i UE* (Eng. The Wagner Group in Belarus - implications for NATO and the EU), PISM, 7 IX 2023, https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-konsekwencje-dla-nato-i-ue [accessed: 7 IX 2023].

Galeotti M., *Russia's coup d'état – Nature and Implications*, In Moscow's Shadows, 27 VI 2023, https://inmoscowsshadows.wordpress.com/2023/06/27/scss10-26-june-2023-russias-coup-detat-nature-and-implications/ [accessed: 27 VI 2023].

Gordon M.R. et al., *Early Intelligence Suggests Prigozhin Was Assassinated, U.S. Officials Say*, The Wall Street Journal, 24 VIII 2023, https://www.wsj.com/world/russia/wagner-prigozhin-russia-assassinated-intelligence-3e456fab [accessed: 24 VIII 2023].

Grove T., Cullison A., Pancevski B., *How Putin's Right-Hand Man Took Out Prigozhin*, The Wall Street Journal, 22 XII 2023, https://www.wsj.com/world/russia/putin-patrushev-plan-prigozhin-assassination-428d5ed8?mod=hp_lead_pos7 [accessed: 26 I 2024].

Guns for gold: the Wagner Network exposed, House of Commons Foreign Affairs Committee, 26 VII 2023, https://committees.parliament.uk/publications/41073/documents/200048/default/ [accessed: 26 VII 2023].

Harris S., Khurshudyan I., *Wagner chief offered to give Russian troop locations to Ukraine*, The Washington Post, 15 V 2023, https://www.washingtonpost.com/national-security/2023/05/14/prigozhin-wagner-ukraine-leaked-documents/ [accessed: 15 V 2023].

Hird K. et al., *Russian Offensive Campaign Assessment, March 10, 2023*, Institute for the Study of War, 10 III 2023, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-march-10-2023 [accessed: 10 III 2023].

Ivanova P., Stognei A., Seddon M., *Russian insurrection: Prigozhin's failed mutiny and the fallout*, Financial Times, 23 VI 2023, https://www.ft.com/content/34f3a349-a05f-4672-b059-6980ecc27adf [accessed: 23 VI 2023].

Jailed former 'Donetsk People's Republic' militia leader to run for president, Novaya Gazeta Europe, 31 VIII 2023, https://novayagazeta.eu/articles/2023/08/31/jailed-former-donetsk-peoples-republic-militia-leader-to-run-for-president-en-news [accessed: 31 VIII 2023].

Jawor A., *Rosyjskie służby po buncie Prigożyna. Putin wyrównuje szeregi w kremlowskich wieżach* (Eng. Russian services after Prigozhin's revolt. Putin aligns ranks in Kremlin towers), InfoSecurity24, 31 VII 2023, https://infosecurity24.pl/za-granica/rosyjskie-sluzby-po-buncie-prigozyna-putin-wyrownuje-szeregi-w-kremlowskich-wiezach [accessed: 31 VII 2023].

Journalists identify head of Wagner Group forces in Belarus as 46-year-old Ukraine native, Meduza, 26 VII 2023, https://meduza.io/en/news/2023/07/26/journalists-identify-head-of-wagner-forces-in-belarus-as-46-year-old-ukraine-native [accessed: 26 VII 2023].

Kacprzak I., *Wagnerowcy sieją zamęt na granicy. Ponad połowa Polaków uważa, że stanowią zagrożenie* (Eng. Wagnerists sow confusion at the border. More than half of Poles consider them a threat), Rzeczpospolita, 1 VIII 2023, https://www.rp.pl/spoleczenstwo/art38884031-wagnerowcy-sieja-zamet-na-granicy-ponad-polowa-polakow-uwaza-ze-stanowia-zagrozenie [accessed: 1 VIII 2023].

Kirillova K., *Propaganda and Repression Turn Against Their Creators in Russia*, The Jamestown Foundation, 25 VII 2023, https://jamestown.org/program/propaganda-and-repression-turn-against-their-creators-in-russia/ [accessed: 25 VII 2023].

Komin M., *"Fighting spirit": Russia's technocrat elite after the Wagner mutiny*, European Council on Foreign Relations, 24 VII 2023, https://ecfr.eu/article/fighting-spirit-russias-technocrat-elite-after-the-wagner-mutiny/ [accessed: 24 VII 2023].

Legucka A., *Konsekwencje buntu Prigożyna dla systemu putinowskiego w Rosji* (Eng. Consequences of Prigozhin's revolt for the Putinist system in Russia), PISM, 26 VI 2023, https://www.pism.pl/publikacje/konsekwencje-buntu-prigozyna-dla-systemu-putinowskiego-w-rosji [accessed: 26 VI 2023].

Legucka A., Bryjka F., *Konsekwencje śmierci Jewgienija Prigożyna* (Eng. Consequences of the death of Yevgeny Prigozhin), PISM, 24 VIII 2023, https://www.pism.pl/publikacje/konsekwencje-smierci-jewgienija-prigozyna [accessed: 24 VIII 2023].

Legucka A., Bryjka F., *Rywalizacja między rosyjską armią a Grupą Wagnera* (Eng. Rivalry between the Russian army and the Wagner Group), PISM, 6 VI 2023, https://www.pism.pl/publikacje/rywalizacja-miedzy-rosyjska-armia-a-grupa-wagnera [accessed: 6 VI 2023].

Mitzer S., Janovsky J., *Chef's Special – Documenting Equipment Losses During The 2023 Wagner Group Mutiny*, Oryx, 24 VI 2023, https://www.oryxspioenkop.com/2023/06/chefs-special-documenting-equipment.html [accessed: 24 VI 2023].

Najemnicy z Grupy Wagnera zasilili białoruski specnaz (Eng. Wagner Group mercenaries reinforced Belarusian specnaz), Belsat, 16 XII 2023, https://belsat.eu/pl/news/16-12-2023-najemnicy-z-grupy-wagnera-zasilili-bialoruski-specnaz [accessed: 26 I 2024].

Operacja RENGAW. Na granicy polsko-białoruskiej rozpoczyna działanie wojskowe zgrupowanie zadaniowe (Eng. Operation RENGAW. A military task force is launched on the Polish-Belarusian border), gov.pl, 12 VIII 2023, https://www.gov.pl/web/obrona-narodowa/operacja-rengaw-na-granicy-polsko--bialoruskiej-rozpoczyna-dzianie-wojskowe-zgrupowanie-zadaniowe [accessed: 26 I 2024].

Pavel Gubarev, associate of Igor Strelkov, reportedly investigated for extremism, Meduza, 23 VII 2023, https://meduza.io/en/news/2023/07/23/pavel-gubarev-associate-of-igor-strelkov-reportedly-investigated-for-extremism [accessed: 23 VII 2023].

Preiherman Y., *What Does Lukashenka's Role as Mediator in Russian Crisis Imply? – Analysis*, Eurasia Review, 29 VI 2023, https://www.eurasiareview.com/29062023-what-does-lukashenkas-role-as-mediator-in-russian-crisis-imply-analysis/ [accessed: 29 VI 2023].

Prigozhin Y., post on Telegram channel, https://t.me/concordgroup_official/1002 [accessed: 20 V 2023].

Prigozhin Y., post on Telegram channel, https://t.me/prigozhin_2023_tg/1844 [accessed: 23 VI 2023].

Prigozhin Y., post on Telegram channel, https://t.me/Prigozhin_hat/3797 [accessed: 23 VI 2023].

Putin breaks silence over Prigozhin's reported death, BBC, 24 VIII 2023, https://www.bbc.com/news/world-europe-66609678 [accessed: 26 I 2024].

Putin Moves to Seize Control of Wagner's Mercenary Empire, Bloomberg, 31 VIII 2023, https://www.bloomberg.com/news/articles/2023-08-31/russia-moves-to-seize-control-of--wagner-empire-after-yevgeny-prigozhin-s-death#xj4y7vzkg [accessed: 31 VIII 2023].

Putin says Wagner Group doesn't legally exist, Meduza, 14 VII 2023, https://meduza.io/en/news/2023/07/14/putin-says-wagner-group-no-longer-legally-exists [accessed: 14 VII 2023].

Rana M., *Volodymyr Zelensky: Russian mercenaries ordered to kill Ukraine's president*, The Times, 28 II 2022, https://www.thetimes.co.uk/article/volodymyr-zelensky-russian--mercenaries-ordered-to-kill-ukraine-president-cvcksh79d [accessed: 19 I 2024].

Russia says genetic tests confirm Prigozhin died in plane crash, Reuters, 27 VIII 2023, https://www.reuters.com/world/europe/russias-investigators-confirm-wagner-mercenary-chief--prigozhin-died-plane-crash-2023-08-27/ [accessed: 27 VIII 2023].

Russia sentences former separatist commander and pro-war blogger Igor Strelkov to four years in prison, Meduza, 25 I 2024, https://meduza.io/en/news/2024/01/25/russia-sentences-former-separatist-commander-and-pro-war-blogger-igor-strelkov-to-four-years-in-prison [accessed: 25 I 2024].

Russia's Prigozhin posts first video since mutiny, hints he is in Africa, Reuters, 22 VIII 2023, https://www.reuters.com/world/africa/russias-prigozhin-posts-first-video-since-mutiny--hints-hes-africa-2023-08-21/ [accessed: 22 VIII 2023].

Sari A., *Hybrid CoE Paper 17: Instrumentalized migration and the Belarus crisis: Strategies of legal coercion*, Hybrid CoE, 25 IV 2023, https://www.hybridcoe.fi/publications/hybrid--coe-paper-17-instrumentalized-migration-and-the-belarus-crisis-strategies-of-legal-coercion/ [accessed: 25 IV 2023].

Satellite Images Show Wagner Camp In Belarus Being Dismantled, Radio Free Europe/Radio Liberty, 24 VIII 2023, https://www.rferl.org/a/belarus-satellite-images-wagner-camp-dismantled/32563104.html [accessed: 24 VIII 2023].

Schwirtz M., *Top Secret Russian Unit Seeks to Destabilize Europe*, The New York Times, 8 X 2019, https://www.nytimes.com/2019/10/08/world/europe/unit-29155-russia-gru.html [accessed: 8 X 2019].

Serwat L., Nsaibia H., Gurcov N., *Moving Out of the Shadows: Shifts in Wagner Group Operations Around the World*, The Armed Conflict Location & Event Data Project (ACLED), 2 VIII 2023, https://acleddata.com/2023/08/02/moving-out-of-the-shadows-shifts-in-wagner-group-operations-around-the-world/#exec [accessed: 2 VIII 2023].

Sprawa Prigożyna a tuszowanie słabości Rosji i rys na jej wizerunku militarnej potęgi (Eng. The Prigozhin case and the cover-up of Russia's weaknesses and cracks in its image of military power), EUvsDisinfo, 29 VI 2023, https://euvsdisinfo.eu/pl/sprawa-prigozyna-a--tuszowanie-slabosci-rosji-i-rys-na-jej-wizerunku-militarnej-potegi/ [accessed: 29 VI 2023].

Stanyard J., Vircoulon T., Rademeyer J., *The Grey Zone: Russia's military, mercenary and criminal engagement in Africa*, Global Initiative Against Transnational Organized Crime, 16 II 2023, https://globalinitiative.net/analysis/russia-in-africa/ [accessed: 16 II 2023].

State Duma passes bill allowing Russia's National Guard troops to use heavy military equipment, Meduza, 19 VII 2023, https://meduza.io/en/news/2023/07/19/state-duma-passes-bill-allowing-russia-s-national-guard-troops-to-use-heavy-military-equipment [accessed: 19 VII 2023].

Stepanenko K., *The Kremlin's Pyrrhic Victory in Bakhmut: A Retrospective on the Battle for Bakhmut*, Institute for the Study of War, 24 V 2023, https://www.understandingwar.org/backgrounder/kremlin%E2%80%99s-pyrrhic-victory-bakhmut-retrospective-battle-bakhmut [accessed: 24 V 2023].

Stepanenko K. et al., *Russian offensive campaign assessment, January 16, 2023*, Institute for the Study of War, 16 I 2023, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-january-16-2023 [accessed: 19 I 2024].

Stognei A., Seddon M., *Yevgeny Prigozhin's 'toxic' media empire left in Kremlin limbo*, Financial Times, 14 VII 2023, https://www.ft.com/content/723a967f-213b-45b4-8ca6-792aa8e10ba0?shareType=nongift [accessed: 14 VII 2023].

Stronski P., *Implausible Deniability: Russia's Private Military Companies*, Carnegie Endowment for International Peace, 2 VI 2020, https://carnegieendowment.org/2020/06/02/implausible-deniability-russia-sprivate- military-companies-pub-81954 [accessed: 2 VI 2020].

Sukhankin S., *Russia's New PMC Patriot: The Kremlin's Bid for a Greater Role in Africa?*, The Jamestown Foundation, 1 VIII 2018, https://jamestown.org/program/russias-new-pmc-patriot-the-kremlins-bid-for-a-greater-role-in-africa/ [accessed: 12 V 2023].

Troianovski et al., *After Prigozhin's Death, a High-Stakes Scramble for His Empire*, The New York Times, 8 IX 2023, https://www.nytimes.com/2023/09/08/world/europe/prigozhin-wagner-russia-africa.html [accessed: 8 IX 2023].

Wagner Group reportedly hands over military equipment and ammunition to Russia's Defense Ministry, Meduza, 12 VII 2023, https://meduza.io/en/news/2023/07/12/wagner-group-reportedly-hands-over-military-equipment-and-ammunition-to-russia-s-defense-ministry [accessed: 12 VII 2023].

Wagner's second-in-command Troshev sided against Prigozhin during the coup – report, The New Voice Ukraine, 18 VII 2023, https://news.yahoo.com/wagner-second-command-troshev-sided-015200321.html [accessed: 18 VII 2023].

Walker S., Beaumont P., Sabbagh D., *Head of Russia's Wagner group says his troops have taken control of Soledar*, The Guardian, 11 I 2023, https://www.theguardian.com/world/2023/jan/10/head-of-wagner-group-says-his-troops-have-taken-control-of-soledar [accessed: 1 I 2024].

'We don't need heroes who marched on Moscow': Kremlin and FSB decided to bury Yevgeny Prigozhin secretly, without military honors, Meduza, 30 VIII 2023, https://meduza.io/en/news/2023/08/30/we-don-t-need-heroes-who-marched-on-moscow-kremlin-and-fsb-decided-to-bury-yevgeny-prigozhin-secretly-without-military-honors [accessed: 30 VIII 2023].

Weiss M., *Russia's Spies Say Putin Faces More Coups*, The Insider, 20 VII 2023, https://theins.ru/en/politics/263596 [accessed: 20 VII 2023].

Weiss M., Vaux P., *The Company You Keep: Yevgeny Prigozhin's Influence Operations in Africa*, Free Russia Foundation, Washington 2020, https://www.4freerussia.org/wp-content/uploads/sites/3/2020/09/The-Company-You-Keep-Yevgeny-Prigozhins-Influence-Operations-in-Africa.pdf [accessed: 16 II 2023].

'Welcome to hell' Prigozhin reappears in Belarus, rallying Wagner Group mercenaries for future work in Africa (but not yet in Ukraine), Meduza, 19 VII 2023, https://meduza.io/en/feature/2023/07/19/welcome-to-hell [accessed: 19 VII 2023].

Yevgeny Prigozhin reportedly dissolving Patriot Media Group, home of his 'troll factory', Meduza, 30 VI 2023, https://meduza.io/en/news/2023/06/30/prigozhin-reportedly-dissolving-patriot-media-group-home-of-his-troll-factory [accessed: 30 VI 2023].

Yongo J., *Central African Republic says Wagner troop movement is rotation not departure*, Reuters, 8 VII 2023, https://www.reuters.com/world/africa/central-african-republic-says-wagner-troop-movement-is-rotation-not-departure-2023-07-08/ [accessed: 8 VII 2023].

Żochowski P., *Rosja i Białoruś oskarżają Polskę o plany agresji* (Eng. Russia and Belarus accuse Poland of aggression plans), OSW, 24 VII 2023, https://www.osw.waw.pl/pl/publikacje/analizy/2023-07-24/rosja-i-bialorus-oskarzaja-polske-o-plany-agresji [accessed: 24 VII 2023].

Russian and Ukrainian Internet sources

В "Ахмате" рассказали о массовом пополнении из экс-бойцов "Вагнера", Риа Новости, 28 X 2023, https://ria.ru/20231028/akhmat-1905834455.html [accessed: 28 X 2023].

Вагнерівці продовжують прибувати у білорусь, Центр Національного спротиву, 22 VII 2023, https://sprotyv.mod.gov.ua/vagnerivtsi-prodovzhuyut-prybuvaty-u-bilorus/ [accessed: 22 VII 2023].

В Білорусі лишилось менше 1000 терористів з «пвк «вагнер», Центр Національного спротиву, 18 IX 2023, https://sprotyv.mod.gov.ua/v-bilorusi-lyshylos-menshe-1000-terorystiv-z-pvk-vagner/ [accessed: 18 IX 2023].

В кафе Петербурга на «творческом вечере» «военкора» Владлена Татарского (у него полмиллиона подписчиков в телеграме) произошел взрыв. Блогер погиб, Meduza, 2 IV 2023, https://meduza.io/feature/2023/04/02/v-peterburge-v-kafe-evgeniya-prigozhina-proizoshel-vzryv-vo-vremya-tvorcheskogo-vechera-voenkora-vladlena-tatarskogo-po-predvaritelnym-dannym-on-pogib [accessed: 2 IV 2023].

В Москве усилили меры безопасности, Tacc, 23 VII 2023, https://tass.ru/proisshestviya/18103225 [accessed: 23 VII 2023].

В Ростове-на-Дону рядом со штабом ЮВО выставили посты, Tacc, 23 VII 2023, https://tass.ru/bezopasnost/18103205 [accessed: 23 VII 2023].

Вагнерівці, які підписали контракт з білоруською ПВК, відправляють в Африку, Центр Національного спротиву, 12 IX 2023, https://sprotyv.mod.gov.ua/vagnerivtsi-yaki-pidpysaly-kontrakt-z-biloruskoyu-pvk-vidpravlyayut-v-afryku/ [accessed: 12 IX 2023].

Вручение генеральских погон высшему офицерскому составу, Президент Республики Беларусь, 27 VII 2023, https://president.gov.by/ru/events/vruchenie-pogon-vysshemu-oficerskomu-sostavu [accessed: 27 VII 2023].

Встреча с Юнус-Беком Евкуровым и Андреем Трошевым, Kremlin.ru, 29 IX 2023, https://kremlin.ru/events/president/news/72391 [accessed: 29 IX 2023].

Генерал Суровикин возглавил координационный комитет СНГ по вопросам ПВО Подробнее, EurAsia Daily, 10 X 2023, https://eadaily.com/ru/news/2023/09/10/general-surovikin-vozglavil-koordinacionnyy-komitet-sng-po-voprosam-pvo [accessed: 10 X 2023].

Грубо говоря, мы начали войну Как отправка ЧВК Вагнера на фронт помогла Пригожину наладить отношения с Путиным – и что такое «собянинский полк». Расследование «Медузы» о наемниках на войне в Украине, Meduza, 13 VII 2022, https://meduza.io/feature/2022/07/13/grubo-govorya-my-nachali-voynu [accessed: 13 VII 2022].

Дурова Д., *В России уже нашли нового министра обороны для Пригожина: в сети назвали имя*, Oboz.ua, 25 VI 2023, https://news.obozrevatel.com/russia/v-rossii-uzhe-nashli-novogo-ministra-oboronyi-dlya-prigozhina-v-seti-nazvali-imya.htm [accessed: 25 VI 2023].

Евгений Пригожин зарегистрировал компанию в Осиповичском районе, Reformation, 22 VII 2023, https://reform-by.cdn.ampproject.org/c/s/reform.by/evgenij-prigozhin-zaregistriroval-kompaniju-v-osipovichskom-rajone/amp [accessed: 22 VII 2023].

Жаба и Минобороны. Как поссорились Евгений Викторович с Сергеем Кужугетовичем, The Insider, 12 V 2023, https://theins.ru/politika/261683 [accessed: 12 V 2023].

Запомнившиеся события августа, смерть Пригожина, Левада-Центр, 1 IX 2023, https://www.levada.ru/2023/09/01/zapomnivshiesya-sobytiya-avgusta-smert-prigozhina/ [accessed: 1 IX 2023].

Источник: врио главкома ВКС назначили генерала Афзалова, Риа Новости, 23 VIII 2023, https://ria.ru/20230823/afzalova-1891645152.html [accessed: 23 VIII 2023].

Картаполов заявил об окончательном расформировании ЧВК «Вагнер», РБК, 2 XI 2023, https://www.rbc.ru/politics/02/11/2023/6543d4389a794741e8fa258e [accessed: 3 XI 2023].

Кто такой Сергей «Пионер» – глава «Вагнера» в Беларуси? Источник, Reformation, 19 VII 2023, https://reform.by/kto-takoj-sergej-pioner-glava-vagnera-belarusi [accessed: 19 VII 2023].

Наемники ЧВК Вагнера объявили, что закрывают свою главную базу в краснодарском Молькино, Meduza, 17 VII 2023, https://meduza.io/news/2023/07/17/naemniki-chvk-vagnera-ob-yavili-chto-zakryvayut-svoyu-glavnuyu-bazu-v-krasnodarskom-molkino [accessed: 17 VII 2023].

Обращение к гражданам России, Kremlin.ru, 24 VI 2023, https://web.archive.org/web/20230628083145/https://kremlin.ru/events/president/news/71496 [accessed: 24 VI 2023].

Песков опроверг утверждения о причастности Кремля к крушению самолета Пригожина, Интерфакс, 25 VIII 2023, https://www.interfax.ru/russia/917796 [accessed: 25 VIII 2023].

Песков подтвердил встречу Путина с Пригожиным и командирами «Вагнера» 29 июня, Интерфакс, 10 VII 2023, https://www.interfax.ru/russia/910904 [accessed: 10 VII 2023].

Против двоих боевиков ЧВК «Вагнер» в разных регионах России возбудили дела об изнасиловании 13-летних девочек, Важные истории, 30 VIII 2023, https://storage.googleapis.com/istories/news/2023/08/30/protiv-dvoikh-boevikov-chvk-vagner-v-raznikh--regionakh-rossii-vozbudili-dela-ob-iznasilovanii-13-letnikh-devochek/index.html [accessed: 30 VIII 2023].

Прошлое и будущее Пригожина. Как владелец ЧВК «Вагнер» создал свою армию – и что будет делать после мятежа, Досье, 6 VII 2023, https://dossier.center/wagner-fall/ [accessed: 6 VII 2023].

Путин поздравил российских военных с освобождением Артемовска, Тасс, 20 V 2023, https://tass.ru/politika/17804025 [accessed: 19 I 2024].

Солопов М., *Силовые ведомства прорабатывают вопрос о переподчинении полицейского спецназа «Гром» Росгвардии*, Ведомости, 4 VII 2023, https://www.vedomosti.ru/politics/articles/2023/07/04/983567-vedomstva-prorabativayut-vopros--o-perepodchinenii-politseiskogo-spetsnaza-rosgvardii [accessed: 4 VII 2023].

Степура А., *Колишні бійці «Вагнера» справді перебувають на Бахмутському напрямку, це психологічна операція*, Суспільне Новини, 27 IX 2023, https://suspilne.media/581703-kolisni-bijci-vagnera-spravdi-perebuvaut-na-bahmutskomu-napramku-ce-psihologicna-operacia-evlas/ [accessed: 27 IX 2023].

ЧВК «Вагнер» предложила бойцам найти другую работу из-за конкуренции с Минобороны и Росгвардией в Африке и на Ближнем Востоке, Важные истории, 30 VIII 2023, https://storage.googleapis.com/istories/news/2023/08/30/chvk-vagner-predlozhila-boitsam-naiti-druguyu-rabotu-iz-za-konkurentsii-s-minoboroni-i-rosgvardiei-v--afrike-i-na-blizhnem-vostoke/index.html [accessed: 30 VIII 2023].

Legal acts

Geneva Conventions for the protection of war victims of 12 August 1949 (Journal of Laws of 1956 no. 38 item 171).

Protocols Additional to the Geneva Conventions of 12 August 1949, Relating to the Protection of Victims of International Armed Conflicts (Protocol I) and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), adopted in Geneva on 8 June 1977 (Journal of Laws of 1992, no. 41, item 175).

Filip Bryjka, PhD

Political scientist and doctor of social sciences in the discipline of security sciences. Assistant professor at the Institute of Political Studies of the Polish Academy of Sciences and analyst at the Polish Institute of International Affairs in Warsaw. He specialises in the issues of hybrid threats, especially Russian disinformation and paramilitary groups. Graduate of political science at the University of Wrocław and national security at the War Studies University. Participant of international research projects on countering disinformation funded by grants from NATO Headquarters and the European Union.

Contact: bryjka@pism.pl

The crime of espionage in new terms, i.e. in light of the amendment to the Criminal Code of 17 August 2023

PIOTR BURCZANIUK

Institute of Legal Sciences,
Cardinal Stefan Wyszyński University
https://orcid.org/0000-0002-6685-8769

Internal Security Review, 2024, no. 30: 305–334

https://doi.org/10.4467/20801335PBW.24.013.19615

ARTICLE

Abstract

The study analysed the scope of changes in the criminalisation of the crime of espionage in Poland that took place with the amendment to the Criminal Code of 17 August 2023, as well as the systemic changes introduced by it in eight other laws, including the competency laws of all Polish special services. The amendments were introduced to increase the powers to combat this type of crime. The primary objective of the analysis was an attempt to answer the question of whether the scope of the changes introduced corresponds to the demands made by legal doctrine as well as practitioners involved in combating espionage in Poland, consequently adjusting the legal state to the current geopolitical situation, mainly related to aggressive non-military actions described in the doctrines of war. The analysis of the introduced changes was shown against the background of the legislative process of the indicated law, and especially the discussion that took place within its framework, without which a proper understanding of the changes would not be possible.

Keywords

espionage, intelligence activities, secret services

On 17 August 2023, the Sejm of the Republic of Poland passed the Act on amending the Act Criminal Code and certain other acts (hereinafter: the Act), which fundamentally changed the way in which the crime of espionage is criminalised in Poland. As indicated in the explanatory memorandum to the Act:

> (…) the main objective of the proposed project is the need to adapt the provisions of the Criminal Code concerning the crime of espionage to the constantly changing geopolitical situation, technological progress and constant modifications of the modus operandi of the potential perpetrators of the offences currently described in Article 130 of the Criminal Code. Also of significance is the current high threat of new open armed conflicts and aggressive non-military actions, which intensifies the undertaking of espionage activities by foreign intelligence and others[1].

In addition to the amendment of criminal provisions, by means of this act systemic changes were made in eight other acts, including the competence acts of all Polish special services. The need for changes in the penalisation of the crime of espionage and the competences and powers of the special services in this respect, aimed at the effective neutralisation of this type of crime, has been postulated for more than ten years both by the legal doctrine (including the author of this study) and by practitioners dealing with this criminal act.

The aim of this study is to analyse the scope of the changes introduced and to try to answer the question whether it is relevant to the demands being made and meets the practical problems encountered by the Polish law enforcement authorities when recognising the crime of espionage. The analysis of the course of the legislative process occupies an important place in these considerations. The discussion that accompanied it is important for the proper understanding - as a kind of authentic interpretation - of the new regulation.

Rationale for the changes

In the postulates formulated, concerning regulatory changes to the crime of espionage, it was pointed out that the manner of defining the elements of the prohibited act, contained in the previous wording of Article 130 of the *Act of 6 June 1997 - Criminal Code* (hereinafter: the Criminal Code), in many dimensions is not very

[1] Explanatory Memorandum to *the Parliamentary Draft Act on amendments to the Criminal Code and certain other acts*, print no. 3232, 17 IV 2023, https://orka.sejm.gov.pl/Druki9ka.nsf/0/F53D07E65F-8EC17AC12589B1003F2A96/%24File/3232.pdf, p. 13 [accessed: 28 VIII 2023].

accurate, often insufficient and, above all, unclear and vague. This has fostered different interpretations of the elements of this offence by the doctrine and often led to different qualification of acts by the prosecution. The just amended regulation of the crime of espionage corresponded directly to the threats to Poland's external security identified in the 1990s. They were based on the concept, developed still in the period of the Cold War, of the bipolarity of the international system, based on two opposing blocs of states competing with each other by military means. From this perspective, the scope of the elements of the prohibited act included in this provision did not correspond to the challenges associated with contemporary threats to the external security of the state, including the phenomena collectively referred to as asymmetric threats.

During the parliamentary debate on the draft act, MP Jarosław Krajewski rightly pointed out that (…) *the crime of espionage is one of the gravest crimes against the Republic of Poland, and if committed by a Polish citizen is de facto treason against our country.* (…) *This is particularly important from the perspective of the current geopolitical situation, which also changes the modus operandi of foreign intelligence services acting against our country*[2]. This geopolitical situation is also referred to in Polish strategic documents, including the *National Security Strategy of the Republic of Poland 2020*. They indicate, among other things, that:

> (…) the most serious threat is the neo-imperialist policy of the Russian Federation authorities, also implemented through military force. (…) The Russian Federation also conducts activities below the threshold of war (of a hybrid nature), carrying the risk of a conflict (including unintentional, resulting from a sudden escalation as a result of an incident, especially a military one), and also undertakes comprehensive and complex actions by non-military means (including: cyber attacks, disinformation) with the aim of destabilising structures of Western states and societies and causing divisions among allied states. It should be assumed that the Russian Federation will continue its policy of undermining the current international order, based on international law, in order to rebuild its superpower position and spheres of influence[3].

[2] Speech by Jarosław Krajewski on 13 June 2023, during the first reading of the parliamentary draft act amending the Criminal Code and certain other acts (prints 3232 and 3232-A), iTV Sejm - archive broadcasts, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?page=9#1C429C6BE7B92E29C12588FB0033AB2F [accessed: 28 VIII 2023].

[3] *National Security Strategy of the Republic of Poland 2020*, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, p. 6 [accessed: 28 VIII 2023].

Indicated in this strategy are actions below the threshold of war, also referred to as fourth-generation warfare, hybrid warfare, non-linear warfare, special warfare, asymmetric conflict as well as the Gerasimov doctrine[4]. It implies that:

> (…) the 'rules of war' themselves have changed significantly. The role of non-military methods in achieving political and strategic objectives has increased, in some cases far outstripping the effectiveness of weapons. The methods of confrontation are shifting towards the extensive use of political, economic, informational, humanitarian and other non-military measures, implemented using the protest potential of the population. All this is complemented by covert military measures, including the implementation of information countermeasures and the actions of special operations forces. The overt use of force is often used under the guise of peacekeeping and crisis management only at a certain stage, mainly to achieve ultimate success in the conflict[5].

In this concept, non-military means are not only to create and provide the conditions for the effective use of military force, but often even to replace it. The axis of the presented concept is thus the coordinated use - in order to defeat the opponent or gain an advantage over him - of the full spectrum of non-military means, including diplomatic, political, economic, technological, humanitarian and informational, while using a wide sphere of psychological and sociological influence on the population of the attacked state. It is (…) *a vision of guerrilla warfare waged on all fronts using a wide variety of tools and people: hackers, media, businessmen, information leaks and, of course, fake news and traditional conventional and asymmetric military means*[6]. Asymmetric measures of a non-military nature are therefore not only used to support military action, but are a pillar of the presented concept of new generation warfare. They are treated as an element of warfare, which is intended to create chaos by maintaining a state of permanent unrest and social tensions in the opponent, and are an assumed strategic objective aimed at achieving victory in

[4] It is named after the Chief of the General Staff of the Armed Forces of the Russian Federation, General Valery Gerasimov, who in the article *Ценность науки в предвидении* (Eng. The value of science lies in prediction) published on 27 II 2013 in the newspaper "Военно-промышленный курьер" (Eng. Military-Industrial Courier) reported on the concept of next-generation warfare. Translations in the article are from the author (editor's note).

[5] В. Герасимов, *Ценность науки в предвидении*, "Военно-промышленный курьер", 27 II 2013, https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html [accessed: 28 VIII 2023].

[6] M.K. McKew, *Doktryna Gierasimowa, czyli rosyjski sposób na wojnę: chaos, a nie bomby* (Eng. The Gerasimov doctrine, or the Russian way to war: chaos, not bombs), Onet, 6 IX 2017, https://wiadomosci.onet.pl/swiat/doktryna-gierasimowa-czyli-rosyjski-sposob-na-wojne-chaos-a-nie-bomby/svh4p0h [accessed: 28 VIII 2023].

war. At the same time, the principles of the use of military force are changed. It has been assumed that (…) *frontal clashes of large groupings of troops (forces) at the strategic and operational level are gradually becoming a thing of the past* (…) *they are being displaced by non-contact, long-range precision strikes, combined with the actions of special forces in conjunction with internal opposition forces*[7].

It is emphasised in security sciences that there is no single pattern of hybrid warfare, especially in its practical version. At most, it is possible to speak of a certain framework within which specific undertakings are implemented that are adapted to the changing circumstances and the external and internal situation of the target state. These activities involve - to varying degrees - many institutions and organs of the state in question or entities dependent on it, with the leading role of the special services being obvious. Importantly, the role of these services is not limited to information gathering, but also includes active intelligence activities known as influence operations. Information gathering, in this case, is combined with disinformation and propaganda, and sometimes with activities bearing the hallmarks of diversion and sabotage, in the form of cyberattacks, covert actions of a provocative nature, aimed at destabilising the socio-political situation or introducing chaos. Dynamic technological progress, especially in the area of communications, mass media and social media, undoubtedly facilitates such activities[8]. *Thanks to the internet and social media, it is now possible to do things that the former Soviet specialists in psychological warfare could only dream of: changing the internal politics of other countries with information alone*[9].

In the context of the described change in the modus operandi of foreign secret services, a significant problem of their qualification within the framework of the description of the elements of the espionage crime in force in Poland arose. This is

---

[7] П. Фельгенгауэр, *Добиться превосходства над остальным человечеством. Начальник российского Генштаба формулирует программу подготовки к масштабной войне* (Eng. In order to achieve superiority over the rest of humanity, the head of the Russian General Staff is formulating a programme of large-scale war preparations), Новая газета, 9 III 2019, https://novayagazeta.ru/articles/2019/03/09/79808-dobitsya-prevoshodstva-nad-ostalnym-chelovechestvom [accessed: 28 VIII 2023].

[8] See in more detail: M. Wojnowski, *Mit "wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku* (Eng. The myth of 'hybrid war'. Conflict on the territory of the Ukrainian state in the light of Russian military thought of the XIX-XXI centuries), "Przegląd Bezpieczeństwa Wewnętrznego" 2015, special issue: *Wojna hybrydowa*, p. 25; Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia* (Eng. Hybrid warfare - the challenge of the future? Selected issues), "Przegląd Bezpieczeństwa Wewnętrznego" 2015, special issue: *Wojna hybrydowa*, pp. 46–47.

[9] M.K. McKew, *Doktryna Gierasimowa*…

because the repealed regulation of Article 130 of the Criminal Code covered only four types of this crime:

- the basic type, which criminalises participation in the activities of a foreign intelligence service (Article 130 § 1),
- the qualified type, where the qualifying circumstance is providing, while participating in or acting for a foreign intelligence service, information to a foreign intelligence service, the transmission of which could cause damage to the Republic of Poland (Article 130 § 2),
- the qualified type, in which aggravated responsibility is connected with the fact of organising or directing the activities of a foreign intelligence service (Article 130 § 4),
- the privileged type, which consists in collecting, storing or entering an information system in order to obtain information for the purpose of providing it to a foreign intelligence service, or declaring readiness to act for a foreign intelligence service against the Republic of Poland (Article 130 § 3).

Legal doctrine and jurisprudence have developed a fairly unambiguous understanding of the key concepts - 'taking part in the activities of a foreign intelligence service' and 'acting for the benefit of a foreign intelligence service'. As Piotr Kardas points out:

> (…) "participation" should be understood as any form of active collaboration with a foreign intelligence service consisting in belonging to the organisational structure of the intelligence service (…) "participation" in the activities of an intelligence service means both the performance of the function of an agent or resident of a foreign intelligence service and the performance of any other function within its organisational structure, such as e.g. the function of a person who recruits collaborators, conducts training of agents, provides or prepares technical means used in the intelligence activity, collects and elaborates information, operates the so-called contact or transfer points, supplies the espionage network with materials and means used in the intelligence activity, etc.[10]

On the other hand, (…) *acting for the benefit of a foreign intelligence service means any form of active cooperation with a foreign intelligence service that does not yet take the form of functioning within its organisational structures, which can be defined as taking part in it. Acting for the benefit of a foreign intelligence service does not require the existence of an organisational link between the perpetrator and the foreign*

[10] P. Kardas, in: *Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-211a* (cz. 1) (Eng. Criminal Code. Specific part. Volume II. Commentary to Articles 117-211a (Part 1)), W. Wróbel, A. Zoll (eds.), Warszawa 2017, Article 130.

intelligence service[11]. It is important to note that from the point of view of the elements of the offence previously provided for in Article 130 § 2 of the Criminal Code, only such action in favour of foreign intelligence which took the form of providing it with the information specified in this provision was criminalised. In view of the regulatory scope of Article 130 of the Criminal Code thus drafted, an important practical problem arose with regard to the qualification of criminal behaviour which did not fulfil the cited definition of "taking part in the activities of a foreign intelligence service". This is because they did not contain elements of active cooperation with a foreign intelligence service combined with affiliation to organisational structures of this service (or such activities where such affiliation could not be substantiated by evidence, which in the case of espionage activities - conducted secretly by definition - is a practically impossible task), and which in fact took the form of 'acting for a foreign intelligence service', but were not combined with the transmission of messages to a foreign intelligence service as part of this cooperation (which was penalised by the Criminal Code), but involved the undertaking of various other types of activities, including what are referred to as influence operations, in line with the Gerasimov doctrine described above. During the debate in the Senate on the act, Senator Magdalena Kochan pointed out that:

> (…) none of us in this room can afford to underestimate Russia's special services. None of us who know, have read (…) have familiarised ourselves with the Gerasimov doctrine can afford to underestimate this doctrine and the disinformation that underpins it. We are all aware of its role during the U.S. elections, we know what role this disinformation played during Brexit, we know what enormous attention Poland probably enjoys, as the fall of the USSR did not cure Russia's great power inclinations. In view of this, and in view of the war going on right next to our border, no threats of espionage in our country can be ignored[12].

Legislative work – historical background

The discussion on the need for regulatory changes to the crime of espionage was initiated back in December 2016 by Piotr Pogonowski, then Head of the Internal

[11] Ibid.

[12] Speech by Magdalena Kochan of 26 VII 2023 during the debate at the 65th session of the Senate of the Republic of Poland of the 10th parliamentary term, https://av8.senat.pl/10Sen651 [accessed: 28 VIII 2023].

Security Agency (hereinafter: ABW). The assumptions he presented became the basis for the development of a draft amendment in the first half of 2017, in cooperation with the Minister of Justice. Firstly, it envisaged supplementing the element of the prohibited act defined in Article 130 § 1 of the Criminal Code in the form of 'taking part in the activity of foreign intelligence' with the element of 'conducting intelligence activity', defined as an activity or a set of activities undertaken, even indirectly, in the interest of a foreign state or a foreign organisation. These activities consist of the acquisition or transmission of information, the disclosure or use of which may damage the interests of the state insofar as this includes, in particular, the protection of the state's independence, territorial integrity, external and internal security, defence, foreign policy, natural or cultural heritage and scientific or economic potential, or the conduct of activities against these interests. Secondly, it provided for the introduction of the issue of so-called hybrid threats into the Criminal Code by adding definitions of the offences of state sabotage and acts of aggression. In addition, the draft provided for the criminalisation of espionage activities conducted on the territory of the Republic of Poland and not directed against it. It also assumed the addition of Article 113a to the Criminal Code, which would regulate the applicability of the Code with regard to offences committed with the use of an ICT system, regardless of the geographical location of the perpetrator or the ICT system used by him. With regard to the offence of espionage, the draft introduces a solution suggested by the author of this article[13], consisting in separating the concept of actual conduct of intelligence activities, i.e. performance of specific actions (objective element) from the concept of participation in the activities of a foreign intelligence service, understood as formal membership in the structures of this service (subjective element). Thus, the proponent has included in the presumption of punishability both the behaviour which amounts to performing certain activities in the interest of a foreign state or foreign organisation, without the need to link it directly to a structurally separate entity - the intelligence service, as well as the very membership of such structures. The presented definition of 'intelligence activities' corresponded with the so-called French model of criminalisation of espionage, shaped by the wording of Articles 411-4 and 411-5 of the Criminal Code of the French Republic. However, a negative position towards this project was presented by the National Public Prosecutor's

[13] P. Burczaniuk, *Przestępstwo szpiegostwa – rys historyczny, aktualne regulacje na tle doświadczeń praktycznych i analizy prawno-porównawczej wybranych państw* (Eng. The crime of espionage - historical background, current regulations against the background of practical experience and comparative legal analysis of selected countries), in: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, P. Burczaniuk (ed.), Warszawa 2017, pp. 106–107.

Office[14], which may have influenced the lack of continuation of the related legislative work. It was resumed on the initiative of the Parliamentary Committee for Special Services. This was mentioned during the debate in the Sejm by Marek Biernacki MP, who recalled that:

> (…) the current definition of espionage does not meet its requirements, it does not serve effectively for the action - protection of Polish interests, it does not serve the Polish state, this has been known for a long time. We also know that in our other neighbours, our partners (the French, other countries), they are working on changing these provisions, and we also started working from 2018 in the Committee for Special Services - I remind you, because this is important. We worked with the then heads of the ABW Prof. Pogonowski and Col. Loba. The prosecution and the judges also participated. Everyone showed that the bill was needed, that the law had to be amended. Suddenly, through the fault of the prosecution, the national prosecutor withdrew this draft, withdrew the work[15].

Work on regulatory changes concerning the crime of espionage was resumed by the Minister of Justice at the end of February 2022, due to the geopolitical situation caused by the armed aggression of the Russian Federation against Ukraine and the related threat to Poland's security. Developed at that time, in cooperation with the Ministry of Internal Affairs and Administration, the National Public Prosecutor's Office and the heads of the special services, the draft focused on making the offence of espionage more severe in terms of punishment, adding the stage form of preparation and introducing its unintentional form. The proposed wording of the provision of Article 130 of the Criminal Code was intended to cover with its scope the criminal activities of entities participating in the activity of foreign intelligence or other intelligence activity against the Republic of Poland. At the same time, the draft provided for the introduction of a definition of intelligence activity, understood as an activity or a set of activities undertaken in the interest of or for the benefit of a foreign state or foreign entity by a person who does not participate in foreign intelligence. These activities would consist of: 1) obtaining or transmitting information, the disclosure or use of which infringes or is likely to infringe the interest of the state in protecting its independence, territorial integrity, external and internal security, defence,

[14] Letter of 21 June 2017 no. PK I BP 0280.122.2017.

[15] Speech by Marek Biernacki on behalf of the parliamentary club on 6 VII 2023 during consideration of the Commission's report on the parliamentary draft act amendingthe Criminal Code and certain other acts (prints nos. 3232, 3232-A and 3358), iTV Sejm - archive broadcasts, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?page=2#0CD6003114C05652C12588FB0033AD73 [accessed: 28 VIII 2023].

foreign policy, international position, scientific or economic potential, or 2) carrying out disinformation or propaganda activities that infringe the interest of the state within the scope specified in item 1, aimed at destabilising the political system or the economy or exerting pressure on public authorities in order for them to undertake or abandon specific actions. Importantly, as the Minister of Justice pointed out, the concept of intelligence activities referred not only to entities emanating from a foreign state, but also to other disguised forms[16], such as companies, foundations and other organisations, formally unrelated to state structures. In addition, it was assumed that the threat of punishment for espionage would be of a preventive nature, which was to justify the clarification and setting the amount of the sanction at a very high ceiling, including life imprisonment in the qualified type. The draft also contained amendments to, inter alia, the *Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency* (hereinafter: the ABW and AW Act) and the *Act of 10 June 2016 on anti-terrorist activities* (hereinafter: the AT Act), in which the competences of the ABW concerning the prevention and combating of terrorist crime were to be extended to crimes of an espionage nature. According to the assumption of the Ministry of Justice, the draft was to be submitted as an auto--amendment to the government's draft law on amendments to the Criminal Code and certain other laws (print no. 2023), which, however, did not happen. This work was returned to in October 2022 by Deputy Minister of Justice Marcin Warchoł, who indicated: (…) *we are after arrangements between the Ministry of Justice and the Ministry of Internal Affairs and Administration. We have worked out the shape of solutions ready for parliamentary work. I hope that the Sejm will deal with them immediately. The decision on this matter is up to the Marshal of the Sejm*[17]. As announced, the proposal was to take the form of a parliamentary motion.

The materialisation of this announcement took place on 17 April 2023, when a parliamentary draft act amending the Criminal Code and certain other acts (print no. 3232) was submitted to the Marshal of the Sejm by a group of Law and Justice MPs, represented by Jarosław Krajewski. The analysis of this draft leads to the conclusion that in terms of direction it coincided with the drafts under consideration earlier, with two significant changes. Firstly, it dropped the element of conducting intelligence activities (and its definition) as a component of the prohibited act

[16] *Amendments to the Criminal Code related to threats to state security*, Ministry of Justice, 29 III 2022, https://www.gov.pl/web/sprawiedliwosc/zmiany-w-kodeksie-karnym-zwiazane-z-zagrozeniem-bezpieczenstwa-panstwa [accessed: 28 VIII 2023].

[17] M. Mikowski, *Wiceszef MS: zmiany ws. surowszych kar za szpiegostwo są już gotowe* (Eng. Deputy Minister of Justice: amendments on tougher penalties for espionage are ready), PAP, 23 X 2022, https://www.pap.pl/aktualnosci/news%2C1460354%2Cwiceszef-ms-zmiany-ws-surowszych-kar-za-szpiegostwo-sa-juz-gotowe.html [accessed: 28 VIII 2023].

of espionage. Secondly, it introduced the criminalisation of a specific type of intelligence activity consisting in disinformation, sabotage, diversion and activities of a terrorist nature. The draft was supplemented by amendments to the *Act of 11 March 2022 on the Defence of the Homeland* (hereinafter: the Homeland Defence Act), providing for a ban on photographing, filming and recording the image of objects of particular importance for the security and defence of the state, as well as of persons and movable property located in these facilities.

The Panoptykon Foundation and the Helsinki Foundation for Human Rights submitted their position on the draft, in a letter dated 16 May 2023. They criticised, first of all, the introduction in the draft of criminal liability for unintentional espionage and the penalisation of the preparation of this crime. The doubts raised in this regard probably influenced the introduction, within the framework of the first reading of the draft (13 June 2023, 77th sitting of the Sejm), of amendments removing the criminalisation of unintentional espionage and narrowing the preparation only to an act within the scope of sabotage, diversion or defined in Article 115 § 20 of the Criminal Code. The National Council of the Judiciary[18] and the Supreme Court[19] also submitted their comments to the draft, and an assessment of the impact of the regulation was provided by the Analyses Bureau of the Sejm[20].

Further parliamentary legislative work proceeded very smoothly, as already at the 78th sitting of the Sejm, on 6 July 2023, the draft was considered at second reading (accepting the majority of amendments of a legislative nature tabled by the Law and Justice parliamentary club), and on 7 July 2023, the law was passed by an overwhelming majority of votes[21]. On 28 July 2023, the act was considered by the Senate of the Republic of Poland[22] by tabling five amendments, only one of which was adopted when the Act was reconsidered by the Sejm of the Republic of Poland on 17 August 2023. The adoption of this amendment resulted in the formal re-enactment of the Act and the change of its date to 17 August 2023. The Act was signed

[18] Opinion of 16 VI 2023.

[19] Comments of the Office of Studies and Analyses of the Supreme Court of 12 June 2023 no. BSA. II.021.29.2023.

[20] Regulatory impact assessment of 22 May 2023 to print no. 3232.

[21] According to the results of vote no. 46 at the 78th sitting of the Sejm, 271 MPs were in favour of the law (all of the Law and Justice club, the majority from the Polish Coalition club and the Confederation club), 1 was against and 179 abstained (the Left club and the majority from the Civic Coalition club), https://www.sejm.gov.pl/sejm9.nsf/agent.xsp?symbol=glosowania&NrKadencji=9&NrPosiedzenia=78&NrGlosowania=46 [accessed: 28 VIII 2023].

[22] During the legislative work, the Ombudsman (letter of 19 July 2023 no. II.510.565.2023.PZ) expressed his critical position towards the Act, and the President of the Personal Data Protection Office (letter of 21 July 2023 no. DOL.401.362.2023.WL.RB) submitted his comments.

into law by President of the Republic of Poland Andrzej Duda on 28 August 2023 and entered into force on 23 September 2023, with the exception of selected provisions which entered into force on 1 October 2023.

Scope of changes to the Criminal Code

There is no doubt that the most substantively significant element of the changes covered by the adopted Act is the redefinition of the offence of espionage by giving a new wording to the entire Article 130 of the Criminal Code. All other changes covered by the adopted amendment remain in systemic relation to this very change. For this reason, the adopted law was often referred to as the anti-spying law during legislative work.

For the correct interpretation of the indicated changes, it is extremely important to conclude that all the above-described drafts, submitted in 2016-2022, assumed the necessity to introduce into the Criminal Code as an element of the criminal offence of espionage the behaviour consisting in conducting intelligence activities, while defining this concept by referring to the so-called French model. This legislative procedure was to be a remedy for the criminalisation of criminal activities related to the activity of foreign special services being an element of hybrid activities. The passed law was the first draft that did not provide for this solution. Pursuant to the finally adopted wording of the provision of Article 130 § 1 of the Criminal Code, the offence of espionage in the basic type may take the form of: taking part in the activities of a foreign intelligence service or acting on its behalf, while in both situations it must be a criminal act directed against the Republic of Poland. Therefore, from 1 October 2023, the basic type of the offence of espionage is fulfilled by conduct taking the form of active cooperation with a foreign intelligence service, consisting in belonging to its organisational structures (taking part), or any active cooperation with a foreign intelligence service, which does not yet take the form of functioning in its organisational structures (acting for its benefit), as long as these activities are directed against the Republic of Poland, i.e. threaten or violate the external or internal interests of the Polish state. Obviously, what is at issue is the potential - albeit demonstrated in a specific state of facts - possibility of causing damage to the Polish state (under the repealed wording, it was already assumed that it was not necessary to demonstrate actual damage).

The adopted solution should be assessed as a step in the right direction and a way out of the reported practical problems. The difficulty, however, is the openness of interpretation of the adopted provision, which, mainly due to the presumption of *in dubio pro reo* and the accompanying prohibition on the use of broad

interpretation in criminal law, may, in the course of consideration of individual cases by courts, encounter a narrowing understanding of the concepts used (mainly the concept of cooperation with foreign intelligence). The consequence of this will be the impossibility to criminalise a certain spectrum of behaviours recognised by the services as hybrid threats conducted by foreign special services. It seems that the definition of intelligence activities formulated in earlier drafts was less prone to such a risk, due to its higher level of definiteness.

The second fundamental change covered by the Act is a significant increase in the amount of criminal sanctions for particular types of espionage offences. As the drafters indicated in the explanatory memorandum to the Act:

> The increase in criminal sanctions is justified by the fact that, in the case of the crime of espionage, the threat of punishment is mainly intended to have a preventive value. 'Professional' spies most often analyse the criminal threat in the laws of individual countries when deciding to take the risk of conducting their activities on the territory of those countries. It is therefore justifiable to set the criminal threat at a very high level, as under this assumption, general prevention will have a more effective impact than in the case of other types of crime, where criminals do not take into account the level of the criminal threat[23].

In the Criminal Code of 1969, the offence of espionage in the basic type was punishable by imprisonment for a term of not less than 5 years or by the death penalty. In the now repealed regulation of Article 130 of the Criminal Code, the basic type of the offence of espionage was punishable by imprisonment for a term of between 1 and 10 years. On the basis of an analysis of 13 sentences passed by criminal courts in espionage cases after the entry into force of the current Criminal Code, the author of this article concluded that the sentences actually oscillate around the lower limit of the prescribed prison term. Only in three cases sentences of more than 3 years imprisonment were passed:

1) to a sentence of 4 years' imprisonment, the Regional Court in Warsaw sentenced in March 2016 the defendant to participate in the activities of the intelligence service of the Republic of Belarus against the Republic of Poland, i.e. an offence under Article 130 § 2 of the Criminal Code, in the period from an undetermined date to 17 February 2014[24];
2) to a sentence of 6 years' imprisonment, deprivation of public rights for 5 years, forfeiture of material evidence and financial gain The Military

[23] Explanatory Memorandum to *the Parliamentary Draft Act amending the Act*…, pp. 13–14.

[24] Ref. no. XVIII K 110/15.

Regional Court in Warsaw sentenced in April 2016 the defendant for taking part in foreign intelligence activities against the Republic of Poland, i.e. an offence under Article 130 § 1 of the Criminal Code[25];

3) to a sentence of 7 years' imprisonment, the Court of Appeal in Warsaw sentenced the defendant for the offence of Article 130 § 1 of the Criminal Code in November 2017[26].

At the same time, in the cases under consideration, there were four convictions with a sentence of 3 years' imprisonment[27]; a sentence of 2 years and 2 months' imprisonment[28]; a joint sentence of 1 year and 6 months' imprisonment[29]; a joint sentence of 1 year and 4 months' imprisonment; forfeiture of an object used to commit a crime and forfeiture of material evidence specified in the list of evidence[30]; a total sentence of 1 year and 2 months' imprisonment[31]; a conviction of two persons, the first to a sentence of 1 year's imprisonment with a conditional suspension of its execution for a probation period of 3 years, the second to a sentence of 1 year's imprisonment[32]; a conviction to a sentence of 6 months' imprisonment, the execution of which was conditionally suspended for a probation period of 2 years, and a fine in the amount of PLN 6,300[33].

Referring to analogous analyses, the legislator decided to significantly increase the criminal sanction for the offence of espionage in the basic type. It established it as a punishment of imprisonment for a term of not less than 5 years (up to 30 years).

In addition, the legislator in the amendment retained the two existing qualified types:

– the first, in which more severe responsibility is attached to providing, while taking part in the activities of a foreign intelligence service or acting on its behalf, to a foreign intelligence service information the transmission of which may cause damage to the Republic of Poland (Article 130 § 2).

[25] Ref. no. So 1/16.

[26] Ref. no. II AKa 269/17.

[27] Subsequently: judgment of the Military Regional Court in Warsaw of 11 April 2001, ref. no. So 24/00; judgment of the Military Regional Court in Warsaw of 3 November 2005, ref. no. So 37/05; judgment of the Regional Court in Warsaw of 22 December 2010, ref. no. VIII K 272/10; judgment of the Regional Court in Warsaw of 8 March 2019, ref. no. XII K 176/18.

[28] Judgment of the Court of Appeal in Białystok of 28 XI 2016, ref. no. II AKa 96/16.

[29] Judgment of the Regional Court in Warsaw of 11 August 2022, ref. no. XVIII K 78/22.

[30] Judgment of the Regional Court in Warsaw of 21 II 2022, ref. no. XVIII K 58/20.

[31] Judgment of the Regional Court in Gdańsk of 17 May 2005, ref. no. IV K 86/05.

[32] Judgment of the Regional Court in Katowice of 19 X 2015, ref. no. V K 141/15.

[33] Judgment of the Military Regional Court in Warsaw of 29 IV 2019, ref. no. So 5/19.

However, it significantly increased the limits of the criminal sanction, from the previous sentence of imprisonment for a term of not less than 3 years to a sentence of imprisonment for a term of not less than 8 years (up to 30 years) or life imprisonment;

– the second, in which the qualification is related to organising or directing foreign intelligence activities (Article 130 § 4). Similarly, the limits of the criminal sanction have been increased from the previous sentence of imprisonment for a term of not less than 5 years or 25 years to a sentence of imprisonment for a term of not less than 10 years (up to 30 years) or life imprisonment.

At the same time, the legislator introduced three new qualified types:

– the first, related to the aggravation of responsibility of the basic type in the situation of perpetration of the offence of espionage by a public official and a person performing territorial military service. In doing so, it provided for a criminal sanction in the form of imprisonment for a term of not less than 8 years (up to 30 years) or life imprisonment (Article 130 § 5);
– the second, in which the qualifying circumstance is the commission, during conduct falling within the basic type, of diversion, sabotage or the commission of a terrorist offence. It has provided for a criminal sanction in this case in the form of imprisonment for not less than 10 years (up to 30 years) or life imprisonment (Article 130 § 7). Significantly, in the case of this criminal act, the legislator has also provided for the criminalisation of its preparation, punishable by imprisonment from 6 months to 8 years (Article 130 § 8);
– the third, in which the qualifying circumstance is the carrying out, in the course of conduct falling within the basic type, of disinformation, consisting in the dissemination of false or misleading information with the aim of causing serious disturbance to the system or economy of the Republic of Poland, an allied state or an international organisation of which the Republic of Poland is a member, or inducing a public authority of the Republic of Poland, an allied state or an international organisation of which the Republic of Poland is a member to take or refrain from taking specific actions, punishable by imprisonment for a period of not less than 8 years (up to 30 years) (Article 130 § 9). It is clear - and this was confirmed during the debate on the Act in the Senate of the Republic of Poland[34] – that the disinformation activity described in the elements does not constitute a separate crime from

[34] Debate during the 65th session of the Senate of the Republic of Poland of the 10th parliamentary term, 26 July 2023, https://av8.senat.pl/10Sen651 [accessed: 28 VIII 2023].

espionage, but is its qualified type. Conducting disinformation is therefore an element of intelligence activity falling within the category of participating in the activities of a foreign intelligence service or activities for its benefit. It is noteworthy that this provision introduces, for the first time in the Polish legal system, the concept of disinformation - which has so far been used mainly in the security sciences - with a simultaneous attempt to construct a definition of activities falling within the scope of its conduct. However, it should be clearly emphasised that the scope of this definition falls within the colloquial understanding of the term. According to the dictionary understanding, disinformation is 'to mislead by giving false information'[35]. This understanding, in Article 130 § 9 of the Criminal Code, has been narrowed down by the legislator by the notion of a public purpose connected with causing serious disturbance to the system or economy of the Republic of Poland, an allied state or an international organisation, or inducing a public authority of the Republic of Poland, an allied state or an international organisation of which the Republic of Poland is a member to take or refrain from taking certain actions. In this context, it should be added that two regulatory approaches to the issue of disinformation are evident in the European Union: horizontal (e.g. Malta) - prohibiting the dissemination of disinformation in any context as long as there is a threat of public harm, and vertical (e.g. Hungary and France) - combating disinformation only in specific areas, e.g. during the electoral process. Two models of liability are also applied - criminal (e.g. Malta) or administrative (e.g. France). Thus, the solution adopted in the Criminal Code duplicates the model of horizontal regulation (albeit narrowed - constituting an element of intelligence activity) with the adopted criminal type of responsibility.

Within the framework of the privileged types, the legislator has retained the previously occurring variant of the offence of espionage, which consists of collecting, storing or entering an information system in order to obtain messages with a view to providing them to foreign intelligence, or reporting a readiness to act for foreign intelligence against the Republic of Poland (Article 130 § 3).

In addition to the aforementioned privileged type, the legislator added a new type of espionage, consisting in taking part in activities of a foreign intelligence service not directed against the Republic of Poland, conducted on its territory without the consent of a competent body granted under separate regulations, punishable by imprisonment from 6 months to 8 years. This is a significant regulatory change with

[35] *Słownik języka polskiego PWN* (Eng. PWN Dictionary of the Polish Language), vol. 1, M. Szymczak (ed.), Warszawa 1999, p. 365.

regard to the offence of espionage, as previously the Criminal Code did not penalise activity consisting in taking part in activities of foreign intelligence not directed against the Republic of Poland, i.e. not threatening or violating the external or internal interests of the Polish state. During the debate on the draft, as an example of such activities, Minister Stanisław Żaryn pointed to activities of a foreign intelligence service conducted on the territory of the Republic of Poland focusing on the recognition of a national minority originating from that country[36]. It should be noted that the legislator introduced into the regulation in question a peculiar counter-type, excluding criminal liability of persons participating in the activities of foreign intelligence, covered by the so-called primary consent of an authorised body. These authorities include the Head of the ABW and the Head of the Military Counterintelligence Service (hereinafter: SKW), as well as the Head of the Foreign Intelligence Agency (hereinafter: AW) and the Head of the Military Intelligence Service (hereinafter: SWW). As indicated in the explanatory memorandum to the draft act (…) *a necessary condition for the issuance of such consent will be that the Head of the relevant service obtains information on the objectives and course of the activity conducted and that such activities are not harmful to the interests of the Republic of Poland*[37]. With regard to the issuance of primary consent, several important issues should be noted. Firstly, the legislator narrowed the elements of the offence specified in Article 130 § 6 of the Criminal Code exclusively to taking part in the activity of a foreign intelligence service not directed against the Republic of Poland conducted on its territory. This was confirmed in the terms of expressing this consent, providing in Article 8a, Section 1 of the ABW and AW Act and in Article 9a of the *Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service* (hereinafter: the SKW and SWW Act) that the heads of these services may grant consent for participation in foreign intelligence activity conducted on the territory of the Republic of Poland in a situation where it is conducted by an organ or service of another state, guided by the premise of not infringing the interest of the Republic of Poland indicated in these provisions. The formulation constructed in this way means that both the privileged type itself and, consequently, the primary consent do not cover conduct consisting in acting for the benefit of foreign intelligence. Secondly, the use of the phrase "taking part in the activity of foreign intelligence services"

[36] Statement of 14 VI 2023 by Stanisław Żaryn, Secretary of State in the Chancellery of the Prime Minister, Government Plenipotentiary for the Security of the Information Space of the Republic of Poland, during the meeting of the Extraordinary Committee for Changes in the Codifications considering the draft law, iTV Sejm - archive broadcasts, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?rok=2023&month=06&page=5#D535320871BCC086C12589CC00473889 [accessed: 28 VIII 2023].

[37] Explanatory Memorandum to *the Parliamentary Draft Act amending the Act*…, p. 14.

in the description of the attributes causes a clear distinction between the primary consent and the subsequent consent referred to in Article 22b(2a) of the ABW and AW Act and Article 27a(2a) of the SKW and SWW Act, which were added by the act. When interpreting these regulations linguistically, it is clearly stated that the primary consent may be granted with regard to the activity of foreign intelligence conducted on the territory of the Republic of Poland if it does not infringe upon the interest of the Republic of Poland, whereas the subsequent consent may be granted only in the situation when such activity is conducted by intelligence of an allied state (more about which later in this article). The obvious result of the linguistic interpretation in this respect is in conflict with the content of the justification to the draft act, in which it is indicated that (…) *the draft also allows for the possibility of conducting on the territory of the Republic of Poland by allied services activities not aimed at the interests of Poland*[38]. Adopting the reasoning presented in the explanatory memorandum would, however, stand in clear contradiction to the fundamental principle of the prohibition of synonymous interpretation[39], with the result that the only acceptable understanding of the norm is the result of linguistic interpretation presented. Thus, in the case of primary consent, the heads of services authorised to give consent are not subjectively limited to allied services only, and the only premise they must be guided by is the potential effect of not infringing, by such activity, the interest of the Republic of Poland. Thirdly, in the context of the wording of the above-mentioned premise, the possibility of withdrawal of the granted consent by the service that issued it in the situation of ascertaining the occurrence of potential infringement of the interest of the Republic of Poland in the course of conducting the activity of a foreign intelligence service also seems obvious. The service issuing the consent is thus forced to constantly monitor intelligence activities. This may, however, be difficult, as this consent lacks solutions analogous to follow-up consent in the form of, inter alia, (…) *ongoing information on the scope of the intelligence activities conducted*. As it seems, this differentiation indicates a certain oversight on the part of the legislator. Withdrawal of consent is also connected with the risk of criminal liability for a person who, despite its withdrawal, continued intelligence activities currently assessed as interfering with the interests of the Republic of Poland. Fourthly, the request for primary consent must precede the initiation of the person's participation in the foreign intelligence activity and must be made not by the person but by an authority or service of another state, through bilateral contacts between the services. That authority or service, through the same contacts, should be informed of the withdrawal of consent.

[38] Ibid.

[39] The prohibition on attributing the same meaning within an act or branch of law to different phrases and concepts.

The authority or service requesting consent must be covered by the consent to cooperate referred to in Article 8 of the ABW and AW Act and Article 9 of the SKW and SWW Act[40]. It should be noted that, on the one hand, Article 130 § 6 of the Criminal Code speaks of consent to the activity of foreign intelligence, however, it follows from Article 8a(1) of the ABW and AW Act and Article 9a(1) of the SKW and SWW Act that the heads of the services grant consent to participate in the activity of foreign intelligence. In view of the above, these provisions should be read comprehensively - in such a way that an authority or service of another state, while requesting consent for a specific intelligence activity, at the same time indicates the persons participating in it. The consent given thus assumes a concretised character in relation to the intelligence activity in question and an individualised character in relation to the persons involved. The lack of individualised character of consent would exclude its counter-typical understanding in the context of the principle of individualisation of criminal liability expressed in Article 21 of the Criminal Code. An authority or service of another state should inform the person who is to take or is taking part in their intelligence activity of the issue of consent or its withdrawal.

In addition to giving new wording to Article 130 of the Criminal Code, the amendment also introduced other changes to the Criminal Code. Firstly, the rules for the application of the criminal measure in the form of deprivation of public rights have been modified, which, in accordance with the added Article 40 § 3, in the event of conviction for the crime of espionage as defined in Article 130 § 1-5 or 7-9, will be imposed by the court on an obligatory basis. This is a significant regulatory novelty with regard to the application of this criminal measure, which was previously adjudicated solely on the basis of the judge's optional discretion, after fulfilling the conditions set out in Article 40 § 2 of the Criminal Code. Secondly, by the addition of the new Article 112a of the Criminal Code, the previous - set out in Article 112 of the Criminal Code - principles of the absolute application of the Polish Criminal Law were extended. According to its wording, the Polish Act will apply, irrespective of the provisions in force in the place where the offence is committed, to a Polish citizen and a foreigner in the event of committing an offence by means of an IT system, an ICT system or an ICT network, if the act in the territory of the Republic of Poland has had or could have had the effect of prejudicing the interest of the state in protecting its independence, territorial integrity, external and internal security, defence, foreign policy, international position or scientific or economic potential. The amendment thus goes beyond the crime of espionage, extending its scope of application to all acts prosecuted in the Polish legal order,

[40] The indicated provisions under the Act have been extended to include the possibility of cooperation with international organisations.

committed in the manner indicated therein, i.e. with the use of an IT system, an ICT system or an ICT network, if the act may have had or has had an effect infringing one of the state interests indicated therein[41].

The last of the changes introduced by the Act to the Criminal Code gives new wording to Article 131 of the Criminal Code regulating the institution of active repentance, excluding, in strictly defined situations, the punishability of perpetrators of certain offences of foreseeable lower harmfulness. However, this is a purely consequential change, related to the addition of new types of offences in Article 130 of the Criminal Code.

Scope of amendments to other laws

As indicated at the outset, in addition to amending the criminal provisions, eight laws were amended by means of the Act to, notably to the competency laws of all Polish special services. Most of these changes are a direct consequence of the redefinition of the wording of the crime of espionage and are mainly related to the increased powers of the services responsible for combating these crimes.

Article 130 § 6 of the Criminal Code introduced, as already mentioned, a peculiar counter-type, excluding criminal liability of persons taking part in the activity of foreign intelligence, covered at the same time by the consent of an authorised body. Through amendments consisting in the addition of Article 8a in the ABW and AW Act and Article 9a in the SKW and SWW Act, the Head of the ABW, the Head of AW and the Head of the SKW and the Head of the SWW were authorised to give such consent. In the case of the Head of the ABW and the Head of the AW, the only prerequisite considered for such consent is the possible infringement by such activity of the interest of the Republic of Poland within the scope defined in Article 112a of the Criminal Code, i.e. within the scope of protection of independence, territorial integrity, external and internal security, defence, foreign policy, international position or scientific or economic potential. In the case of the Heads of the SKW and SWW, such a premise is the absence of a possible finding of a breach of state defence, security and combat capability of the Polish Armed Forces or organisational units of the Ministry of National Defence. Moreover, each of the Heads has been obliged to keep a register of consents issued by them and to provide the other Heads with information collected in the register kept by them in order to perform their tasks concerning the expression

[41] The manner in which Article 112a was introduced into the Criminal Code was criticised by the Ombudsman, as expressed during legislative work in the Senate of the Republic of Poland (letter of 19 July 2023, no. II.510.565.2023.PZ).

of the consent in question. In this way, the register is intended to perform the coordination function of the services in the process of granting such consent.

The analysed Act also introduced very important modifications to the powers of the ABW, granted to it in 2016 by the AT Act. Under it, the ABW gained a number of powers directed at preventing, counteracting and combating terrorist incidents, set out primarily in Chapter 2 (*anti-terrorist activities preventing terrorist incidents*) – which concern, among others, under Article 9 of that Act, carrying out so-called covert operations against foreigners, and in provisions then added to the ABW and AW Act, including Article 22b (on the secret cooperation with the ABW of a perpetrator of an espionage offence or a suspected perpetrator of a terrorist offence nature), Article 32a (concerning the assessment by the ABW of the security of information and communication systems), Article 32b (concerning the provision, at the request of the Head of the ABW, of information on the construction, functioning and principles of operation of information and communication systems) and Article 32c (concerning the blocking of the availability in an information and communication system of specific information data or information and communication services connected with an event of a terrorist nature). The anti-espionage law analysed extended all the powers indicated, beyond the hitherto exclusive area of terrorist offences, also to the crime of espionage[42]. As indicated in the explanatory memorandum to the draft act, (…) *the adoption of* [this] *legal solution is necessary due to the need to minimise the impact of adverse effects in the regulated matter arising as a result of the armed conflict in Ukraine, in particular the significantly increased activity of intelligence activities directed against Poland by the services of the Russian Federation and Belarus*[43].

As a result of the above changes, according to Article 9(1) of the AT Act, in order to recognise, prevent, combat and detect terrorist offences or the offence of espionage and to prosecute their perpetrators, the Head of the ABW may order, for a period not exceeding 3 months, an undercover operation to be carried out against a person who is not a citizen of the Republic of Poland and in relation to whom there is a concern as to the possibility of his/her conducting terrorist activities or committing a crime of espionage, which may include:

1) obtaining and recording the content of conversations conducted with the use of technical means, including by means of telecommunications networks;

[42] The scope of the amendments in question prompted the Legislative Bureau of the Sejm to submit a proposal to amend the title of the AT Act by extending its material scope to include the offence of espionage. However, the MPs did not approve the proposal.

[43] Explanatory Memorandum to *the Parliamentary Draft Act amending the Act*…, p. 15.

2) obtaining and recording the image or sound of persons from premises, means of transport or places other than public places;
3) obtaining and recording the content of correspondence, including correspondence conducted by means of electronic communication;
4) obtaining and recording data contained on computer data carriers, telecommunication terminal equipment, information and data communication systems;
5) gaining access to and controlling the content of consignments.

Analysing the wording of the provision of Article 22b of the ABW and AW Act, it should be pointed out that, as of 2 July 2016, it provided for the possibility of the Head of the ABW (on the basis of the SKW and SWW Act - the Head of the SKW), where it is justified by reasons of state security, to waive the obligation to notify the competent prosecutor of a justified suspicion that a crime has been committed and of a person who, according to the information or materials obtained by the ABW (SKW), may be its perpetrator, if the information or materials obtained by the ABW (SKW) in the course of performing the tasks referred to in Article 5(1) of the ABW and AW Act (in Article 5(1) of the SKW and SWW Act), indicate the commission of an offence of espionage or make it probable that an activity aimed at committing a terrorist offence has been committed. By virtue of the amended Act, this entitlement has been extended, by sec. 2a added to Article 22b of the ABW and AW Act, by the possibility of this waiver, also in the case of the perpetrator of the offence referred to in Article 130 § 6 of the Criminal Code (i.e. espionage not directed against the Republic of Poland), when the intelligence of an allied state in whose activities the person participated - firstly, discloses the circumstances of the committed act or the conducted activity; secondly, undertakes to continue to conduct it within the framework of secret cooperation with the ABW or to provide current information on the scope of activities conducted by this intelligence - obtaining a subsequent consent in accordance with the principles set forth in Article 8a. The same power was also obtained, by virtue of paragraph 2a added to Article 27a of the SKW and SWW Act, by the Head of the SKW. The legislator did not provide for the possibility of granting the indicated subsequent consent by the Heads of the AW and the SWW, although they grant the primary consent. As it seems, this is a deliberate procedure, as the sequence of events described in the normatively indicated provisions de facto concerns the situation of recognition by the Polish counterintelligence service, i.e. the ABW or the SKW, of persons participating in activities of foreign intelligence services not directed against the Republic of Poland, but conducted in the territory of the Republic of Poland, to whose activities, prior to the formal institution of preparatory proceedings, the intelligence service of an allied state, which is behind these activities, admits and discloses the circumstances

of the committed act or conducted activities, undertaking to continue conducting them jointly with the ABW (or SKW) or to provide current information on the scope of their activities. As it seems - the project's explanatory memorandum does not contain such information - the purpose of this regulation, which introduces a kind of 'abolitionist act', is to secure Poland's allied cooperation by giving counterintelligence services the right to 'legalise' such activities in order to pursue common strategic interests. This reasoning is confirmed by the legislature's use of the phrase 'intelligence of an allied state' and not, as in the case of the primary consent, 'foreign intelligence'. It should also be noted that the Act does not define the concept of allied state intelligence (as discussed in more detail earlier). In understanding the concept of an allied state, reference should be made to doctrinal considerations developed on the basis of the so-called reciprocity principle set out in Article 138 of the Criminal Code. As Kardas points out:

> (…) the concept of an allied state is normative in nature, related to regulations contained in acts of public international law. An allied state is a state that, under international agreements or treaties (multilateral or bilateral), has been recognised as a political and military ally of the Republic of Poland. In other words, it is a state with which the Republic of Poland has concluded a political or military alliance. Allied states of the Republic of Poland include, inter alia, all states remaining in the NATO structure since the Republic of Poland's accession to the pact[44].

Thus, primary consent may be granted for participation in the activities of a foreign intelligence service conducted on the Polish territory if this does not infringe on the interests of the Republic of Poland. The subsequent consent, on the other hand, under the same conditions, may be granted only in the situation of conducting activities by the intelligence of an allied state. This consent, similarly to the primary consent, may be withdrawn by the ABW or SKW in the situation of failure to fulfil the conditions of its granting. Its withdrawal may take place: firstly, in a situation where the conducted activity begins to infringe the interests of the Republic of Poland; secondly, when information is obtained indicating the misleading of Polish services with regard to the circumstances of the committed act or the conducted activity; thirdly, when the intelligence of an allied state ceases to conduct further activity jointly with the ABW (or SKW) or ceases to provide current information on the scope of its activities.

In addition, in accordance with the amended wording of Article 32a of the ABW and AW Act, the ABW was given the power to conduct security

[44] P. Kardas, in: *Kodeks karny*…, Article 138.

assessments of ICT systems of public administration bodies or ICT networks covered by the uniform list of objects, installations, devices and services constituting critical infrastructure, as well as ICT systems of owners, sole and dependent owners of objects, installations or devices of critical infrastructure referred to in Article 5b(7)(1) of the *Act of 26 April 2007 on crisis management*, or data processed in these systems. This power has been granted not only, as before, in order to prevent and counteract terrorist incidents and to detect and prevent terrorist offences in this area as well as to prosecute their perpetrators, but also in order to prevent and counteract events that make the commission of the offence of espionage probable and to recognise, detect and prevent the crime of espionage.

In the same scope, the Head of the ABW obtained, by virtue of the amended Article 32b of the ABW and AW Act, the power to demand from the above-mentioned entities to present information on the construction, functioning and principles of exploitation of the ICT systems held, including information containing computer passwords, access codes and other data enabling access to the system and their use, in order to respond to and prevent incidents of a terrorist nature or making it probable that an offence of espionage has been committed, concerning these systems or data, as well as to recognise, prevent and detect offences of a terrorist nature and an offence of espionage in this area and to prosecute their perpetrators.

Similarly, with regard to the offence of espionage, the possibility was extended for the Head of the ABW to apply, on the basis of Article 32c of the ABW and AW Act, for the application by the court, after obtaining the written consent of the Prosecutor General, of the so-called blocking accessibility, i.e. blocking by the service provider supplying electronic services the accessibility in the ICT system of specific IT data connected with an event of a terrorist nature or making it probable that an offence of espionage has been committed, or specific ICT services serving or used to cause an event of a terrorist nature or making it probable that an offence of espionage has been committed. This power becomes particularly important in the context of Article 130 § 9 of the Criminal Code in which the legislator directly included the activities of conducting disinformation as an element of intelligence activities. Until now, only Article 180 of the *Telecommunications Act of 16 July 2004* obliged telecommunications companies to immediately block telecommunications connections or information transmissions, at the request of authorised entities (i.e. Police, the Internal Supervision Bureau, the Border Guard, the Internal Inspectorate of the Prison Service, the State Protection Service, the Internal Security Agency, the Military Counterintelligence Service, the Military Police, the Central Anticorruption Bureau and the National Revenue Administration), if these calls could threaten the defence, state security and public safety and order, or to allow them to carry out such blocking. The amended provision in the ABW and

AW Act - going beyond the previous limitation to offences of a terrorist nature and encompassing within its scope also the offence of espionage - gives a basis for the service provider supplying electronic services to block the availability in an ICT system of specific IT data or specific ICT services, disseminating false or misleading information in order to cause serious disturbances in the system or economy of the Republic of Poland, an allied state or an international organisation of which the Republic of Poland is a member, or to induce a public authority of the Republic of Poland, an allied state or an international organisation of which the Republic of Poland is a member to take or refrain from taking specific actions.

In the context of the changes described above, it should be added that the Act also made changes to Article 32aa of the ABW and AW Act, added to it in 2018 by the *Act of 5 July 2018 on the national cybersecurity system*, obliging the ABW to implement, operate and coordinate the functioning of the early warning system for threats occurring online. Similar to the amendments discussed earlier, the purpose of operating the system has been extended - beyond preventing, countering and preventing terrorist incidents and beyond identifying, detecting and preventing terrorist offences and prosecuting their perpetrators - to preventing, countering and preventing incidents that make it likely that an espionage offence has been committed and to identifying, detecting and preventing the crime of espionage and prosecuting its perpetrators.

In addition, (…) *in order to build a coherent catalogue of sanctions, as well as preventive measures*[45], through amendments to the pension law for officers of uniformed services and professional soldiers, the crime of espionage was added to the catalogue of offences the commission of which, confirmed by a valid court judgment, by a soldier, officer or police pensioner results in the loss of pension rights.

In addition to the changes indicated, the Act introduced several additional changes to the competence acts of the special services, not directly related to the changes in the scope of the crime of espionage, being the result of the experience of the functioning of the services, such as the extension, in the case of the ABW, AW, SKW and SWW, of the authority to undertake cooperation not only with the competent authorities and services of other states, but also with international organisations.

One of these changes is particularly significant from the perspective of overall state security. This is because the Act amended the Homeland Defence Act by establishing, in Article 616a, a prohibition - without a permit - on photographing, filming or otherwise recording the picture or image of facilities of particular importance for the security or defence of the state, facilities of the Ministry of National

[45] Explanatory Memorandum to *the Parliamentary Draft Act amending the Act*…, p. 14.

Defence not recognised as facilities of particular importance for the security or defence of the state, facilities of critical infrastructure, if they have been marked with a graphic sign expressing this prohibition, and persons or movables located in these facilities. The marking of a facility with a sign prohibiting photography is to be decided by the authority competent for the protection of that facility, taking into account the risks to its security. Coupled with this prohibition is a new offence punishable by imprisonment or a fine for any person who, without authorisation, photographs, films or otherwise records an image of an object marked with a 'no photography' sign or an image of a person or movable property within such a facility.

Summary

Summing up the above considerations, it should be indicated that the Act amending the Criminal Code and certain other acts passed by the Sejm of the Republic of Poland on 17 August 2023, which significantly changed the way in which the offence of espionage is penalised in Poland, must be assessed positively. After several years of legislative work, which resulted from the demands made both by the representatives of the legal doctrine and practitioners dealing with this prohibited act, an amendment appeared, which, in principle, adjusted the provisions of the Criminal Code in this area to the current geopolitical situation, shaped mainly by the high threat of new open armed conflicts and aggressive non-military actions described in the doctrines of war. Furthermore, this amendment corresponds with the threats posed by technological advances and the described modus operandi of potential perpetrators of the crime of espionage.

It is obvious that the adopted changes, including, inter alia, the use of new notions in the attributes of criminal acts, which have not been present in the legal system so far, including many notions which are broad in meaning and susceptible to diverse interpretations, will have to be verified in terms of their effectiveness through the practice of criminal proceedings. This practice will bring an answer in particular, to the question as to whether the practical understanding of the new provisions does not, as a consequence, deprive the criminalisation of a certain spectrum of behaviours recognised by the services as hybrid threats carried out by foreign special services.

In the coming years, analyses of this effectiveness should be undertaken, based on the experience from the practice in applying the new regulations. If the legal solutions adopted prove to be ineffective, then consideration should be given to reconsidering the proposals that were made during the legislative process described above, including the definition of intelligence activities formulated at that time.

Bibliography

Burczaniuk P., *Przestępstwo szpiegostwa – rys historyczny, aktualne regulacje na tle doświadczeń praktycznych i analizy prawno-porównawczej wybranych państw* (Eng. The crime of espionage - historical background, current regulations against the background of practical experience and comparative legal analysis of selected countries), in: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia*, P. Burczaniuk (ed.), Warszawa 2017, pp. 86–107.

Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-211a (cz.1) (Eng. Criminal Code. Specific part. Volume II. Commentary to Articles 117-211a (Part 1)), W. Wróbel, A. Zoll (eds.), Warszawa 2017.

Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia* (Eng. Hybrid warfare - the challenge of the future? Selected issues), "Przegląd Bezpieczeństwa Wewnętrznego" 2015, special issue: *Wojna hybrydowa*, pp. 39–50.

Słownik Języka Polskiego PWN (Eng. PWN Dictionary of Polish Language), vol. 1, M. Szymczak (ed.), Warszawa 1999.

Wojnowski M., *Mit "wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku* (Eng. The myth of 'hybrid war'. Conflict on the territory of the Ukrainian state in the light of Russian military thought of the XIX-XXI centuries), "Przegląd Bezpieczeństwa Wewnętrznego" 2015, special issue: *Wojna hybrydowa*, pp. 7–38.

Internet sources

Amendments to the Criminal Code related to threats to state security, The Ministry of Justice, 29 III 2022, https://www.gov.pl/web/sprawiedliwosc/zmiany-w-kodeksie-karnym-zwiazane-z-zagrozeniem-bezpieczenstwa-panstwa [accessed: 28 VIII 2023].

Consideration of the Commission's report on the parliamentary draft act amending - the Criminal Code and certain other acts (nos. 3232, 3232-A and 3358), iTV Sejm - archive broadcasts, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?page=2#0CD6003114C05652C12588FB0033AD73 [accessed: 28 VIII 2023].

Explanatory Memorandum to *the Parliamentary Draft Act on amending the Criminal Code and certain other acts* (print no. 3232), https://orka.sejm.gov.pl/Druki9ka.nsf/0/F53D07E65F8EC17AC12589B1003F2A96/%24File/3232.pdf [accessed: 28 VIII 2023].

McKew M.K., *Doktryna Gierasimowa, czyli rosyjski sposób na wojnę: chaos, a nie bomby* (Eng. The Gerasimov doctrine, or the Russian way to war: chaos, not bombs), Onet, 6 IX 2017, https://wiadomosci.onet.pl/swiat/doktryna-gierasimowa-czyli-rosyjski-sposob-na-wojne-chaos-a-nie-bomby/svh4p0h [accessed: 28 VIII 2023].

Mikowski M., *Wiceszef MS: zmiany ws. surowszych kar za szpiegostwo są już gotowe* (Eng. Deputy Minister of Justice: amendments on tougher penalties for espionage are ready), PAP, 23 X 2022, https://www.pap.pl/aktualnosci/news%2C1460354%2Cwiceszef-ms-zmiany-ws-surowszych-kar-za-szpiegostwo-sa-juz-gotowe.html [accessed: 28 VIII 2023].

Recording of the meeting of the Sejm Extraordinary Committee for Amendments to the Codifications - 14 VI 2023, iTV Sejm - archive broadcasts, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?rok=2023&month=06&page=5#D535320871BCC086C12589CC00473889 [accessed: 28 VIII 2023].

Recording of the 77th sitting of the Sejm - 13 VI 2023, iTV Sejm - archive broadcasts, https://www.sejm.gov.pl/sejm9.nsf/transmisje_arch.xsp?page=9#1C429C6BE7B92E29C12588FB0033AB2F [accessed: 28 VIII 2023].

Recording of the 65th sitting of the Senate of the Republic of Poland of the 10th parliamentary term - 26 July 2023, https://av8.senat.pl/10Sen651 [accessed: 28 VIII 2023].

Vote no. 46 at the 78th sitting of the Sejm on 07-07-2023 at 19:21:18, https://www.sejm.gov.pl/sejm9.nsf/agent.xsp?symbol=glosowania&NrKadencji=9&NrPosiedzenia=78&NrGlosowania=46 [accessed: 28 VIII 2023].

Russian Internet sources

Герасимов В., *Ценность науки в предвидении*, "Военно-промышленный курьер", 27 II 2013, https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html [accessed: 28 VIII 2023].

Фельгенгауэр П., *Добиться превосходства над остальным человечеством Начальник российского Генштаба формулирует программу подготовки к масштабной войне*, Новая газета, 9 III 2019, https://novayagazeta.ru/articles/2019/03/09/79808-dobitsya-prevoshodstva-nad-ostalnym-chelovechestvom [accessed: 28 VIII 2023].

Legal acts

Act of 17 August 2023 amending the Act - Criminal Code and certain other acts (Journal of Laws of 2023, item 1834).

Act of 11 March 2022 on the defence of the homeland (consolidated text of Journal of Laws of 2024, item 248).

Act of 5 July 2018 on the national cybersecurity system (consolidated text of Journal of Laws of 2023, item 913, as amended).

Act of 10 June 2016 on antiterrorist activities (consolidated text of Journal of Laws of 2022, item 2632).

Act of 26 April 2007 on crisis management (consolidated text of Journal of Laws of 2023, item 122).

Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service (consolidated text of Journal of Laws of 2023, item 81, as amended).

Act of 16 July 2004 telecommunications law (consolidated text of Journal of Laws of 2022, item 1648, as amended).

Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency (consolidated text of Journal of Laws of 2023, item 1136, as amended).

Act of 6 June 1997 - Criminal Code (consolidated text of Journal of Laws of 2022, item 1138, as amended).

Case law

Judgment of the Court of Appeal in Białystok of 28 XI 2016, ref. no. II AKa 96/16.

Judgment of the Court of Appeal in Warsaw of 24 XI 2017, ref. no. II AKa 269/17.

Judgment of the Regional Court in Gdańsk of 17 V 2005, ref. no. IV K 86/05.

Judgment of the Regional Court in Katowice of 19 X 2015, ref. no. V K 141/15.

Judgment of the Regional Court in Warsaw of 11 VIII 2022, ref. no. XVIII K 78/22.

Judgment of the Regional Court in Warsaw of 21 II 2022, ref. no. XVIII K 58/20.

Judgment by the Regional Court in Warsaw of 8 III 2019, ref. no. XII K 176/18.

Judgment of the Regional Court in Warsaw of 23 III 2016, ref. no. XVIII K 110/15.

Judgment of the Regional Court in Warsaw of 22 XII 2010, ref. no. VIII K 272/10.

Judgment of the Military Regional Court in Warsaw of 29 IV 2019, ref. no. So 5/19.

Judgment of the Military Regional Court in Warsaw of 26 IV 2016, ref. no. So 1/16.

Judgment of the Military Regional Court in Warsaw of 3 XI 2005, ref. no. So 37/05.

Judgment of the Military Regional Court in Warsaw of 11 IV 2001, ref. no. So 24/00.

Other documents

National Security Strategy of the Republic of Poland 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [accessed: 28 VIII 2023].

Piotr Burczaniuk, PhD

Doctor of Law, Assistant Professor at the Institute of Legal Sciences of Cardinal Stefan Wyszyński University, legal counsel, legislator. He specialises in legal theory, business law and IT law.

Contact: p.burczaniuk@uksw.edu.pl

Information activities of the Russian Federation in 2023

KAROLINA KUŚMIREK

Independent author

https://orcid.org/0000-0001-6679-2088

Internal Security Review, 2024, no. 30: 335–352

https://doi.org/10.4467/20801335PBW.24.014.19616

ARTICLE

Abstract

The subject of information activities carried out by the Russian Federation was taken up as a result of the dynamic changes taking place in the security environment. Research methods from the field of scientific research methodology typical for social sciences were used to implement the undertaken research problem. The comparative method was used to juxtapose narratives. The method of content analysis included the analysis of the source material obtained from the information environment. The introduction presents information on the essence of information activities as an element of military activities. The next section of the article presents information activities that enabled the achievement of political goals both in Russia itself and on the international arena. The conclusions indicate those activities that diversified the recipients. The result of the conducted research was the identification of those information activities that allowed the Russian Federation to impose its arguments on the Russian society and in the global competition of superpowers.

Keywords

international security, Russian Federation, information activities, NATO

Introduction

The dynamic changes in the international environment that have taken place in the modern world have resulted in information becoming a weapon as effective as conventional weapons. The conduct of the Russian Federation (RF) has changed the security structure in Europe and led to the imposition of a new order. Information operations[1] of the RF were intended to influence the will of the adversary in such a way that it would interpret the situation as the Russian authorities intended and that its ability to respond would be limited[2].

The research problem undertaken makes it possible to present, using the example of the RF, the ways in which a superpower can achieve its strategic objectives and consolidate its position on the international stage using information activities.

The article analyses the various planes of influence and presents selected examples of the implementation of the RF's information activities, which introduced information chaos, led to the undermining of the legitimacy of power and lowered trust in the administration of other states. The result of the research is the identification of specific actions of the RF that influenced the change of security architecture in Europe.

The publication uses research methods typical of the social sciences. The comparative method was used in contrasting the narratives of the RF and Western states. The content analysis method involved exegesis of source material obtained from the international information environment and national documents.

Of particular relevance to the subject matter are publications on information operations [e.g. Zbigniew Modrzejewski's *Operacje informacyjne* (Eng. Information Operations)] or geopolitics (e.g. Samuel Ramani's *Putin's War on Ukraine*).

To date, there have been few scholarly publications that focus on outreach, rather than the propaganda or disinformation activities that are only part of it.

---

1 *Operacje informacyjne* (Eng. Information operations) *DD-3.10(A)*, Centrum Doktryn i Szkolenia Sił Zbrojnych Rzeczypospolitej Polskiej, Bydgoszcz 2017, p. 15; *Operacje psychologiczne (*Eng. Psychological operations) *DD-3.10.1(B)*, Centrum Doktryn i Szkolenia Sił Zbrojnych Rzeczypospolitej Polskiej, Bydgoszcz 2017, p. 13.

2 *Operacje informacyjne DD-3.10(A)*…, pp. 15–17; Z. Modrzejewski, *Operacje informacyjne* (Eng. Information operations), Warszawa 2015, in many places; *Informacyjny wymiar wojny hybrydowej* (Eng. The information dimension of hybryd warfare), M. Wrzosek et al. (sci. ed.), Warszawa 2018, pp. 183–200.

Information activities of the Russian Federation

The Russian Federation is conducting information activities in Central Europe, including in relation to the Republic of Poland (RP). It seeks to achieve strategic goals that would enable it to return to its glory days, and therefore focuses on finding gaps in its security system and testing the resistance of Polish citizens to Russian propaganda.

Russia uses information activities, including propaganda and disinformation activities, and information techniques. It uses, for example, key opinion leaders to amplify its own message, disseminates topics that are sensitive and resonate well in the news environment, such as refugees or the possibility of nuclear weapons[3].

Actions against the Republic of Poland

The Russian Federation began to intensively influence the perception of both the international community, including the Baltic states, and its own society from 2014. Back then, it portrayed Poles as mercenary soldiers at the service of Kiev's fascists. This is confirmed by the opinion expressed by Leonid Baranov, Minister of State Security of the Donetsk People's Republic, that 105 Polish mercenaries took part in the fighting in the Donbass[4]. The Russian propaganda apparatus is gradually moving away from depicting Polish mercenaries as committing reprehensible acts, such as raping local women, to depreciating the participation of Polish citizens in the Russian-Ukrainian war[5]. Such a narrative influences the perception of the audience and masks the lack of progress of the "special military operation"[6]. In addition, it is becoming a source of animosity between Ukrainians and Poles.

---

[3] L. Phillips, D. Crouch, *Have Chemical Weapons been Used in Ukraine?*, RUSI, 20 VI 2023, https://rusi.org/explore-our-research/publications/commentary/have-chemical-weapons-been-used-ukraine [accessed: 7 VII 2023]; W. Courtney, *Countering Russia's Nuclear Threat in Europe*, RAND, 20 IV 2023, https://www.rand.org/blog/2023/04/countering-russias-nuclear-threat-in-europe.html [accessed: 7 VII 2023].

[4] *ДНР заявляет о взятых в плен польских наемниках*, РИА Новости, 2 IX 2014, https://ria.ru/20140902/1022431781.html [accessed: 7 VII 2023].

[5] *СМИ сообщили об изнасиловании несовершеннолетней наемниками из Польши*, Известия, 10 II 2023, https://iz.ru/1468024/2023-02-10/smi-soobshchili-ob-iznasilovanii-nesovershennoletnei-naemnikami-iz-polshi [accessed: 7 VII 2023].

[6] The term "special military operation" is used by the Russian side to refer to the war in Ukraine, which Russia started in the Donbass in 2014 and then extended to the whole of Ukraine 24 II 2022.

The Russian Federation has been conducting propaganda activities against Poland in the international information environment. Poland was portrayed there as a state ready to realise its goals and aspirations, e.g. the appropriation of Ukraine's western lands, especially Lviv, without regard for international relations. Such fake news appeared in 2014, when attempts were made to convince the international community that Ukraine should be divided among European states and such a plan was allegedly being prepared by the European Union (EU). On the one hand, the claims of the RP were presented, while on the other hand, the dysfunction of the EU was pointed out. The aim of such actions was to arouse emotions in the public and to portray Poland as an aggressor instead of an assisting state.

Disinformation activities are conducted by the Russian Federation on a long-term basis. Russia highlights sensitive topics that become a tool for fuelling social unrest. It first tests individual messages that strike at citizens' sense of security, and then creates information campaigns out of them that undermine the credibility of state institutions and uniformed services. In this way, the state and the pillars of its security are decomposed[7].

In order to achieve the desired informational effects, the Russian Federation additionally engages public opinion leaders, including government representatives, academics and so-called useful idiots. An example is the statement by Russian historian Oleg Nazarov, who indicated that Poland was seeking to annex the western part of Ukraine.

Representatives of the Russian administration were also opinion leaders. In 2023, the head of the Foreign Intelligence Service of the Russian Federation (Служба Внешней Разведки Российской Федерации) Sergei Naryshkin echoed the narrative of Poland's desire to annex the western lands of Ukraine and, in this context, invoked the statement that Poland was the hyena of Europe[8]. In the message to its own public, Russia is portrayed as a state forced to fight for its integrity

[7] See: K. Kuśmirek, *Działania informacyjne i propagandowe Federacji Rosyjskiej na wybranych przykładach* (Eng. Information and propaganda activities of the Russian Federation with selected examples), in: *Zarządzanie informacją i wiedzą na potrzeby analiz strategicznych i operacyjnych Sił Zbrojnych RP*, J. Tarczyński, A. Lis (eds.), Warszawa–Bydgoszcz 2022, pp. 79–93; J. Fiszer, M. Fiszer, *Wojna w Ukrainie. Od napaści do kontrofensywy* (Eng. The war in Ukraine. From assault to counter-offensive), Warszawa 2023, in many places.

[8] M. Sławiński, *Szef rosyjskiego wywiadu poszedł z tym do Łukaszenki: Polska czeka na odpowiedni moment* (Eng. Russian intelligence chief went to Lukashenko with this: Poland is waiting for the right moment), Wprost, 27 VI 2023, https://www.wprost.pl/swiat/11165518/szef-rosyjskiego-wywiadu-poszedl-z-tym-do-lukaszenki-polska-czeka-na-odpowiedni-moment.html [accessed: 6 VII 2023].

and values as the West tries to destroy it. In the case of RP, there is talk of its Russophobic behaviour[9]. Such a phenomenon is called the besieged fortress syndrome.

In 2023, there was an intensification of Russian rhetoric directed against Poland. This was due to Poland's involvement in lobbying for Ukraine. Russian politician Dmitry Medvedev spread particularly hostile propaganda against, among others, the Polish President: *Polish scum named "duda" have offered to execute Russia like a rabid beast. And anyone else hoping to negotiate with such bastards? It makes no sense*[10]. Depreciating the image of the Polish President, he used the pejorative term bastard to create an alternative reality. Belarusian President Alexander Lukashenko in April 2023 accused Poland of training mercenaries for an armed uprising against the Belarusian regime. In effect, he was preparing Belarusian society for the necessity of a clash between Belarus and the West. The Republic of Poland is identified in the Belarusian information environment with the North Atlantic Treaty Organisation (North Atlantic Alliance, NATO), therefore the fight against it is a fight against the Alliance as a whole.

Prigozhin's rebellion in the Russian news environment

Yevgeny Prigozhin Head of the Wagner Group[11] began his march to the Kremlin on 24 June 2023. Its aim was to change key positions in the Russian Armed Forces and (…) *restore justice*[12]. This was the result of forcing Group members to sign contracts

[9] *Польские бизнесмены ответят за русофобию Варшавы*, ВЗГЛЯД, 14 VII 2023, https://vz.ru/politics/2023/7/14/1221118.html [accessed: 31 VII 2023].

[10] *Медведев считает, что заявления Польши подтверждают бессмысленность каких-либо переговоров*, Tacc, 27 VI 2023, https://tass.ru/politika/18100221 [accessed: 6 VII 2023]. Translations in the article are from the author (editor's note).

[11] The Wagner Group was established in 2014 as a private military company. It is named after the pseudonym of its founder Dmitry Utikin aka Wagner. See: A.M. Dyner, W. Lorenz, F. Bryjka, *Grupa Wagnera na Białorusi – konsekwencje dla NATO i UE* (Eng. The Wagner Group in Belarus - implications for NATO and the EU), Polski Instytut Spraw Międzynarodowych, 7 IX 2023, https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-konsekwencje-dla-nato-i-ue [accessed: 18 I 2024].

[12] *Ekspert: śmierć Prigożyna to dobra wiadomość, zaostrza się walka o władzę w otoczeniu osłabionego Putina* (Eng. Expert: Prigozhin's death is good news, power struggle intensifies around a weakened Putin), PAP, 24 VIII 2023, https://www.pap.pl/aktualnosci/ekspert-smierc-prigozyna-dobra-wiadomosc-zaostrza-sie-walka-o-wladze-w-otoczeniu [accessed: 18 I 2024].

and be conscripted into the Russian military[13]. An additional factor was the conflict between Prigozhin and the Russian military over the war in Ukraine and how the Wagner Group would be used. Within hours, the mutiny was abandoned and the Russian Defence Ministry guaranteed the safety of mercenaries who contact the department or law enforcement agencies.

Russian President Vladimir Putin, in a speech broadcast the day after the revolt, called the Wagnerists traitors and proposed moving the Wagner Group to Belarus[14]. However, it is important to consider whether Prigozhin's action was part of Russia's maskirovka to shift forces to Belarus and conduct further hybrid actions against NATO. This is confirmed by the words of President Lukashenko, who stated that the Wagnerists wanted (…) *to go on a trip to Warsaw and Rzeszów*[15].

The information that Prigozhin and his mercenaries had left the Russian Federation for Belarus was not published in the Russian news environment until several hours after the event. Information chaos was introduced as no reasons were given for Prigozhin's change of plans and a narrative was promoted that the mercenaries did not have sufficient support to continue the rebellion. Putin's authority and image as a strong leader was undoubtedly shaken. The Russian public's access to information was restricted by the introduction of censorship. The psychological measures of the Russian Federation towards its own society focused on changing perceptions

[13] M. Murphy, *Ukraine war: Russia moves to take direct control of Wagner Group*, BBC, 11 VI 2023, https://www.bbc.com/news/world-europe-65871232 [accessed: 25 VII 2023]. Mykhailo Podolak, an advisor to Ukrainian President Volodymyr Zelensky, commented on the putsch as an example of the lack of consent to violence. A different opinion was presented by journalist Vladislav Davidzon, who stated that it was a form of humiliation of Russian President Vladimir Putin and showed the extent of internal divisions within the system he leads. Experts from The Atlantic Council were of a similar opinion, pointing out that the Kremlin would lose the trust of the oligarchs and the war in Ukraine would no longer be a priority for them.

[14] *Putin wygłosił przemówienie do Rosjan. Mówił o "zdradzie organizatorów buntu"* (Eng. Putin gave a speech to Russians. He spoke of the "betrayal of the organisers of the revolt"), Rzeczpospolita, 26 VI 2023, https://www.rp.pl/swiat/art38660701-putin-wyglosil-przemowienie-do-rosjan-mowil-o-zdradzie-organizatorow-buntu [accessed: 30 I 2024].

[15] Łukaszenko w rozmowie z Putinem: *Wagnerowcy chcą jechać na wycieczkę do Warszawy i Rzeszowa* (Eng. Lukashenko in conversation with Putin: Wagnerists want to go on a trip to Warsaw and Rzeszów), Rzeczpospolita, 23 VII 2023, https://www.rp.pl/polityka/art38770821-lukaszenko-w-rozmowie-z-putinem-wagnerowcy-chca-jechac-na-wycieczke-do-warszawy-i-rzeszowa [accessed: 18 I 2024]. See: M. Duningan, *Where Will All the Wagner Group Mercenaries Go Now That Russia Has Exiled Their Leader?*, RAND, 3 VII 2023, https://www.rand.org/blog/2023/07/where-will-all-the-wagner-group-mercenaries-go-now.html [accessed: 25 VII 2023]; М. Сакавик, *Зачем Путин и Лукашенко угрожают Польше "вагнеровцами"?*, DW, 24 VII 2023, https://www.dw.com/ru/spektakl-putina-i-lukasenko-zacem-polse-ugrozaut-vagnerovcami/a-66332295 [accessed: 26 VII 2023]; G. Kuczyński, *Wagnerowcy. Psy wojny Putina* (Eng. Wagnerists. Putin's dogs of war), Warszawa 2022, in many places.

of the situation and intimidating the population. Internationally, on the other hand, Putin was no longer seen as a capable leader[16]. As a result, action on a global scale is expected to rebuild Putin's reputation as the ruler of an empire.

The Russian Federation used the involvement of key leaders, including politicians, to make the message credible. Putin was supported by Russian Ambassador to Minsk Boris Gryzlov, as well as soldiers from the 155th Marine Brigade of the Pacific Fleet, who recorded a video message of support for the president[17]. Representatives of the media also took a stand on the issue, including Vladimir Solovyov, president of the Union of Russian Journalists, appealing to Russian journalists not to succumb to provocations and to continue working for the good of society[18]. In addition, the entire propaganda apparatus was launched, including cultural institutions and so-called useful idiots. Representatives of the Russian Military-Historical Society particularly condemned the attempted mutiny and called on citizens not to support the mercenaries. Such gestures of acceptance reinforced the president's positive image and were proof of loyalty to authority.

The Russian Federation also used ethnic minorities to convince public opinion of the unity of the federal state. During the annexation of Crimea, great attention was paid to the issue of the Crimean Tatars. It should be pointed out that appreciation of the importance of national minorities is an important part of the identity of Russian society. In the crisis situation, Nikolai Doluda, ataman of the All-Russian Cossack Society, and Ismail Berdiev, representative of the Coordination Centre of Muslims of the North Caucasus, stood behind the commander-in-chief and considered the rebellion a betrayal of the state and leading to anarchy.

In order to intimidate the Russian public, it was pointed out that the mercenaries were trying to provoke a fratricidal civil war and had access to a nuclear arsenal.

To stabilise the external situation after Prigozhin's rebellion, the Russian Federation used a diplomatic corps, but also pursued an intensive foreign policy in the international information environment. Countries such as Venezuela, India, Iran, Saudi Arabia showed support for the Russian President. Some of these countries are

[16] Prigozhin died in a plane crash on 23 August 2023. His death may be a warning that the Russian president must not be defied.

[17] *Глава Приморья опубликовал обращение 155-й бригады морской пехоты в поддержку Путина*, Tacc, 25 VI 2023, https://tass.ru/armiya-i-opk/18109961 [accessed: 26 VII 2023].

[18] *Глава СЖР призвал журналистов не поддаваться на провокации*, РИА Новости, 24 VI 2023, https://ria.ru/20230624/zhurnalisty-1880217102.html [accessed: 26 VII 2023].

mentioned in the Security Strategy of the Russian Federation (2021), which indicates bilateral relations with them[19].

The dislocation of the Wagner Group after the Prigozhin putsch should be seen as a redeployment of Russian forces to Belarus and a strengthening of that direction[20]. The venture was intended to confuse public opinion (the technique used was the accumulation of information) and to mask real moves. The Wagner Group's activities must be categorised as hybrid actions. It was more effective to neutralise them at that moment by taking non-kinetic rather than purely kinetic actions.

The Wagner Group continues its activities as a company and documents them on its Wagner Orchestra profile on Telegram. There, it presents progress on the battlefield, such as at Bachmut, where the Group destroyed a Polish Krab cannon. It also carries out psychological activities aimed at building a positive image, e.g. it reported on a meeting with children from the patriotic club Ryś. This changed the image of the Wagnerists in Belarusian society. The same activities were carried out during the annexation of Crimea. Their aim was to convince the public of the Group's peaceful intentions and create the impression that its members were part of the community[21].

Information activities consist of reinforcing favourable attitudes towards the Russian Federation on the part of representatives of other states that legitimise its actions and confirm its position in the global security system.

NATO summit in Vilnius

At the NATO summit in Vilnius (11-12 July 2023), the Russian Federation used a technique of contrasting: bad West against good Russia. At the same time, it demonstrated that it alone is capable of ensuring global security (the technique used is an overstatement), while NATO is an archaic structure that fails to deliver on its promises and prioritises vested interests. The arrival of United States of America (US) President Joe Biden at the summit reinforced the rivalry between the superpowers.

---

[19] *Указ Президента Российской Федерации от 02.07.2021 г. № 400*, http://www.kremlin.ru/acts/bank/47046 [accessed: 27 VI 2023].

[20] *Лукашенко подтвердил приезд главы ЧВК "Вагнер" Пригожина в Беларусь*, БЕЛТА, 27 VI 2023, https://www.belta.by/president/view/lukashenko-podtverdil-priezd-glavy-chvk-vagner-prigozhina-v-belarus-574036-2023/ [accessed: 10 VII 2023].

[21] *Wagnerowcy odwiedzili "patriotyczne" białoruskie dzieci* (Eng. Wagnerists visited 'patriotic' Belarusian children), Belsat, 27 VII 2023, https://belsat.eu/pl/news/27-07-2023-wagnerowcy-odwiedzili-patriotyczne-bialoruskie-dzieci [accessed: 28 VII 2023]. See in more detail: Оркестр Вагнера, post on Telegram channel, https://t.me/s/orchestra_w [accessed: 28 VII 2023].

Representatives of the Ukrainian administration and media, including Serhiy Sydorenko, editor of the European Pravda portal, expressed the opinion that the failure to present Ukraine with a concrete plan for joining NATO at this summit would be a blow to Ukraine[22]. Ukrainian President Volodymyr Zelenski has been building in the minds of the international community the need for Ukraine to join NATO, including through diplomatic action. An example of this was his appeal to President Biden to invite Ukraine to join NATO, even if it was to become a member of the organisation after the war. The Vilnius summit was supposed to be a milestone for Ukraine in its accession to the North Atlantic Alliance and a strong wake-up call for the Russian Federation. It would have boosted morale and given strength to the Ukrainian soldiers and population to continue fighting. However, it should be stressed that joining NATO is conditional by law, as exemplified by Sweden, which has not yet been integrated into the Alliance structure[23]. The Vilnius summit was only a prelude to the meeting to be held in Washington in 2024. Decisive commitments will not be made until after the U.S. presidential election (autumn 2024) and the next U.S. administration takes office, and after the change in the position of NATO Secretary General, which will take place during the Washington summit.

In the Russian news environment, the Vilnius summit was portrayed as an event where NATO countries sought to deploy 300,000 of their troops along the border with the Russian Federation. At the same time, Russia was portrayed as a victim of the Alliance's actions and it was reiterated that it was only seeking to ensure the security of its citizens[24]. The message was given credence by President Putin, who confirmed that: *When it comes to Ukraine's membership of NATO, we have repeatedly said that this obviously poses a threat to Russia's security. And in fact, one of the reasons for the special military operation is the threat of Ukraine joining NATO*[25].

---

[22] *Ukraina w NATO? Publicysta: Brak konkretnego planu na szczycie w Wilnie będzie dla nas ciosem* (Eng. Ukraine in NATO? Publicist: the lack of a concrete plan at the Vilnius summit will be a blow to us), TVP Info, 21 VI 2023, https://www.tvp.info/70705131/ukrainski-publicysta-przedstawienie-na-szczycie-w-wilnie-niekonkretnego-planu-czlonkostwa-ukrainy-w-nato-bedzie-dla-nas-ciosem [accessed: 7 VII 2023].

[23] The article was completed on 30 IX 2023. At this time, Sweden has the status of a NATO invited state, not a NATO member state.

[24] *Политолог назвала главное событие предстоящего саммита НАТО в Вильнюсе*, Известия, 10 VII 2023, https://iz.ru/1542191/2023-07-10/politolog-nazvala-glavnoe-sobytie-predstoiashchego-sammita-nato-v-vilniuse [accessed: 18 VII 2023].

[25] *Путин назвал последствия принятия Украины в НАТО*, РИА Новости, 13 VII 2023, https://crimea.ria.ru/20230713/putin-nazval-posledstviya-prinyatiya-ukrainy-v-nato-1130043821.html [accessed: 18 VII 2023].

In addition to this, the Russian Federation reacted negatively to NATO's declaration of the transfer of cluster munitions to the Ukrainian side. Russia recognised that the Ukrainian Armed Forces would use these weapons to strike civilian targets and would therefore fight with them[26]. The outreach activities carried out towards the Russian public were aimed at changing perceptions, as well as reinforcing negative emotions towards Western countries, which were presented as a threat to Russia's sovereignty.

The Western mass media mainly focused on showing the unity of the Alliance, but at the same time pointed out the duality of expectations between the Ukrainian side and the member states. The Ukrainians were of the opinion that, after 500 days of war, they had proved their readiness for accession, while NATO took the position that an enlargement of the North Atlantic Treaty Organisation to include Ukraine was not possible until the war was over. Indeed, Ukraine's membership could encourage the Russian Federation to escalate to other European states[27]. Such a situation contributes to building internal divisions within NATO and creating space for Russian propaganda depreciating Ukraine in the West.

A different picture of the current geopolitical situation was shaped in the U.S. news environment. In the USA, the Vilnius summit has been used as a prelude to the presidential campaign, in which the Ukrainian theme will be addressed through the prism of money spent and support given. This thesis was confirmed by Lorne Cook in a publication in The Washington Post, in which he summarised the summit. He indicated that the Ukrainian administration was grateful for the promises of more arms and ammunition, while at the same time disappointed that no specific date was set for Ukraine's accession to NATO. The publicist drew attention to the issue of funding and the failure of the allies to deliver on their commitment to

[26] Г. Мишутин, Н. Гасымов, *Чем для Украины закончился саммит НАТО в Вильнюсе*, Ведомости, 13 VI 2023, https://www.vedomosti.ru/politics/articles/2023/07/13/985067-mezhdunarodnie-novosti [accessed: 18 VII 2023].

[27] M. Gebauer, R. Naukirch, Ch. Schult, *Gehört die Ukraine in die NATO?*, Spiegel, 10 VII 2023, https://www.spiegel.de/politik/nato-gipfel-in-vilnius-gehoert-die-ukraine-in-das-buendnis-a-e79ca421-d4d9-4663-9fac-1530b01b3b43 [accessed: 17 VII 2023]; N. Barotte, *Garanties de sécurité, processus d'adhésion de l'Ukraine… Les grands enjeux du sommet de l'OTAN à Vilnius*, Le Figaro, 10 VII 2023, https://www.lefigaro.fr/international/otan-quelles-garanties-de-securite-pour-l-ukraine-le-dilemme-allie-20230710 [accessed: 17 VII 2023]; *NATO summit: Ukraine's future membership to be discussed by leaders in Vilnius,* BBC, 11 VI 2023, https://www.bbc.com/news/world-europe-66157625 [accessed: 18 VII 2023].

increase defence GDP[28]. The outreach activities of the RF and the US will evolve depending on developments in the international security environment.

Perspectives

Russia's outreach activities in Central Europe will focus on creating a new order, as well as stirring up public emotions. This is driven by the desire to rebuild imperial influence and the need to ensure the security of Russian-speaking citizens in various countries.

It is important to note that the RF influences the international community by instilling fear and transgressing boundaries respected by democratic states.

Non-kinetic activities including information activities will be the same as before. Only the timing and tools change, while the information techniques remain the same. Parts of the Russian narrative have been replicated since the annexation of Crimea in 2014 and remain relevant. The content promoted includes:

1) the strong and unbreakable historical ties of the Donbass with Russia,
2) the intensification of NATO activities along the border with the Russian Federation, which are interpreted as an attack on Russian sovereignty,
3) Russophobia of the West, especially the US[29].

Their aim is to influence bilateral relations between Russia and the West and to undermine the position of the legally elected government in Ukraine. The president of the Russian Federation has called on the Ukrainian armed forces to overthrow the government in Kiev and forcibly take control of the state. This attitude of the Russian Federation was the subject of a speech by John Kelley U.S. political minister, who said, among other things: *We have heard Russia claim that it is not the aggressor, that it is trying to stop the 'genocide' in eastern Ukraine, that it needs to 'denazify' the Ukrainian government and fight drug addicts and satanists. Whatever today's excuse is, it cannot hide the fact that Russia is not the victim it claims to be*[30].

---

[28] L. Cook, *NATO summit results in brief: Mixed news for Ukraine, hope for Sweden and a response to Russia*, The Washington Post, 12 VI 2023, https://www.washingtonpost.com/world/2023/07/12/nato-summit-vilnius-lithuania-ukraine/980690b6-20c8-11ee-8994-4b2d0b694a34_story.html [accessed: 17 VII 2023]. Cf.: *Despite Successes at NATO Summit, Divisions Remain*, The New York Times, 12 VII 2023, https://www.nytimes.com/2023/07/12/world/europe/nato-summit-ukraine-biden.html [accessed: 17 VII 2023]. See: S. Ramani, *Putin's War on Ukraine*, London 2023, in many places.

[29] *В ДНР рассказали, что стало точкой невозврата в Донбассе*, РИА Новости, 13 IV 2021, https://ria.ru/20210413/operatsiya-1728010412.html [accessed: 10 VII 2023].

[30] J. Kelley, *Remarks at a UN Security Council Briefing Called by Russia on Russophobia,* The U.S. Mission to the United Nations, 14 III 2023, https://usun.usmission.gov/remarks-at-a-un-security-council-

Russia influenced the Polish information environment both during the Russian-Belarusian military exercises Zapad-21 and during the exercises carried out by Poland (e.g. Anaconda exercises)[31]. It has sought over the years to highlight topics that would discredit the Polish government administration and uniformed services, including deprecating high-ranking officers through the preparation of interviews (e.g. an interview with Major General Maciej Jabłoński in 2018)[32], disinformation on the fulfilment of allied commitments and the purchase of armaments.

Cyberoperations are another information threat that destabilises the information environment. These include *deepfake*, a tool of image falsification that Russia is developing to gain public trust or discredit decision-makers.

The common denominator of the non-kinetic activities undertaken by the RF is the desire to maintain its position as hegemon in Central Europe. Given the military purchases made by Poland, Russian activity aimed at diminishing the potential of the Polish Armed Forces is to be expected.

The actions of the adversary at the border with Poland generate many threats, e.g. escalation of the migration crisis, sabotage, attack on critical infrastructure[33]. The response from the Polish side may become a pretext for the RF to completely annex Belarus and thus provide assistance to it. It should be noted, however, that ensuring the safety of Polish citizens is a priority in the face of the threat.

As the geopolitical situation in the Middle East and Indo-Pacific is increasingly tense, the Russian Federation will pursue outreach activities (e.g. psychological actions such as demonstration of force and psychological pressure) that will stabilise

briefing-called-by-russia-on-russophobia/ [accessed: 10 VII 2023]. Countering the disinformation promoted by Russia is reliable public information. See: *EU response to Russia's invasion of Ukraine*, European Council, 7 VII 2023, https://www.consilium.europa.eu/en/policies/eu-response-ukraine-invasion/ [accessed: 10 VII 2023].

[31] Exercises Zapad-21 focused on, inter alia, psychological actions destabilising the internal security system of the Republic of Poland. The exercise was additionally a show of force by the Russian Armed Forces and a way to divert public attention from current international challenges.

[32] A fake news item about the Anaconda-18 exercises, along with a statement by Major General Jabłoński, was published on the pro-Russian disinformation portal Niezależny Dziennik Polityczny. See: *Gen. Jabłoński OSTRO: Dowódca Operacyjny zhańbił moją dywizję bojową! O co chodzi?* (Eng. Gen. Jabłoński FIERCELY: The Operational Commander has disgraced my combat division! What is it all about?), Niezależny Dziennik Polityczny, 13 XI 2018, https://dziennik-polityczny.com/2018/11/13/gen-jablonski-ostro-dowodc%D0%B0-operacyjny-zhanbil-moja-dywizje-bojowa-o-co-chodzi/ [accessed: 7 VII 2023].

[33] A.M. Dyner, *Grupa Wagnera na Białorusi – potencjalne zagrożenia dla Polski* (Eng. The Wagner Group in Belarus - potential threats to Poland), Polski Instytut Spraw Międzynarodowych, 27 VII 2023, https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-potencjalne-zagrozenia-dla-polski [accessed: 28 VII 2023].

its position in the Baltic and force concessions from the West and temporarily freeze its actions in Europe (war with Ukraine)[34].

Conclusions

The Russian Federation conducts outreach activities by adapting to the realities of the functioning of individual states (political, social, economic conditions, etc.). The diversification of states has enabled the RF to use tools, such as, for example, psychological influence products, which exert pressure on the will of decision-makers and the public's understanding of the situation. Russia is once again trying to influence the security architecture.

The main conclusions include:

1) The information activities of the Russian Federation are conducted on a long-term basis and aimed at maintaining the role of hegemon and the desire to return to the glory days of the Russian empire.
2) Information activities are part of the power play at the global level. The intensification of a potential conflict in the Indo-Pacific will change the balance of power in the world.
3) The 2023 NATO summit in Vilnius was a prelude to discussions on the current geopolitical situation including existing conflicts in the international arena and their consequences. The final decisions on the Alliance's actions will be made at the 2024 meeting in Washington, D.C. They will be heavily influenced by the new American administration, which will set its tone in global relations.
4) The Russian Federation is permanently infiltrating the Baltic Sea states with information in order to undermine NATO's dominance there. It disseminates narratives and uses tools that have proven successful in previous conflicts.
5) Russia is escalating tensions by threatening to use tactical nuclear charges. This may be a prelude to creating conditions in which it will use weapons of mass destruction.
6) The Russian-Ukrainian war has led to a situation where Ukraine has become the most militarised state in Europe. This has consequently verified the technological capabilities of the West and the Russian Federation itself.

[34] See: M. Priebe, *Alternative Futures Following a Great Power War: Miranda Priebe and Bryan Frederick in Conversation*, RAND, 9 V 2023, https://www.rand.org/blog/2023/05/alternative-futures-following-a-great-power-war-miranda.html [accessed: 7 VII 2023].

Many of the Russian Federation's domestic and foreign policy outreach activities have enabled it to achieve some of its strategic objectives and information effects. Russia remains a player in international relations and continues to be an active participant in global competition. The Russian Federation's information activities in Europe are carried out towards international relations actors in order to consolidate the Russian position in the region and to achieve the intended information effects. Changing the perception of audiences and creating an alternative reality is an important factor in destabilising Western states. The information activities of the RF have a strong impact on the societies of Poland and the Baltic States. The sense of fear among citizens influences their political decisions and is a factor determining social attitudes.

The Russian authorities are also influencing their own society to gain support for the "special military operation" and to consolidate the desire to return to the glory days of the empire. Typical of Russian society, the superiority of collective behaviour over individual behaviour, a hostile attitude to changing realities and thinking of Greater Russia through the prism of ethnic minorities underpin the RF's information activities.

It is important to recognise that the issues presented in the publication are an important subject for representatives of both the scientific and military communities. Conclusions from the presented research can serve as a starting point for the preparation of a report for decision-makers. The article is not exhaustive and does not address many aspects of the topic, which provides an assumption for further research.

Bibliography

Fiszer J., Fiszer M., *Wojna w Ukrainie. Od napaści do kontrofensywy* (Eng. The war in Ukraine. From assault to counter-offensive), Warszawa 2023.

Informacyjny wymiar wojny hybrydowej (Eng. The information dimension of hybridwarfare), Wrzosek M. et al. (sci. ed.), Warszawa 2018.

Information operations DD-3.10(A), Centrum Doktryn i Szkolenia Sił Zbrojnych Rzeczypospolitej Polskiej, Bydgoszcz 2017.

Kuczyński G., *Wagnerowcy. Psy wojny Putina* (Eng. Wagnerists. Putin's dogs of war), Warszawa 2022.

Lis A., Tarczyński J., *Zarządzanie informacją i wiedzą na potrzeby analiz strategicznych i operacyjnych Sił Zbrojnych RP* (Eng. Information and knowledge management for strategic and operational analyses of the Polish Armed Forces), Warszawa–Bydgoszcz 2022.

Modrzejewski Z., *Operacje informacyjne* (Eng. Information operations), Warszawa 2015.

Psychological Operations DD-3.10.1(B), Centrum Doktryn i Szkolenia Sił Zbrojnych Rzeczypospolitej Polskiej, Bydgoszcz 2017.

Ramani S., *Putin's War on Ukraine*, London 2023.

Internet sources

Barotte N., *Garanties de sécurité, processus d'adhésion de l'Ukraine… Les grands enjeux du sommet de l'OTAN à Vilnius*, Le Figaro, 10 VII 2023, https://www.lefigaro.fr/international/otan-quelles-garanties-de-securite-pour-l-ukraine-le-dilemme-allie-20230710 [accessed: 17 VII 2023].

Cook L., *NATO summit results in brief: Mixed news for Ukraine, hope for Sweden and a response to Russia,* The Washington Post, 12 VI 2023, https://www.washingtonpost.com/world/2023/07/12/nato-summit-vilnius-lithuania-ukraine/980690b6-20c8-11ee-8994-4b2d0b694a34_story.html [accessed: 17 VII 2023].

Courtney W., *Countering Russia's Nuclear Threat in Europe,* 20 IV 2023, https://www.rand.org/blog/2023/04/countering-russias-nuclear-threat-in-europe.html [accessed: 7 VII 2023].

Despite Successes at NATO Summit, Divisions Remain, The New York Times, 12 VII 2023, https://www.nytimes.com/2023/07/12/world/europe/nato-summit-ukraine-biden.html [accessed: 17 VII 2023].

Duningan M., *Where Will All the Wagner Group Mercenaries Go Now That Russia Has Exiled Their Leader?*, RAND, 3 VII 2023, https://www.rand.org/blog/2023/07/where-will-all-the--wagner-group-mercenaries-go-now.html [accessed: 25 VII 2023].

Dyner A.M., *Grupa Wagnera na Białorusi – potencjalne zagrożenia dla Polski* (Eng. The Wagner Group in Belarus - potential threats to Poland), Polski Instytut Spraw Międzynarodowych, 27 VII 2023, https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-potencjalne-zagrozenia-dla-polski [accessed: 28 VII 2023].

Dyner A.M., Lorenz W., Bryjka F., *Grupa Wagnera na Białorusi – konsekwencje dla NATO i UE* (Eng. The Wagner Group in Belarus - implications for NATO and the EU), Polski Instytut Spraw Międzynarodowych, 7 IX 2023, https://www.pism.pl/publikacje/grupa-wagnera-na-bialorusi-konsekwencje-dla-nato-i-ue [accessed: 18 I 2024].

Ekspert: śmierć Prigożyna to dobra wiadomość, zaostrza się walka o władzę w otoczeniu osłabionego Putina (Eng. Expert: Prigozhin's death is good news, power struggle intensifies around a weakened Putin), PAP, 24 VIII 2023, https://www.pap.pl/aktualnosci/ekspert-smierc-prigozyna-dobra-wiadomosc-zaostrza-sie-walka-o-wladze-w-otoczeniu [accessed: 18 I 2024].

EU response to Russia's invasion of Ukraine, European Council, 7 VII 2023, https://www.consilium.europa.eu/en/policies/eu-response-ukraine-invasion/ [accessed: 10 VII 2023].

Gebauer M., Naukirch R., Ch. Schult, *Gehört die Ukraine in die Nato?*, Spiegel, 10 VII 2023, https://www.spiegel.de/politik/nato-gipfel-in-vilnius-gehoert-die-ukraine-in-das-buendnis-a-e79ca421-d4d9-4663-9fac-1530b01b3b43 [accessed: 17 VII 2023].

Gen. Jabłoński OSTRO: Dowódca Operacyjny zhańbił moją dywizję bojową! O co chodzi? (Eng. Gen. Jabłoński FIERCELY: The Operational Commander has disgraced my combat division! What is it all about?), Niezależny Dziennik Polityczny, 13 XI 2018, https://dziennik-polityczny.com/2018/11/13/gen-jablonski-ostro-dowodc%D0%B0-operacyjny-zhanbil-moja-dywizje-bojowa-o-co-chodzi/ [accessed: 7 VII 2023].

Kelley J., *Remarks at a UN Security Council Briefing Called by Russia on Russophobia,* The U.S. Mission to the United Nations, 14 III 2023, https://usun.usmission.gov/remarks-at-a-un-security-council-briefing-called-by-russia-on-russophobia/ [accessed: 10 VII 2023].

Łukaszenko w rozmowie z Putinem: *Wagnerowcy chcą jechać na wycieczkę do Warszawy i Rzeszowa* (Eng. Lukashenko in conversation with Putin: Wagnerists want to go on a trip to Warsaw and Rzeszów), Rzeczpospolita, 23 VII 2023, https://www.rp.pl/polityka/art38770821-lukaszenko-w-rozmowie-z-putinem-wagnerowcy-chca-jechac-na-wycieczke-do-warszawy-i-rzeszowa [accessed: 18 I 2024].

Murphy M., *Ukraine war: Russia moves to take direct control of Wagner Group*, BBC, 11 VI 2023, https://www.bbc.com/news/world-europe-65871232 [accessed: 25 VII 2023].

NATO summit: Ukraine's future membership to be discussed by leaders in Vilnius, BBC, 11 VI 2023, https://www.bbc.com/news/world-europe-66157625 [accessed: 18 VII 2023].

Phillips L., Crouch D., *Have Chemical Weapons been Used in Ukraine?*, RUSI, 20 VI 2023, https://rusi.org/explore-our-research/publications/commentary/have-chemical-weapons-been-used-ukraine [accessed: 7 VII 2023].

Priebe M., *Alternative Futures Following a Great Power War: Miranda Priebe and Bryan Frederick in Conversation*, RAND, 9 V 2023, https://www.rand.org/blog/2023/05/alternative-futures-following-a-great-power-war-miranda.html [accessed: 7 VII 2023].

Putin wygłosił przemówienie do Rosjan. Mówił o "zdradzie organizatorów buntu" (Eng. Putin gave a speech to Russians. He spoke of the "betrayal of the organisers of the revolt"), Rzeczpospolita, 26 VI 2023, https://www.rp.pl/swiat/art38660701-putin-wyglosil-przemowienie-do-rosjan-mowil-o-zdradzie-organizatorow-buntu [accessed: 30 I 2024].

Sławiński M., *Szef rosyjskiego wywiadu poszedł z tym do Łukaszenki: Polska czeka na odpowiedni moment* (Eng. Russian intelligence chief went to Lukashenko with this: Poland is

waiting for the right moment), Wprost, 27 VI 2023, https://www.wprost.pl/swiat/11165518/szef-rosyjskiego-wywiadu-poszedl-z-tym-do-lukaszenki-polska-czeka-na-odpowiedni-moment.html [accessed: 6 VII 2023].

Ukraina w NATO? Publicysta: Brak konkretnego planu na szczycie w Wilnie będzie dla nas ciosem (Eng. Ukraine in NATO? Publicist: The lack of a concrete plan at the Vilnius summit will be a blow to us*)*, TVP Info, 21 VI 2023, https://www.tvp.info/70705131/ukrainski-publicysta-przedstawienie-na-szczycie-w-wilnie-niekonkretnego-planu-czlonkostwa-ukrainy-w-nato-bedzie-dla-nas-ciosem [accessed: 7 VII 2023].

Wagnerowcy odwiedzili "patriotyczne" białoruskie dzieci (Eng. Wagnerists visited 'patriotic' Belarusian children*),* Belsat, 27 VII 2023, https://belsat.eu/pl/news/27-07-2023-wagnerowcy-odwiedzili-patriotyczne-bialoruskie-dzieci [accessed: 28 VII 2023].

Russian Internet sources

В ДНР рассказали, что стало точкой невозврата в Донбассе, РИА Новости, 13 IV 2021, https://ria.ru/20210413/operatsiya-1728010412.html [accessed: 10 VII 2023].

Глава Приморья опубликовал обращение 155-й бригады морской пехоты в поддержку Путина, Tacc, 25 VI 2023, https://tass.ru/armiya-i-opk/18109961 [accessed: 26 VII 2023].

Глава СЖР призвал журналистов не поддаваться на провокации, РИА Новости, 24 VI 2023, https://ria.ru/20230624/zhurnalisty-1880217102.html [accessed: 26 VII 2023].

ДНР заявляет о взятых в плен польских наемниках, РИА Новости, 2 IX 2014, https://ria.ru/20140902/1022431781.html [accessed: 7 VII 2023].

Лукашенко подтвердил приезд главы ЧВК "Вагнер" Пригожина в Беларусь, БЕЛТА, 27 VI 2023, https://www.belta.by/president/view/lukashenko-podt-verdil-priezd-glavy-chvk-vagner-prigozhina-v-belarus-574036-2023/ [accessed: 10 VII 2023].

Медведев считает, что заявления Польши подтверждают бессмысленность каких-либо переговоров, Tacc, 27 VI 2023, https://tass.ru/politika/18100221 [accessed: 6 VII 2023].

Мишутин Г., Гасымов Н., *Чем для Украины закончился саммит НАТО в Вильнюсе*, Ведомости, 13 VI 2023, https://www.vedomosti.ru/politics/articles/2023/07/13/985067-mezhdunarodnie-novosti [accessed: 18 VII 2023].

Оркестр Вагнера*,* post on Telegram channel, https://t.me/s/orchestra_w [accessed: 28 VII 2023].

Политолог назвала главное событие предстоящего саммита НАТО в Вильнюсе, Известия, 10 VII 2023, https://iz.ru/1542191/2023-07-10/politolog-nazvala-glavnoe-so-

bytie-predstoiashchego-sammita-nato-v-vilniuse [accessed: 18 VII 2023].

Польские бизнесмены ответят за русофобию Варшавы, ВЗГЛЯД, 14 VII 2023, https://vz.ru/politics/2023/7/14/1221118.html [accessed: 31 VII 2023].

Путин назвал последствия принятия Украины в НАТО, РИА Новости, 13 VII 2023, https://crimea.ria.ru/20230713/putin-nazval-posledstviya-prinyatiya-ukrainy-v-nato-1130043821.html [accessed: 18 VII 2023].

Сакавик М., *Зачем Путин и Лукашенко угрожают Польше "вагнеровцами"?*, DW, 24 VII 2023, https://www.dw.com/ru/spektakl-putina-i-lukasenko-zacem-polse-ugrozaut-vagnerovcami/a-66332295 [accessed: 26 VII 2023].

СМИ сообщили об изнасиловании несовершеннолетней наемниками из Польши, Известия, 10 II 2023, https://iz.ru/1468024/2023-02-10/smi-soobshchili-ob-iznasilovanii-nesovershennoletnei-naemnikami-iz-polshi [accessed: 7 VII 2023].

Указ Президента Российской Федерации от 02.07.2021 г. № 400, http://www.kremlin.ru/acts/bank/47046 [accessed: 27 VI 2023].

Karolina Kuśmirek, PhD

Doctor in political science, analyst, her research focuses on information warfare and special forces operations in the world.

Contact: karolinakusmirek@gmail.com

Critical analysis of the effectiveness of EU financial sanctions against the Russian Federation

ANGELA PACHOLCZAK

Independent author

https://orcid.org/0009-0000-4670-2364

Internal Security Review, 2024, no. 30: 353–383

https://doi.org/10.4467/20801335PBW.24.015.19617

ARTICLE

Abstract

The article focuses on the issue of international sanctions of a financial nature in the context of, in particular, the challenges to their effectiveness generated by the cryptocurrency market. An essential point of reference for this analysis is the current case of sanctions imposed by the Council of the European Union (supported by the application of complementary sanctions by part of the international community) on the Russian Federation in relation to that country's military aggression against Ukraine. The aim of this article is to show different perspectives on the assessment of the effectiveness of sanctions and, in particular, to identify the sources why, in a key number of cases, while weakening the economic potential of the sanctioned state, they nevertheless fail to achieve the original objective of their imposition, i.e. the deterrence of military action. In this subject, the axis of interest is the current and prospective impact of blockchain-based financial solutions on the creation of an important loophole in the sanctions regime to eliminate or marginalise the effects of international financial sanctions. The issue is also assessed through the prism of the crypto-asset market regulation entering into force in the European Union in the near future and the implementation of the so-called travel rule for cryptocurrency transactions.

Keywords

Russian Federation, financial international sanctions, crypto-assets, decentralised finance, DeFi, central bank digital currency, CBDC, MiCA regulation

War is merely the continuation of policy by other means.
Carl von Clausewitz, *On the Nature of War* (1832)

Engaging in military action by the international community in response to a violation of international law by one state can hardly be considered a good option when the overriding objective is to avoid an escalation of armed conflict. Consequently, a better, and sometimes the only choice for the international community becomes the use of sanctions, which are seen as a liberal alternative to war. However, in the context of achieving the main objective of the application of sanctions, i.e. deterring military aggression, they are more of a signal[1], rather than having a real impact on the party covered by them, especially its policy-makers and circles linked to the centres of power.

The concept of sanctions is primarily associated with the use of economic tools directly relating to the economic sphere, which involves the cessation or threat of cessation of existing trade or financial relations. Sanctions are more than a mere diplomatic declaration and their real effectiveness is conditional on causing a drastic impact on the economy of the sanctioned country.

The view should be shared that the effective enforcement of financial sanctions is far easier than the enforcement of trade sanctions[2], which is due to the fact that financial institutions and states are important providers or guarantors of financial flows. Moreover, there is far more supervision over the financial market than over the trade market. Financial activities should therefore, at least in principle, be easier to monitor and possibly identify violations of sanctions. In addition, studies have confirmed the greater effectiveness of financial sanctions compared to trade sanctions[3]. Indeed, it cannot be overlooked that, in an economic environment,

[1] This is due to the way in which the normative basis is understood, according to which it is assumed that through punishment and shaming it is possible to create moral motivations. This is related to the understanding of international sanctions as a negative reaction of the international community towards a state that violates its norms. See: R. Bierzanek, J. Symonides, *Prawo międzynarodowe publiczne* (Eng. Public international law), Warszawa 2003, p. 24.

[2] G.C. Hufbauer et al., *Economic Sanctions Reconsidered: Supplemental case histories*, Washington 2007, pp. 97–98.

[3] In a study by Gary C. Hufbauer, Jeffrey J. Schott and Kimberly A. Elliott conducted in 1985 (updated in 1990 and 2007), with regard to financial sanctions caseloads, 19 cases out of 53 involving the application of financial sanctions alone (36%), 32 cases out of 101 involving the application of financial and trade sanctions (32%) and 8 cases out of 21 involving the freezing of assets (38%) were considered successful. By contrast, in a situation involving the application of commercial sanctions only, a positive outcome was recorded in 10 cases out of 40 reviewed (25%). See: G.C. Hufbauer et al., *Economic Sanctions Reconsidered*…, p. 98.

trading activities require access to financial resources. Thus, financial sanctions have a complementary effect on trade flows as they avoid the problem of enforcement of sanctions against them[4]. However, counterintuitively, like other types of sanctions, financial sanctions can also be inhumane in nature and cause irreparable harm to the civilian population of the sanctioned country, but do not necessarily have a direct impact on the situation of its policy-makers.

This raises an important question about the impact of the developments in financial markets, globally observed for more than a decade (including innovative alternatives to traditional banking systems that increasingly interact with state monetary and currency systems), on undermining the effectiveness of international sanctions. Indeed, the question can be raised not only about the validity of the relevant laws, but also about the possibility of expressing in them norms that fully regulate the new solutions applied in the financial markets, which would indirectly ensure the enforcement effectiveness of the established sanctions. The aim of this article is to show the complexity of this issue in the context of access to and use of new financial instruments by state apparatuses. It is not limited to dogmatic research on this issue, but, due to the perception of law as a multifaceted cultural phenomenon[5], reference is made to the results of economic and political scientific research on the effectiveness of international sanctions, including a review of innovative financial instruments relevant to the EU sanctions imposed on the Russian Federation (RF) in connection with its military aggression against Ukraine.

The ineffectiveness of economic sanctions

There is a misconception associated with sanctions that enforcing an expected norm of behaviour will be triggered by mere concern about economic performance on the part of the covered state. Contrary to this assumption, economic research conducted in 1990 by Gary C. Hufbauer, Jeffrey J. Schott and Kimberly A. Elliott showed that the effectiveness of economic sanctions was relatively low at about 34%[6]. As a result of a critical analysis of these studies in political science terms,

[4] Ibid, pp. 47–48, 97.

[5] See: K. Opałek, J. Wróblewski, *Zagadnienia teorii prawa* (Eng. Issues in legal theory), Warszawa 1969; the same, *Prawo. Metodologia, filozofia, teoria prawa* (Eng. Law. Methodology, philosophy, theory of law), Warszawa 1991.

[6] The 1990 study included 116 cases in which sanctions were applied. In 40 cases, their application was found to have had a positive effect.

Robert A. Pape concluded that of the 40 cases identified in them, only five could be considered a real success of the application of sanctions[7].

The ineffectiveness of sanctions is influenced by a number of factors, primarily these are the inadequacy and insufficiency of the measures used. This makes it easier to avoid sanctions or at least minimise their negative implications. In this context, the basic condition for effectiveness is the unanimity of the international community on the imposition of sanctions on a country. The absence of this solidarity opens the door to the possibility of limiting and neutralising the effects of sanctions. For example, in terms of trade, this opens up new import destinations and changing markets for exports. At the same time, through new trade destinations, it becomes possible to 'smuggle' sanctioned goods to countries formally applying sanctions[8]. With regard to the financial system, on the other hand, it is possible to secure it through the so-called economy vaccination, which involves insulating it from the impact of sanctions by either securing a remedy to the sanctions or gaining easy access to alternatives[9].

Sanctions are also associated with the phenomenon of intensification of nationalist attitudes in the state against which they are applied. This is pointed out by Robert A. Pape, who unequivocally points out the ineffectiveness of sanctions when not only the state apparatus, but also citizens are willing to endure severe sanctions in the name of national interests. Such tendencies especially characterise autocratic systems, in which the authority can accept high costs in social terms if it enables it to achieve its own goals[10]. Thus, this phenomenon contradicts claims that striking at the economic interests of a country's citizens must involve their advocacy of political change.

In the current reality, the ineffectiveness of financial sanctions is also linked to the growing global importance of cryptocurrencies. They can play an important role in minimising sanctions both individually and involving a country's financial system.

---

[7] Pape corrected the number of cases examined - there were 115, not 116. He considered 5 cases to be repetitions, similarly, among the 40 cases classified as a success, he identified 1 repetition, in 18 cases the settlement actually resulted from the direct or indirect use of force, in 8 cases the sanctions had no effect, as the countries covered by them made no concessions, and 6 cases involved trade disputes, not strictly economic sanctions for political purposes. In 3 cases, evaluation for the effectiveness of sanctions is impossible. See: R.A. Pape, *Why Economic Sanctions Do Not Work*, "International Security" 1997, vol. 22, no. 2, p. 93, 99.

[8] Naturally, this nevertheless entails negative consequences for the sanctioned country due to a drop in the price of exported raw materials and goods.

[9] A. Demarais, *Backfire: How Sanctions Reshape the World Against U.S. Interests*, New York 2022, pp. 35–50.

[10] R.A. Pape, *Why Economic Sanctions*…, p. 106.

Russian case

In view of the hostilities against Ukraine and the illegal annexation of the Donetsk, Luhansk, Zaporozhye and Kherson regions (2022), and in view of the restrictive measures imposed on the Russian Federation in connection with the annexation of Crimea (2014), among others, the European Union (EU)[11] decided to impose further sanctions on the country. These were restrictive measures in the form of both individual sanctions as well as economic and visa sanctions. As of 5 March 2024, the EU Council had adopted 13 sanctions packages.

Focusing solely on the issue of direct impact on the Russian financial system, the following EU sanctions should be pointed out:

- A ban on financing the Russian government and the Central Bank of Russia, CBR (Russian: Центральный банк Российской Федерации or Банк России) and any transactions related to the management of its reserves and assets (foreign exchange reserve freeze), as well as bodies, entities or persons acting on behalf of or under its direction [e.g., the Russian National Wealth Fund (Фонд национального благосостояния)];
- A ban on the export of banknotes and the sale of negotiable securities[12] to Russia denominated in euros and other official EU currencies[13];
- A ban on investing in projects co-financed by the Russian Direct Investment Fund (Российский фонд прямых инвестиций), as well as participating in or making other contributions to projects[14];
- A ban on all transactions with certain Russian state-owned enterprises in various sectors that make up the Kremlin's military-industrial complex[15],

[11] In addition to the EU sanctions (and its member states, which retained the ability to impose separate, additional sanctions), measures have also been imposed on Russia by: US, UK, Canada, Switzerland, Japan, Singapore, South Korea, Australia, New Zealand and Taiwan. The scope of these sanctions is not uniform in many cases. Singapore, for example, opted only to impose limited financial sanctions and export controls on weapons and items for offensive cyberoperations. See: *Sanctions and Restrictions Against Russia in Response to its Invasion of Ukraine*, Ministry of Foreign Affairs Singapore, 5 III 2022, https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/03/20220305-sanctions [accessed: 5 III 2024].

[12] Linked to this ban is the prohibition on EU central securities depositories to hold accounts for Russian clients.

[13] Exceptions include funds necessary for the personal use of travellers to Russia or official purposes of diplomatic missions, consular missions, international organisations.

[14] In this respect, strict derogations are provided for contracts concluded before 2 March 2022.

[15] The complete list of the above-mentioned entities is set out in the list of Annex XIX of *Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*.

as well as a ban on holding positions in the governing bodies of these enterprises;
- A ban on the listing of shares of Russian state-owned entities on EU trading venues and the provision of related services;
- Prohibition of direct or indirect purchase, sale or provision of investment services or assistance in issuance and other activities with respect to marketable securities and money market instruments with respect to, among others, the Government of Russia and the CBR, legal persons, entities and bodies acting on their behalf, as well as entities identified in Annexes V and VI of *Council Regulation (EU) No. 833/2014 of July 31 2014 concerning restrictive measures in view of Russia's actions destabilizing the situation in Ukraine* (hereinafter: Regulation 833/2014);
- Prohibition on providing business services directly or indirectly, such as accounting, auditing, statutory auditing, bookkeeping and tax consulting, information technology consulting, legal consulting, architecture and engineering, management consulting, public relations, market and public opinion research, technical research and analysis, advertising and rating services;
- A ban on providing key Russian banks with specialised financial messaging services used to exchange financial data within the Society for Worldwide Interbank Financial Telecommunication (SWIFT)[16];
- A ban on providing public financing or financial assistance for trade with the Russian side or investment in the Russian Federation[17];
- A ban on the participation of Russian contractors in public contracts and concessions awarded in EU member states;
- A ban on EU Central Securities Depositories (CSDs) maintaining accounts for Russian clients and selling them euro-denominated securities;
- A ban on accepting deposits from citizens or Russian residents, legal persons, entities or bodies based in Russia, or legal persons, entities or bodies

[16] The sanctions under the third package of 2 March 2022 covered seven Russian banks, namely Банк Открытие (Bank Otkritie), Новикомбанк (Novikombank), Промсвязьбанк (Promsvyazbank), Банк "Россия" (Rossiya Bank), Совкомбанк (Sovcombank), Vnesheconombank (VEB, VEB.RF) and Банк ВТБ (WTB Bank), as well as all legal persons, entities or bodies established in Russia in which more than 50% of the ownership rights are directly or indirectly held by the above institutions. Subsequently, as part of the sixth package of 3 June 2022, the exemption from SWIFT was extended to Сбербанк России (Sberbank of Russia), Московский кредитный банк (Credit Bank of Moscow) and Российский сельскохозяйственный банк (Россельхозбанк) - (Russian Agricultural Bank).

[17] The exceptions are: the reservation to finalise contracts concluded before 26 February 2022 and special cases concerning trade in food products, agricultural, medical or humanitarian measures, and concerning EU programmes for small and medium-sized enterprises - up to a certain amount.

based outside the EU, where more than 50% of the ownership rights belong directly or indirectly to Russian citizens or natural persons residing in Russia, if the total value of their deposits per credit institution exceeds the amount of EUR 100,000;
- A ban on the provision of financial planning advice and trusts as well as the acceptance of large deposits by EU banks;
- A ban on the provision of cryptographic services initially of high value (i.e. EUR 10,000) and then regardless of value.

At the same time, following the introduction of the thirteenth package of sanctions against Russia, a total of 2,177 individuals and entities[18] were subjected to individual sanctions involving, among other things, the freezing of assets and the prohibition of funds or economic resources. New sanctions were also established against Belarus (due to actions undermining the territorial integrity, sovereignty and independence of Ukraine) and Iran (in connection with its military support in the form of the delivery of unmanned aerial vehicles). As for individual sanctions imposed on Belarus, they were applied to 271 individuals and entities[19], and on Iran - to 280 individuals and entities[20].

The enforcement of sanctions adopted by the Council of the EU rests with member states, which are responsible for their implementation. In this regard, they are supported by the European Commission (EC), which is responsible for the uniformity of these measures and their international coordination[21].

EU sanctions targeting Russia and Belarus are supplemented in Poland by domestic sanctions. In this respect, the most important piece of legislation is the *Act of 13 April 2022 on special solutions to counter support for aggression against Ukraine*

---

[18] As set out in Annex I of *Council Regulation (EU) No 269/2014 of 17 March 2014 on restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine* - with 36 persons and entities having been removed from the list as at 5 March 2024, 2141 persons and entities therefore remain subject to sanctions.

[19] As set out in Annex I of *Council Regulation (EC) No 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and in view of Belarus' involvement in Russia's aggression against Ukraine* - with 1 entity having been removed from the list as of 5 March 2024, 270 persons and entities remain subject to sanctions.

[20] As set out in Annex I of *Council Regulation (EU) No 359/2011 of 12 April 2011 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran* - with 8 persons having been removed from the list as at 5 March 2024, 272 persons and entities therefore remain subject to sanctions.

[21] To this end, the EC has set up a Freeze and Seize task force to coordinate at EU level the implementation of individual sanctions against individuals. This group is also responsible for cooperation within the REPO (Russian Elites, Proxies, and Oligarchs) task force, which manages EU cooperation with the G7 (Group of Seven) countries and Australia.

and serving to protect national security, stipulating, inter alia, the establishment of an additional national sanctions list maintained by the minister responsible for internal affairs[22].

Pursuant to the provisions of this Act, a fine, imposed by the Head of the National Revenue Administration by way of an administrative decision, of up to PLN 20 million[23] shall be imposed on a person or entity who, with respect to a listed person or entity, fails to comply with: the obligation to freeze financial assets, funds or economic resources or the prohibition on making financial assets, funds or economic resources available, as set out in Article 2 (1) or (2) of *Council Regulation (EC) No 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and Belarus' involvement in Russia's aggression against Ukraine* (hereinafter: Regulation 765/2006) or Article 2 of *Council Regulation (EU) No 269/2014 of 17 March 2014 on restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine* (hereinafter: Regulation 269/2014), or the obligation to communicate promptly the information required under Article 4(2) or 5 of Regulation 765/2006 or under Article 7(1) or 8 of Regulation 269/2014; or fail to comply with the prohibition on knowingly and intentionally participating in activities the object or effect of which is to circumvent the application of the measures set out in Article 2(1) or (2) of Regulation 765/2006 or Article 2 of Regulation 269/2014.

One has to agree with Pape that despite the comprehensiveness of the sanctions, their imposition on the Russian Federation has been a failure. They are undoubtedly harsh on the economy[24], but they do not actually force Russia to stop its

[22] The list is independent of the lists of persons and entities set out in Regulations 765/2006 and 269/2014, as the scope of measures applicable to persons and entities included in it may not duplicate the scope of measures laid down in respect of them in those Regulations (Article 2(2) of the aforementioned Act). As updated on 29 February 2024 by the Ministry of Internal Affairs, the list included 427 individuals and 82 entities. At the same time, 1 natural person and 8 entities were removed from the list between 2022 and 2023. As a result, 426 natural persons and 74 entities remained sanctioned as at the aforementioned date.

[23] Article 6 of the *Act on special solutions to prevent support for aggression against Ukraine and to protect national security*.

[24] This is confirmed, among other things, by the recorded decline in Russian gross domestic product (GDP). According to analyses by the World Bank, the International Monetary Fund and the Organisation for Economic Co-operation and Development, Russian GDP declined by 2.1% in 2022, with growth of 3% projected before the invasion by the Federal State Statistics Service, Rosstat (Федеральная служба государственной статистики, Росстат). See: *Wpływ sankcji na rosyjską gospodarkę* (Eng. The impact of sanctions on the Russian economy), Council of the EU, https://www.consilium.europa.eu/pl/infographics/impact-sanctions-russian-economy/ [accessed: 5 III 2024].

ongoing "military operation"[25]. The example of this country shows the full extent of the limitations on the effectiveness of the international sanctions regime.

The main factor determining the low effectiveness of the sanctions applied was, as mentioned above, the lack of unanimity of the international community on the subject, especially the negative attitude to the application of sanctions of China, India, Iran and the states of the former Soviet republics of Central Asia and the Caucasus or Turkey. Anticipation of the international community's lack of unanimity made it possible to inoculate the Russian economy and find alternatives to reduce the severity of the sanctions, as exemplified by the increase in the amount of foreign currency and gold reserves held in the years preceding the aggression against Ukraine[26]. Despite the freezing of part of Russia's foreign exchange reserves as a result of sanctions, their key reserves were preserved as a result of the CBR maintaining the highest level of reserves in gold (so-called monetary gold) deposited in vaults on the territory of the Russian Federation (21.7%), as well as placing approximately 13.8% of all reserves in China. It is also important to note that the foreign exchange reserves did not comprise only the euro and the dollar, but were successively invested primarily in the renminbi (yuan), as well as, for example, the yen and the rupee[27]. The CBR policy allowed, in the new environment, to preserve the necessary means to intervene in the foreign exchange and debt markets. Also, the loss of access to SWIFT did not turn out to be, as predicted, a 'financial nuclear weapon'[28]. Despite the application of this drastic sanction, Russian banks are still able to operate and raise cash resources to conduct business and interact with external markets. This is due to the availability of various alternatives to bypass

[25] R.A. Pape, entry on LinkedIn, https://www.linkedin.com/posts/robert-pape_someone-asked-my-view-on-how-sanctions-are-activity-6970475273985171456-6ora [accessed: 5 III 2024].

[26] *Annual value of international reserves of Russia from 2012 to 2022, by type*, Statista, https://www.statista.com/statistics/1049298/russia-international-reserves-value-by-type/ [accessed: 5 III 2024].

[27] *Bank of Russia foreign exchange and gold asset management report*, Bank of Russia, Moscow 2022, https://www.cbr.ru/Collection/Collection/File/39685/2022-01_res_en.pdf [accessed: 5 III 2024].

[28] French Finance Minister Bruno Le Maire, following a meeting of EU finance ministers on 25 February 2022, expressed the opinion that the exclusion of the FR from the SWIFT international payment system should be considered as a last resort. He stated that "SWIFT is a financial nuclear weapon. (...) The fact remains that when you have a nuclear weapon in your hands, you think before you use it. Some member countries have expressed reservations, we take them into account". Translations in the text are from the author - editor's note. See: G. Leali, *France not opposed in principle to cutting Russia from SWIFT: Bruno Le Maire*, Politico, 25 II 2022, https://www.politico.eu/article/frances-le-maire-not-against-cutting-russia-out-of-swift/ [accessed: 5 III 2024]. It should be noted that it was this sanction that was considered the most drastic, which, at the time of the Russian invasion of Crimea in 2014, resulted in the rejection of calls to exclude the Russian Federation from SWIFT already at that time, as this step was considered an excessive escalation of the conflict.

the sanctions. As a result of concerns about the exclusion of the Russian banking sector from SWIFT, the CBR had already started testing a financial message transmission system, the so-called SPFS (Система передачи финансовых сообщений), during the annexation of Crimea in 2014. According to a CBR statement, by July 2023, the system was already processing 70% of domestic financial transactions[29]. However, it is not exclusively for domestic settlements. As of January 2024, it is used by 557 entities, including 157 foreign entities from 20 countries[30]. An option for circumventing sanctions is also the use of the cross-border interbank payment system - CIPS (Chinese Cross-Border Interbank Payment System) - and its possible integration with the SPFS, especially for Sino-Russian cross-border settlements.

Despite the negative impact on the economy and social conditions, sanctions have also not triggered significant political changes, but on the contrary have unleashed a large adaptive potential that has facilitated the stabilisation of the economic situation. It is projected that in the long run, as a result of increasing control of the economy and the entrenchment of the model of state capitalism, this may also contribute to further empowerment of the authorities[31].

Cryptocurrency as an object of sanctions against the Russian Federation

In February 2022, Bloomberg, citing Russian government estimates[32], reported that Russian citizens held RUB 16.5 trillion (USD 214 billion) worth of crypto assets, which represented 12% of the global total. It was estimated that more than 17 million Russians held such assets[33]. According to the Cambridge Centre for Alternative Finance (CCAF)'s 2021/2022 assessments, Russia was also one of the top

[29] *В ЦБ сообщили о 70% внутрироссийского трафика у национального аналога SWIFT*, Известия, 3 VII 2023, https://iz.ru/1538263/2023-07-03/v-tcb-soobshchili-o-70-vnutrirossiiskogo-trafika-u-natcional nogo-analoga-swift [accessed: 5 III 2024].

[30] *Российский аналог SWIFT распространяется на Восток*, News.Ru, 27 I 2024, https://news.ru/economics/rossijskij-analog-swift-rasshiryaet-svoe-vliyanie [accessed: 5 III 2024].

[31] I. Wiśniewska, *Russian economy in 2022. Adaptation and a growing budget gap*, OSW, 16 II 2023, https://www.osw.waw.pl/en/publikacje/osw-commentary/2023-02-16/russian-economy-2022-adaptation-and-a-growing-budget-gap [accessed: 5 III 2024].

[32] The estimate was based, among other things, on an analysis of the IP addresses of the largest users of cryptocurrency exchanges.

[33] E. Pismennaya, *Russia Values Local Crypto at $200 Billion as Rules Near*, Bloomberg, 1 II 2022, https://www.bloomberg.com/news/articles/2022-02-01/russia-values-local-crypto-market-at-200-billion-as-rules-near#xj4y7vzkg [accessed: 5 III 2024].

five mining centres for bitcoin - providing 4.66% of its global production[34]. Confirming fears that cryptocurrencies could be a significant loophole in the financial sanctions regime targeting Russia and a way to limit their impact, there were reported increases in trading volumes between the rouble and the major cryptocurrencies[35]. In response to this threat, the so-called *Compliance package* of 9 March 2022 relating to Belarus clarified that the non-exhaustive definition of funds in Regulation 269/2014 also includes cryptocurrencies, and the definition of economic resources may also apply to certain cryptoassets. Accordingly, cryptoassets were to be subject to the asset-freezing provisions and the prohibition on making funds or economic resources available to persons on sanctions lists. It was also considered that, for the purposes of Regulation 833/2014, transferable securities include cryptoassets with the exception of payment instruments. In addition, it was emphasised that cryptoassets should not be used to circumvent any EU sanctions[36].

However, key restrictions in this area were only introduced as part of the fifth package of sanctions on 8 April 2022. At that time, it was decided to prohibit the provision of services involving the provision of crypto wallets, accounts or cryptoasset storage to Russian nationals or natural persons resident in Russia, or legal persons, entities or bodies based in Russia, if the total value of the cryptoassets of the natural or legal person, entity or body per wallet or account provider or per cryptoasset storage entity exceeds EUR 10,000[37]. This sanction has been tightened in the Eighth Package of 5 October 2022 by adopting a total ban on such services to the above-mentioned persons and entities, regardless of the value of the wallet amount[38].

---

[34] *Bitcoin Mining Map*, CCAF, https://ccaf.io/cbnsi/cbeci/mining_map [accessed: 5 III 2024].

[35] Following the introduction of the sanctions in February 2022, an increase in turnover was particularly observed on tether and bitcoin purchase transactions, which was primarily conditioned by the initial drastic fall in the value of the rouble. See: T. Wilson, *Rouble-crypto trading soars as sanctions hit Russian currency*, Reuters, 28 II 2022, https://www.reuters.com/markets/europe/rouble-crypto-trading-soars-sanctions-hit-russian-currency-2022-02-28/ [accessed: 5 III 2024].

[36] Press release from the European Commission: *Ukraine: EU agrees to extend the scope of sanctions on Russia and Belarus*, 9 III 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1649 [accessed 5 III 2024]; *Crypto-assets. Relevant provision: Article 5b(2) of Council Regulation (EU) No 833/2014. Frequently asked question*s, UE, 21 III 2023, https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [accessed: 5 III 2024].

[37] Article 1(18) of *Council Regulation (EU) 2022/576 of 8 April 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.*

[38] Article 1(10) of *Council Regulation (EU) 2022/1904 of 6 October 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.*

Cryptocurrency as a source of vulnerability in the international financial sanctions regime

Some commentators[39] did not attribute much importance to the possibility of a loophole in the financial sanctions regime. They mainly pointed to the reduced liquidity of the cryptocurrency market, which could not meet the scale of Russian needs. Hence, it was considered that the Russian Federation more broadly would not be able to replicate the strategy of Iran, which legalised cryptocurrency payments on imports in the face of sanctions. However, it should be noted that in a situation of tightening Western sanctions, the Russian side was considering formalising the possibility of using cryptocurrencies in cross-border settlements[40].

It also highlighted the error of seeing decentralisation as a guarantee that users would remain fully anonymous[41]. Blockchain technology is a public ledger of activity, enabling the monitoring of fund flows between wallets. However, this argument was dismissed in the face of the indication that identification on blockchain is based on public key addresses, rather than real identity, potentially allowing for the avoidance of sanctions when a false identity is used. Sceptics considered such a threat to be marginal in view of the fact that the majority of cryptocurrency

[39] See: *Cryptocurrencies: a way to evade sanctions?*, BAFFI – Centre on Economics, Finance and Regulation, https://baffi.unibocconi.eu/research-units/mints-alternative-monies/newsletter/issue-0/cryptocurrencies-way-evade-sanctions [accessed: 5 III 2024].

[40] The main opponent of the implementation of such a solution is the CBR which is extremely sceptical of the cryptocurrency market itself. This institution also had the greatest influence on the content of Federal Law No. 331-FZ "On the amendment of certain legislative acts of the Russian Federation and on the suspension of certain provisions of Article 5(1) of the Federal Law «On banks and banking activities»", amending Federal Law No. 259-FZ "On digital financial assets, digital currency and amendments to certain legislative acts of the Russian Federation", by adding in its Article 4(10) which reads: "It is forbidden to accept digital financial assets as a means of payment or other remuneration for donated goods, work performed, services rendered, as well as in any other way allowing payment for goods (work, service) with a digital financial asset, except in cases provided for by federal laws". However, in view of the Russian Ministry of Finance's articulation of the expectation that cryptocurrencies can be used as a means of cross-border settlement, the CBR promotes the use of the digital rouble in this regard. See: *ЦБ предложил дать зарубежным банкам доступ к цифровому рублю с 2025 года*, RBC.ru, 10 X 2023, https://www.rbc.ru/finances/10/10/2023/6523e87b9a7947b24f71b430 [accessed: 5 III 2024].

[41] See: C.S. Wright, *Bitcoin Is Anything BUT Anonymous*, Bitcoin & Blockchain Tech, 1 IX 2019, https://craigwright.net/blog/bitcoin-blockchain-tech/bitcoin-is-anything-but-anonymous/ [accessed: 5 III 2024]. The concept of anonymity should be distinguished from privacy and confidentiality. Complete anonymity may be an unnecessary and in most cases undesirable element, while it is possible to maintain privacy and confidentiality while accepting the requirement to prove one's identity. Thus, privacy hides the details of a transaction from the public at large, but not from those involved in the exchange, and not from those who are authorised by law to monitor exchanges.

trading takes place with intermediaries, such as cryptocurrency exchangers and exchanges or cryptocurrency wallet providers. Due to these factors, in most jurisdictions this trading is subject to anti-money laundering and anti-terrorist financing regulations. A large number of cryptocurrency exchanges also implement Know Your Customer, KYC, principles[42].

For example, in the Polish *Act of 1 March 2018 on the prevention of money laundering and terrorist financing*, due to the introduction of a legal definition of the virtual currency concept (Article 2(2)(26)), the catalogue of obliged institutions was expanded to include entities that are engaged in the business of providing the following services: exchange between virtual currencies and means of payment, exchange between virtual currencies themselves, intermediation in their exchange, as well as maintaining their accounts (so-called wallets)[43]. As a result, entities providing such services remain obliged to fulfil AML/CFT tasks[44].

However, cryptocurrency, as mentioned, can provide solutions to avoid financial sanctions, especially individual ones. These include, for example:

- chain-hopping - involving a rapid change of cryptographic assets to make a change to the blockchain that makes it difficult to trace the flow of funds[45],
- mixers, tumblers, foggers - services that mix potentially identifiable or tainted cryptocurrency funds with others in order to make it impossible to trace their true source,
- non-hosted wallets - which allow funds to be moved without being monitored by cryptocurrency exchanges, unlike the hosted wallets they provide; however, they require disclosure if one wishes to exchange cryptocurrency

[42] KYC is a mandatory process for financial institutions to identify and verify a customer's identity when they open an account and then re-evaluate that customer on a cyclical basis.

[43] Article 2(1)(12) of the Act on the prevention of money laundering and terrorist financing recognises the aforementioned entities as obliged institutions, which, inter alia, are obliged to apply security measures in the case of an occasional transaction using virtual currency of the equivalent of EUR 1,000 or more (Article 35(1)(2)(c) of the aforementioned Act). At the same time, the activity in the field of virtual currencies itself is a regulated activity within the meaning of the provisions of the Act of 6 March 2018 - Entrepreneurs' Law and may be performed after obtaining an entry in the register of activities in the field of virtual currencies made by the Minister of Finance. At the same time, it is necessary to meet the requirements of not having a criminal record and having relevant knowledge or experience when performing this type of activity (Articles 129m-129w of the Act).

[44] AML/CFT (*Anti Money Laundering/Counter Financing of Terrorism*) – a summary definition of the rules and principles that financial service providers are required to apply to prevent money laundering and terrorist financing.

[45] This technique has been used effectively by, among others, the North Korean group Lazarus to conceal the transfer path of funds stolen from cryptocurrency exchanges.

for fiat currency. Nevertheless, it is then possible to use exchanges in jurisdictions with low AML/CFT or KYC requirements,
– privacy-oriented cryptocurrencies, the so-called privacy tokens or private coins - their use is close to the implementation of the idea of anonymous transactions, because despite the visibility of the transaction itself in the public ledger (blockchain), the addresses of the wallets of the parties to the transaction remain invisible. An example of this is the cryptocurrency monero, which uses hidden addresses in transactions to protect the privacy of the recipient[46], but for the protection of the sender uses so-called ring signatures, which involve combining the user's account key with public keys from the blockchain,
– decentralised finance (DeFi) - based on peer-to-peer (P2P) exchange[47].

Despite the importance of Financial Intelligence Units (FIUs)[48] in relation to cryptocurrencies, the key role of financial sanctions enforcement falls to commercial financial institutions. These, subject to strict supervisory regulation by states, are forced to track the sources of money flows and verify that parties to transactions are not on sanction lists. When an entity is subject to financial sanctions, it becomes necessary for it to seek alternative solutions to preserve its ability to move capital. This is where the potential of cryptoassets as an instrument for circumventing sanctions lies. The existence of digital assets in the virtual space has the fundamental advantage that financial transactions can take place bypassing monitored markets, global payment networks or strictly regulated financial systems.

At the time of the introduction of EU sanctions, the market for payment tokens (bitcoin, altcoin and stablecoin) and investment and utility tokens remained effectively outside the regulation and supervision of the EU and its member states.

Pursuant to Polish regulations, the cryptocurrency market is not identified as a financial market segment within the meaning of the provisions of the *Act of 21 July 2006 on financial market supervision*. Thus, the Polish Financial Supervision Authority only supervises the activities of virtual currency exchanges and

[46] In order to avoid recording the recipient's wallet address on the blockchain, a Stealth Address system is used in which each transaction is sent to a unique, one-off address. The recipient has access to the funds sent to the stealth address, without revealing connections to the real public wallet and transaction history.

[47] Such a catalogue of possible solutions was pointed out, among others, in the document: K.E. Busch, P. Tierno, *Russian Sanctions and Cryptocurrency*, Congressional Research Service, 4 V 2022, https://crsreports.congress.gov/product/pdf/IN/IN11920 [accessed: 5 III 2024].

[48] In Poland, the main element of the anti-money laundering and terrorist financing system is the General Inspector of Financial Information, which performs its tasks through the Financial Information Department separated within the structure of the Ministry of Finance.

bureaux de change related to the provision of payment services by these entities on the basis of the stipulations of the *Act of 19 August 2011 on payment services*.

Cryptocurrency exchanges take place through encrypted transfers between wallets using a two-key mechanism: transfers require a public key, which is the address of the wallet, and a private key, which acts as a password. Both keys are alphanumeric codes. As mentioned earlier, wallets can be custodial (trusted, hosted), which involves the investor entrusting a third party with the management and protection of its wallet keys. This results in the custodian assuming responsibility for the investor's property. At the opposite extreme are so-called non-custodial (non-trustee, non-hosted) wallets. There are important differences between these types of wallets. First and foremost, custodian wallet owners entrust their private keys to crypto-asset service providers (CASPs), while both the private and public keys of non-custodian wallets are at the sole disposal of their owners, who make transfers via P2P transactions. Service providers, being the intermediary platform, will require at least bank account or credit card details to be disclosed in order to identify the customer. Non-trusted wallets, on the other hand, do not require a trusted intermediary in the form of an external institution to guarantee the security of the transaction. The second major difference is that transactions between custodial wallets are not stored on the blockchain until the funds are withdrawn from the CASP, whereas P2P transactions are immediately recorded.

CASPs, compared to the banking sector, have far fewer enforcement tools to identify customers, despite being formally bound by the same AML/CFT requirements that apply to financial institutions. This raises difficulties for non-custodial wallets, as only some transaction data on the blockchain is recorded by P2P transfers. As a result, establishing ownership of such wallets would require linking transaction details to the IP addresses of the parties to the transaction[49].

[49] A separate problem is that illicit money transfers are also facilitated by the vulnerability of blockchain and CASPs to cyberattacks, which involves secondary vulnerabilities. An example is taking control of 51% of the blockchain's computing power (hush rate) and, as a result, gaining the ability to modify or change details of transactions that have not yet been approved. Similarly, it is possible to exploit so-called cross-chain bridges, which are decentralised platforms that ensure the transfer of tokens between separate networks and guarantee the interoperability of cryptocurrency ecosystems. At the same time, attacks enable anonymity in P2P transactions. Normally, such transfers are encrypted but not anonymous, allowing payers to be identified through details and encrypted aliases stored on the blockchain by linking transactions to personal computers via IP addresses. As this information is masked or altered on the blockchain prior to validation, cyberattacks allow illegal transactions to take place without risk of identification. In the case of CASPs, the application of criminal procedures against them is made all the easier by the fact that these institutions are custodians for many wallets.

This situation will be changed, at least in part, by the entry into force of the provisions of *Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on cryptocurrency markets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937* (the so-called MiCA Regulation). It establishes a legal framework for service providers for both cryptocurrency and consumer protection. These regulations are intended to strengthen the protection of purchasers and holders of cryptocurrencies and, as a consequence, affect not only the security of trading but, above all, its transparency. The regulation distinguishes between three types of cryptoassets, i.e. asset-linked tokens (ART), tokens that are electronic money (EMT) and utility tokens. The provision of a crypto-asset service will only be allowed by legal entities established in an EU Member State that have been authorised as a provider of such services[50]. With that said, the MiCA regulation makes it easier for entities such as credit institutions, brokerage houses, CSDs or e-money institutions to provide them, as it does not require them to obtain a licence to provide crypto services. Only the requirement to notify the competent supervisory authority is established[51].

The MiCA Regulation pays particular attention to money laundering and terrorist financing issues in relation to sanctions. In addition to the fact that CASPs will be included in the catalogue of obliged institutions under AML, at the same time the AML and privacy (anonymity) threads refer, inter alia, to the prohibition of the release of cryptoassets that have a built-in anonymisation function[52]. A CASP operating a cryptocurrency trading platform will have to have procedures in place to prevent its infrastructure from being used for money laundering or terrorist financing purposes, and the mere exposure of the activity

[50] The application for authorisation as a cryptoasset service provider will mainly have to include: a description of the procedure and system for detecting market abuse, a description of the principles of the cryptoasset trading platform, a description of the provider's IT systems and security solutions. A register of cryptoasset service providers will be maintained by the European Securities and Markets Authority (ESMA).

[51] At the same time, it is explicitly indicated in the MiCA Regulation that certain services can only be provided by certain entities. This includes making a public offering or applying for admission to trading of EMTs, which can only be done by a credit institution or an e-money institution that is also the issuer of such a token (Article 48(1) of the MiCA Regulation). Similarly, credit institutions will not be required to obtain a licence to offer to the public or apply for admission to trading of ART. As in the case of a CASP licence, in this respect the credit institution is required to draw up an information document, appropriate documentation and to notify the supervisory authority [paragraph (44) of the preamble and Article 17 of the MiCA Regulation].

[52] Except when the CASP running the trading platform will be able to identify crypto holders and transaction history.

by the CASP's governing body to the risk of money laundering is a mandatory ground for refusal of authorisation. The lack of effective internal AML procedures, on the other hand, will be an obligatory ground for revocation of the licence. In addition, the current obligation to apply KYC procedures starting at €1,000 in the absence of any suspicion of a customer carrying out a transaction in future will be reduced to €1. This will result in an obligation to verify every transaction and thus to use financial security measures. This will significantly affect anonymity, particularly in terms of exchanging cryptocurrencies for fiat currencies. Non-EU entities will in principle lose the possibility to offer cryptocurrency services within the Union. At this point in time, however, the MiCA Regulation does not refer to the situation of entities from the European Free Trade Association (EFTA) and the European Economic Area (EEA). The territorial scope of the MiCA Regulation is, however, limited as a result of allowing third-country firms to carry out the activities covered by its scope in a reverse solicitation model, i.e. on the sole initiative of the client[53].

The MiCA regulations, in an area where they introduce transparent regulation of the flow of cryptoassets, are seen as a source of increasing the effectiveness of sanctions. However, it should be taken into account that the EU regulation will only formally take effect from 30 December 2024, with a transitional period until even 1 July 2026 during which CASPs may continue to provide services in an unregulated manner. It is important to note that the MiCA Regulation did not cover a number of sensitive issues[54], including those related to international sanctions,

[53] Based on well-established interpretations under, inter alia, the regulations of *Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU* (the so-called Markets in Financial Instruments Directive, MiFID II), however, the model of providing a service at the sole initiative of the client should not apply in situations where: undertaking promotional campaigns targeting a particular market, creating a permanent business model based on reverse solicitation, actively soliciting service recipients from another country, having a website with a particular country domain, and initiating the publication of press releases in portals or magazines dedicated to a particular market.

[54] The MiCA does not, for example, address so-called security tokens, which can be considered as tradable securities, and other cryptoassets that constitute financial instruments within the meaning of MiFID II, as well as deposits, securitisation positions and insurance and pension products. Similarly, the MiCA Regulation does not cover the issue of unique (non-fungible tokens) - (NFTs) to the most important extent, unless they replicate a financial instrument or where the issuer creates a 'pool' of assets for purchase.

which is particularly true for decentralised finance (DeFi)[55] and Central Bank Digital Currency (CBDC)[56].

With the entry into force of the MiCA Regulation, the complementary *Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying funds transfers and certain cryptoassets and amending Directive (EU) 2015/849* (hereinafter: TFR Regulation) will become applicable. It implements the recommendations of the Financial Action Task Force (FATF) on the so-called travel rule. In this respect, there will be an extension of the obligations for EU payment service providers (including CASPs) to monitor transfers of both cash and crypto-assets, which will involve the obligation to provide detailed information on the payer (originator) and recipient of the transaction (beneficiary). However, the Travel Rule, as with the MiCA, will not apply where the initiator of the transaction and the beneficiary are PSPs or CASPs acting on their own behalf, as well as in transfers between persons carried out without the involvement of a CASP (Article 2(4) of the TFR Regulation)[57].

The sanction gap of decentralised finance

As signalled earlier, paragraph (22) of the preamble of the MiCA Regulation specifies that cryptocurrency-related services, as defined in the Regulation, do not fall within the scope of regulation when provided in a fully decentralised manner, without intermediaries. Despite this, the issue of DeFi raises quite a few questions under the MiCA Regulation. For example, a problem arises regarding the provision

[55] Recital (22) of the preamble to the MiCA Regulation stipulates the exclusion of the application of the Regulation provisions to crypto services provided in a fully decentralised manner without intermediaries. However, the MiCA Regulation contains review clauses under Articles 140(2)(t) and 142(2)(a) - insofar as they relate to decentralised finance - which mandate reporting on the assessment of the development of DeFi in crypto markets and the appropriate regulatory treatment of decentralised crypto systems, including an assessment of the necessity and feasibility of regulating decentralised finance.

[56] Recital (13) of the preamble to the MiCA Regulation specifies that it does not apply to digital assets issued by central banks acting as monetary authorities, which includes CBDCs. Similarly, related services provided by these central banks acting as monetary authorities are not subject to the EU framework.

[57] The first exception follows directly from the fact that the TFR Regulation does not apply to transfers of funds for which the payer and the payee are payment service providers acting on their own account (Article 2(4)(c) of the TFR Regulation). The second exception, on the other hand, stems from the scope of Article 2(1) of the TFR Regulation, i.e. the application only to payment service providers, crypto-asset service providers or intermediary payment service providers established in the EU.

of cryptocurrency exchange services or the operation of cryptocurrency trading platforms within decentralised exchanges (so-called DEX). This is because there are problems in deciding what full decentralisation is within the meaning of the regulation. This difficulty relates to the peculiarities of the construction of the blockchain network, which results in DeFi using a hierarchical layered architecture with different purposes[58]. Under the MiCA Regulation, it remains unresolved which aspect of decentralisation is at stake, as it can be referred to both in relation to the settlement layer[59], the way cryptocurrencies are stored, and the management of the organisation and ownership of the protocol. Due to the lack of clarity in the MiCA Regulation, the assessment of the degree of decentralisation is left to the sole discretion of the crypto service provider, who is expected to define their business model through this prism.

In the current environment of technological development, it is difficult to imagine the establishment of a regulatory framework over decentralised finance that would provide a real possibility of enforcement. This is supported by the problem of defining an appropriate legal order governing market access and supervision rules, due to the high geographical dispersion of users and the lack of central entities responsible for providing services. Given this, the real gap in the international sanctions regime in the future will be decentralised finance, as a new model for organising financial transfers without any intermediaries, with the automatic execution of transactions concluded through smart contracts, which are protocols that operate on the blockchain network.

As a kind of ecosystem of decentralised financial applications based on this technology, DeFi offers the possibility of a wide range of contracts. In essence, the system replicates existing financial service models bypassing their centralised intermediaries[60]. As a result, under DeFi, users retain full control of their assets

[58] A distinction is made between three essential layers, i.e. billing, protocol and interfaces. The billing layer (layer one) consists of the distributed ledger technology (DLT) and its native resource, containing the basic principles of the ecosystem. The protocol layer (layer two) includes the compiler, providing the ability to create application programming interfaces. An application programming interface (API) is a set of definitions and protocols for building and integrating application software. In the interface layer (layer three), user-oriented applications are developed, allowing interaction with the application via a web page. See: G. Maia, J. Vieira dos Santos, *MiCA and DeFi ("Proposal for a Regulation on Market in Cryptoassets" and "Decentralised Finance")*, "Revista Electrónica de Direito" 2022, vol. 28, no. 2, pp. 63–65.

[59] In this layer, a network of nodes not relying on a central server or central organisation consists of an unprivileged blockchain through P2P connections between unrelated and independent agents.

[60] E. Avgouleas, A. Seretakis, *How Should Crypto Lending Be Regulated Under EU Law?*, "European Business Organization Law Review" 2023, vol. 24, n. 3, pp. 423–424. https://doi.org/10.1007/s40804-023-00293-3.

through synergies with the ecosystem via decentralised P2P applications. These applications also do not need entities to settle possible disputes[61], as the predetermined code will do this on its own in predictable situations, as a so-called Lex Cryptographia[62], and thus according to rules governed by self-executing smart contracts and decentralised (autonomous) organisations[63]. However, with the acceptance of the 'code is law' idea comes the effect of technology displacing state legal systems[64].

When analysing the issue of smart contract, it is important to refer to the original definition of the term proposed by Nick Szabo, who described it as a computerised transactional protocol that automatically implements the terms of a contract. The design goals are to meet typical contractual conditions, minimise the occurrence of exceptions (both malicious and accidental) and eliminate any trusted intermediaries[65]. Indeed, the idea is based on the exclusion of the need for trust between the parties due to the increased certainty of performance of the contract, as designed, as a result of the guarantee of unalterability of the contract (code). Therefore, from an economic point of view, mental and computational additional costs are reduced, lowering the losses associated with potential fraud, arbitration and enforcement costs as well as transaction costs.

---

[61] Through a probabilistic approach, blockchain solved the reconciliation issue considered in game theory, cryptography and distributed systems theory, identified in 1980 by Marshall C. Pease, Leslie Lamport and Robert Shostak as the problem of Byzantine generals. See: M. Pease, L. Lamport, R. Shostak, *The Byzantine Generals Problem*, "ACM Transactions on Programming Languages and Systems" 1982, vol. 4, n. 3, pp. 382–401. https://doi.org/10.1145/357172.357176.

[62] Blockchain significantly changes the way law is understood by detaching it from the need for any cultural backing or legitimisation by state authority. According to Katrin Becker, blockchain decouples the concept of law from the three key dimensions of territory, language (and associated interpretation) and matter. See: K. Becker, *Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*, "Law and Critique" 2022, vol. 33, pp. 113–130. https://doi.org/10.1007/s10978-021-09317-8.

[63] A. Wright, P. De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, SSRN, 12 III 2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, p. 4 [accessed: 5 III 2024]. http://dx.doi.org/10.2139/ssrn.2580664.

[64] D.A. Zetzsche, D.W. Arner, R.P. Buckley, *Decentralized Finance*, "Journal of Financial Regulation" 2020, vol. 6, n. 2, p. 184. https://doi.org/10.1093/jfr/fjaa010.

[65] N. Szabo, *Smart Contracts*, 1994, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html [accessed: 5 III 2024]; the same, *Smart Contracts: Building Blocks for Digital Markets*, 1996, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_ contracts2.html [accessed: 5 III 2024].

Currently, the term 'smart contract' is defined as an implementation code running in a blockchain environment[66]. In this sense, it is algorithmic code in a computer program, typed and based on data in a blockchain[67]. All commitments in smart contracts remain in accordance with the classical Boolean logic[68], underlying all digital processing, i.e. 'if this then that' (IFTTT).

In the context of international sanctions, an important threat to their real effectiveness is the possibility of aggregating multiple contracts by creating applications with advanced functionalities. Examples include lending platforms[69], liquidity pools[70], social media platforms or distributed asset management systems (so-called decentralised autonomous organisations). It should be emphasised that smart contracts escape the legal regulation of the MiCA Regulation, nor are they defined in Polish legislation and other legal regimes. Of course, it can be assumed that the construction of these contracts resembles a specific type of automated deposit (escrow) or electronic bill of exchange. In legal terms, a smart contract could be regarded as a special form of contract, but only on the assumption that its conclusion is based on a conscious declaration of intent by the parties that they wish

[66] V. Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2014, https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [accessed: 5 III 2024].

[67] R. Wilkens, R. Falk, *Smart Contracts. Grundlagen, Anwendungsfelder und rechtliche Aspekte*, Wiesbaden 2019, pp. 3–4.

[68] George Boole in 1854 created the so-called Boolean algebra - a mathematical structure consisting of three binary operations: ∨ (or, or, alternative) - an action similar to addition; ∧ (i, and, conjunction) - equivalent to multiplication; ~ (no, not, logical negation) and the distinguished elements 0 (false), 1 (true). See: S. Givant, P. Halmos, *Introduction to Boolean Algebras (Undergraduate Texts in Mathematics)*, New York 2009, pp. 8–9.

[69] The funds lent on lending platforms by their users are provided by the users themselves, and consequently the provision of funds to such services is a *staking* within the same platform. An example is the MakerDAO project that allows Ethereum (ETH) holders to lend money between community members in the form of stablecoin DAI (trying to maintain a 1:1 value to the US dollar). The system involves locking up a certain amount of ETH in smart contracts, which allows investors to mint new DAI and thus establish collateral for loans. Once the debt is repaid with interest, ETH is unlocked. However, when the value of the ETH falls below the amount borrowed in the DAI, the loan is liquidated by selling the ETH to repay the borrowed DAI. The mere threat of liquidation deters excessive borrowing. Indeed, in the event that the price of ETH falls sharply, DAI loans are liquidated, in which case Maker Token Holders (MKR) are the lenders of last resort. MKRs are created and sold to repay the loans, and all MakerDAO fees are also paid in them. Liquidation penalties, on the other hand, are used to repurchase MKRs, which are then incinerated.

[70] Liquidity pools are a collection of funds locked into a smart contract, which are the basis of decentralised exchanges (DEXs) such as Uniswap, which use smart contracts to facilitate transactions.

to enter into a contract with a specific content between themselves[71]. This content could, in principle, be code placed on the blockchain. The call of a code function on the blockchain would constitute the submission of an instruction generating the execution of a contract. However, to consider a smart contract as a contract in the sense of civil law would imply assuming that a fully informed declaration of intent actually took place. Fulfilment of this condition would require the parties to the smart contract to have created the code themselves, or at least to have the ability to read it, i.e. to know the programming language in which the smart contract was encoded[72]. The question arises as to whether it is at all possible to attribute the value of a conscious declaration of intent as to the content of the contract when the declaration is made in the form of a code. Hypothetically, such a problem could be disregarded if the smart contract was the subject of prior negotiations, the arrangements of which would be written down in natural language and only subsequently encoded in the smart contract. In that case, the code could only be treated in terms of a tool to implement contractual obligations and not as the basis for the creation of those obligations. However, there is no requirement to draft the smart contract in natural language. Furthermore, defining all elements in the code itself automatically guarantees that the parties to the smart contract remain fully anonymous.

Digital rouble – centralised cryptocurrency

Another factor related to cryptocurrencies and blockchain technology that may affect the weakening of the financial sanctions regime is the development of Central Bank Digital Currency (CBDC). The Bank for International Settlements defines CBDC as (...) *a digital payment instrument denominated in a national unit of account, representing a direct obligation of the central bank*[73].

On 1 August 2023, the provisions of Federal Law No. 339-FZ "Amending Articles 128 and 140 of Part One, Part Two and Articles 1128 and 1174 of Part Three of the Civil Code of the Russian Federation" and Federal Law No. 340-FZ "Amending Certain Legal Acts of the Russian Federation" came into force. These regulations constituted the blockchain-based digital rouble as the new national currency of the Russian Federation. The regulations defined the rules for its introduction into

[71] Article 60 of the *Act of 23 April 1964 - Civil Code*.

[72] Currently, the most prominent platform for the implementation of smart contracts is Ethereum, which implements a complete Turing programming language called Solidity.

[73] *Central bank digital currencies: foundational principles and core features*, Bank for International Settlements, 2020, https://www.bis.org/publ/othp33.pdf, p. 3 [accessed: 5 III 2024].

circulation and the conditions for its use in settlements. It also specified the powers of the CBR as the operator of its platform, as well as the role of credit institutions in carrying out transactions by customers and the organisational basis for the use of the digital rouble by natural and legal persons as a new payment method, including in operations for foreigners.

By 31 December 2024, the Board of Directors of the CBR, together with the Federal Financial Monitoring Service of the Russian Federation (Федеральная служба по финансовому мониторингу, Rosfinmonitoring), must define the scope of users of the digital rouble platform who will be authorised to carry out digital rouble transactions on the platform, as well as the list of permissible types of transactions and the threshold amounts for such operations. As originally envisaged, the possibility to access the digital rouble platform creates the need to open a digital rouble account, which is a new type of bank account. The parties to the digital rouble account contract will be the user and the CBR, and the financial institution where the user has a classical bank account will be the intermediary representing the CBR in its relations with the user in order to use the digital rouble platform. Russia is therefore replicating in this respect the positive Chinese experience with the implementation of the digital yuan (e-CNY).

The difference between cryptocurrencies and digital national currencies is fundamental. CBDC may resemble what is known as stablecoin - a digital currency (payment token) whose value is linked to a stable reserve asset in circulation (e.g. fiat currency or gold). Above all, CBDC, like stablecoin, and unlike altcoin, is (at least in theory) subject to marginal fluctuations in value. The key difference is that CBDC is, unlike cryptocurrencies, legal tender in the country of issue, backed by the government[74]. However, centralised digital national currencies, managed by national central banks, cannot provide users with full anonymity. Indeed, while both parties to a transaction will remain anonymous externally, they will no longer be anonymous from the central bank's point of view, which will give the authorities the opportunity to fully monitor financial flows in real time[75].

[74] Due to their specific nature, stablecoins could, in principle, meet the definition of e-money established by the *Act on payment services*.

[75] Such a variant refers to an account-based model, where transaction approval by the principal and beneficiary is based on verification of the users' identities, as their transactions are assigned to identity-based accounts. Another solution is a token-based CBDC, where the transaction is approved by the originator and beneficiary based on a public-private key pair and digital signatures. Such a system does not require access to the user's identity, which provides a high level of privacy. See: *Central Bank Digital Currencies. Building Block of the Future of Value Transfer*, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/financial-services/in-fs-cbdc-noexp.pdf [accessed: 5 III 2024].

From the perspective of the state, the CBDC provides new monetary policy tools and can be an effective instrument to influence, among other things, the dynamics of the money supply in the economy. The most important objective of implementing this instrument in the context of handling cross-border exchanges is the expectation of breaking the dominance of the dollar in trade settlements. It should be noted that the full implementation of the digital rouble includes plans to launch a platform for cross-border settlements within the post-Soviet space of the Eurasian Economic Union and the Commonwealth of Independent States, as well as with regard to the BRICS countries[76]. Consequently, the development of CBDCs from the perspective of these countries could significantly contribute to the marginalisation of the importance of Western international sanctions as these countries gain the ability to make payments without foreign commercial banks and financial infrastructure such as SWIFT[77]. It is the commercial banks that are the key link in the enforcement of Western sanctions, not only because of the powers of these banks, but also because they bear the responsibility for blocking transactions involving sanctioned entities. Because of US sanctions in particular, even institutions in countries formally not applying them, if there is a dollar element or other US link, must approach transactions with the Russian side with great caution for fear of secondary sanctions being imposed on these institutions.

In this context, a digital rouble in the future could enable cross-border payments without the need to use the banking system of other countries, by handling transactions exclusively through the CBR digital rouble platform.

[76] BRICS is a form of cooperation between countries of a political and economic nature. Originally, the group comprised Brazil, Russia, India and China and, since 2011, South Africa. As of January 2024, it was to expand its membership to include more countries, namely Argentina, Egypt, Ethiopia, Saudi Arabia, Iran and the United Arab Emirates. According to the official communication, Argentina eventually dropped its plan to join the group, while in the case of Saudi Arabia, its membership is still not officially confirmed. The main objective of this group is to create a new monetary system. See: BRICS Information Portal, http://infobrics.org/ [accessed: 5 III 2024]; K. Karwowski, *Jeden statek – różni kapitanowie. Grupa BRICS po rozszerzeniu* (Eng. One ship - different captains. The BRICS group after enlargement), Instytut Nowej Europy, 20 III 2024, https://ine.org.pl/jeden-statek-rozni-kapitanowie-grupa-brics-po-rozszerzeniu/ [accessed: 26 III 2024].

[77] K. Izenman, *The Other Side of the Digital Coin: Central Bank Digital Currencies and Sanctions*, RUSI, 26 V 2021, https://rusi.org/explore-our-research/publications/commentary/other-side-digital-coin-central-bank-digital-currencies-and-sanctions [accessed: 5 III 2024].

Conclusions

The Russian case illustrates well the problem of assessing the effectiveness of economic sanctions. Under the assumption that their purpose is to discipline and punish the countries[78] on which they are imposed, sanctions applied against the Russian Federation should be considered to have fulfilled their function. They undeniably have a negative impact on the Russian economy and its financial system, limiting the authorities' available economic and political choices, resulting in greater centralisation of the economy and dependence on available trading partners. However, from the perspective of the original and primary objective of getting the Russian Federation to abandon its military offensive in Ukraine, the sanctions applied have not had the desired effect. There is also the fundamental problem that the escalating impact of economic sanctions, negatively affecting the country's economic growth and investment capacity, is accompanied by a natural tendency to create resistance to them, as the capacity to effectively circumvent them takes shape.

The analysis presented confirms the doubt indicated at the outset regarding the real effectiveness of sanctions in view of the development of innovative financial instruments. In this context, it would be wrong to overlook the growing potential of digital assets, particularly the DeFi variant and their specific type in the form of central bank digital currencies. These instruments may, in the near future, allow for the creation of new alternative channels for financial flows, independent of the currently existing Western payment systems. Their further development could carve out a sanction-free financial transaction space and make the effects of any sanctions imposed, both financially and commercially, exclusively or predominantly negative for the countries using them. What is now a niche and marginal means of evading the enforcement of international sanctions could, in the not too distant future, become a powerful tool for shaping a new international order. This will become a challenge not only for financial market supervisory regimes, but also for those responsible for countering money laundering and terrorist financing.

Unfortunately, the question of what legal measures would fully eliminate the existence of loopholes in the international financial sanctions regime cannot be answered unequivocally, particularly with regard to the caseload of large global economies, and with a view to the further development of the possibilities of using blockchain technology. It is also utopian to expect to obtain international decision-making unanimity both on the inclusion of a country in preventive measures and on the identity of the scale and type of sanctions to be applied. Nevertheless,

[78] J. Field, *Sanctions, Russia and 'crypto crime'*, CoinGeek, 7 IV 2023, https://coingeek.com/sanctions-russia-and-crypto-crime/ [accessed: 5 III 2024].

for EU countries, the postulate should be the proper and smooth implementation of the MiCA Regulation, seeking to clearly specify the legal definition of the so-called full decentralisation concept. The aim is above all to avoid a situation in which decentralised activities unjustifiably escape the regulatory framework or room for discretion on the part of regulators as to their classification is created. Thus, with regard to decentralised finance, the *condicio sine qua non* remains the development of a basic classification mechanism (taxonomy) for this concept at the level of all member states and, more broadly, on a global scale[79].

Bibliography

Avgouleas E., Seretakis A., *How Should Crypto Lending Be Regulated Under EU Law?*, "European Business Organization Law Review" 2023, vol. 24, n. 3, pp. 421–438. https://doi.org/10.1007/s40804-023-00293-3.

Becker K., *Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*, "Law and Critique" 2022, vol. 33, pp. 113–130. https://doi.org/10.1007/s10978-021-09317-8.

Bierzanek R., Symonides J., *Prawo międzynarodowe publiczne* (Eng. Public international law), Warszawa 2003.

Demarais A., *Backfire: How Sanctions Reshape the World Against U.S. Interests*, New York 2022.

Givant S., Halmos P., *Introduction to Boolean Algebras (Undergraduate Texts in Mathematics)*, New York 2009.

Hufbauer G.C. et al., *Economic Sanctions Reconsidered: Supplemental case histories*, Washington 2007.

Maia G., Vieira dos Santos J., *MiCA and DeFi ("Proposal for a Regulation on Market in Cryptoassets" and "Decentralised Finance")*, "Revista Electrónica de Direito" 2022, vol. 28, no. 2, pp. 57–82.

Opałek K., Wróblewski J., *Prawo. Metodologia, filozofia, teoria prawa* (Eng. Law. Methodology, philosophy, theory of law), Warszawa 1991.

[79] The need for a unified systematics for DeFi and digital assets has been signalled, among others, in the document: *Decentralised Finance – Principles for building a robust digital economy*, AFME, 6 VI 2023, https://www.afme.eu/ Portals/0/DispatchFeaturedImages/AFME%20DeFi%20Whitepaper.pdf [accessed: 5 III 2024].

Opałek K., Wróblewski J., *Zagadnienia teorii prawa* (Eng. Issues in legal theory), Warszawa 1969.

Pape R.A., *Why Economic Sanctions Do Not Work*, "International Security" 1997, vol. 22, no. 2, pp. 90–136.

Pease M., Lamport L., Shostak R., *The Byzantine Generals Problem*, "ACM Transactions on Programming Languages and Systems" 1982, vol. 4, n. 3, pp. 382–401. https://doi.org/10.1145/357172.357176.

Wilkens R., Falk R., *Smart Contracts. Grundlagen, Anwendungsfelder und rechtliche Aspekte*, Wiesbaden 2019.

Zetzsche D.A., Arner D.W., Buckley R.P., *Decentralized Finance*, "Journal of Financial Regulation" 2020, vol. 6, n. 2, pp. 172–203. https://doi.org/10.1093/jfr/fjaa010.

Internet sources

Annual value of international reserves of Russia from 2012 to 2022, by type, Statista, https://www.statista.com/statistics/1049298/russia-international-reserves-value-by-type/ [accessed: 5 III 2024].

Bank of Russia foreign exchange and gold asset management report, Bank of Russia, Moscow 2022, https://www.cbr.ru/Collection/Collection/File/39685/2022-01_res_en.pdf [accessed: 5 III 2024].

Bitcoin Mining Map, Cambridge, CCAF, https://ccaf.io/cbnsi/cbeci/mining_map [accessed: 5 III 2024].

BRICS Information Portal, http://infobrics.org/ [accessed: 5 III 2024].

Busch K.E., Tierno P., *Russian Sanctions and Cryptocurrency*, Congressional Research Service, 4 V 2022, https://crsreports.congress.gov/product/pdf/IN/IN11920 [accessed: 5 III 2024].

Buterin V., *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2014, https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [accessed: 5 III 2024].

Central Bank Digital Currencies. Building Block of the Future of Value Transfer, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/financial-services/in-fs-cbdc-noexp.pdf [accessed: 5 III 2024].

Central bank digital currencies: foundational principles and core features, Bank for International Settlements, 2020, https://www.bis.org/publ/othp33.pdf [accessed: 5 III 2024].

Cryptocurrencies: a way to evade sanctions?, BAFFI – Centre on Economics, Finance and Regulation, https://baffi.unibocconi.eu/research-units/mints-alternative-monies/newsletter/issue-0/cryptocurrencies-way-eva de -sanctions [accessed: 5 III 2024].

Crypto-assets relevant pro-vision: Article 5b(2) of Council Regulation (EU) No 833/2014 – frequently asked questions, Council of the EU, 21 III 2023, https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [accessed: 5 III 2024].

Decentralised Finance. Principles for building a robust digital economy, AFME, 6 VI 2023, https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME%20DeFi%20Whitepaper.pdf [accessed: 5 III 2024].

Field J., *Sanctions, Russia and 'crypto crime'*, CoinGeek, 7 IV 2023, https://coingeek.com/sanctions-russia-and-crypto-crime/ [accessed: 5 III 2024].

Izenman K., *The Other Side of the Digital Coin: Central Bank Digital Currencies and Sanctions*, RUSI, 26 V 2021, https://rusi.org/explore-our-research/publications/commentary/other-side-digital-coin-central-bank-digital-currencies-and-sanctions [accessed: 5 III 2024].

Karwowski K., *Jeden statek - różni kapitanowie. Grupa BRICS po rozszerzeniu* (Eng. One ship - different captains. The BRICS group after enlargement), Instytut Nowej Europy, 20 III 2024, https://ine.org.pl/jeden-statek-rozni-kapitanowie-grupa-brics-po-rozszerzeniu/ [accessed: 26 III 2024].

Leali G., *France not opposed in principle to cutting Russia from SWIFT: Bruno Le Maire*, Politico, 25 II 2022, https://www.politico.eu/article/Frances-le-maire-not-against-cutting-russia-out-of-swift/ [accessed: 5 III 2024].

Pape R.A., entry on LinkedIn, https://uk.linkedin.com/posts/robert-pape_someone-asked-my-view-on-how-sanctions-are-activity-6970475273985171456-6ora [accessed: 5 III 2024].

Pismennaya E., *Russia Values Local Crypto at $200 Billion as Rules Near*, Bloomberg, 1 II 2022, https://www.bloomberg.com/news/articles/2022-02-01/russia-values-local-crypto-market-at-200-billion-as-rules-near#xj4y7vzkg [accessed: 5 III 2024].

Press release from the European Commission: *Ukraine: EU agrees to extend the scope of sanctions on Russia and Belarus*, 9 III 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1649 [accessed: 5 III 2024].

Sanctions and Restrictions Against Russia in Response to its Invasion of Ukraine, Ministry of Foreign Affairs Singapore, 5 III 2022, https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/03/20220305-sanctions/ [accessed: 5 III 2024].

Szabo N., *Smart Contracts*, 1994, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html [accessed: 5 III 2024].

Szabo N., *Smart Contracts: Building Blocks for Digital Markets*, 1996, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html [accessed: 5 III 2024].

Wilson T., *Rouble-crypto trading soars as sanctions hit Russian currency*, Reuters, 28 II 2022, https://www.reuters.com/markets/europe/rouble-crypto-trading-soars-sanctions-hit-russian-currency-2022-02-28/ [accessed: 5 III 2024].

Wiśniewska I., *Russian economy in 2022. Adaptation and a growing budget gap*, OSW, 16 II 2023, https://www.osw.waw.pl/en/publikacje/osw-commentary/2023-02-16/russian-economy-2022-adaptation-and-a-growing-budget-gap [accessed: 5 III 2024].

Wpływ sankcji na rosyjską gospodarkę (Eng. The impact of sanctions on the Russian economy), Rada UE, https://www.consilium.europa.eu/pl/infographics/impact-sanctions-russian-economy/ [accessed: 5 III 2024].

Wright A., De Filippi P., *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, preprint, SSRN, 12 III 2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 [accessed: 5 III 2024]. http://dx.doi.org/10.2139/ssrn.2580664.

Wright C.S., *Bitcoin Is Anything BUT Anonymous*, Bitcoin & Blockchain Tech, 1 IX 2019, https://craigwright.net/blog/bitcoin-blockchain-tech/bitcoin-is-anything-but-anonymous/ [accessed: 5 III 2024].

Russian Internet sources

В ЦБ сообщили о 70% внутрироссийского трафика у национального аналога SWIFT, Известия, 3 VII 2023, https://iz.ru/1538263/2023-07-03/v-tcb-soobshchili-o-70-vnutrirossiiskogo-trafika-u-natcionalnogo-analoga-swift [accessed: 5 III 2024].

ЦБ предложил дать зарубежным банкам доступ к цифровому рублю с 2025 года, RBC.ru, 10 X 2023, https://www.rbc.ru/finances/10/10/2023/6523e87b9a7947b24f71b430 [accessed: 5 III 2024].

Российский аналог SWIFT распространяется на Восток, News.Ru, 27 I 2024, https://news.ru/economics/rossijskij-analog-swift-rasshiryaet-svoe-vliyanie [accessed: 5 III 2024].

Legal acts

Council Regulation (EU) 2024/745 of 23 February 2024 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (Official Journal of the EU L of 23 February 2024).

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on cryptocurrency markets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Official Journal of the EU L 150/40 of 9 June 2023).

Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying funds transfers and certain cryptoassets and amending Directive (EU) 2015/849 (Official Journal of the EU L 150/1 of 9 June 2023).

Council Regulation (EU) 2022/1904 of 6 October 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (Official Journal of the EU LI 259/3 of 6 October 2022).

Council Regulation (EU) 2022/576 of 8 April 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's destabilising action in Ukraine (Official Journal of the EU L 111/1 of 8 April 2022, as amended).

Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (Official Journal of the EU L 229/1 of 31 July 2014, as amended).

Council Regulation (EU) No 269/2014 of 17 March 2014 on restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine (Official Journal of the EU L 78/6 of 17 March 2014, as amended).

Council Regulation (EU) No 359/2011 of 12 April 2011 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran (Official Journal of the EU L 100/1 of 14 April 2011, as amended).

Council Regulation (EC) No 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and its involvement in Russia's aggression against Ukraine (Official Journal of the EU L 134/1 of 20 May 2006, as amended).

Act of 13 April 2022 on special solutions to prevent support for aggression against Ukraine and to protect national security (consolidated text of Journal of Laws 2023, item 1497, as amended).

Act of 6 March 2018 - Entrepreneurs' Law (consolidated text of Journal of Laws 2023, item 221, as amended).

Act of 1 March 2018 on the prevention of money laundering and terrorist financing (consolidated text of Journal of Laws 2023, item 1124, as amended).

Act of 19 August 2011 on payment services (consolidated text of Journal of Laws 2022, item 2360, as amended).

Act of 21 July 2006 on financial market supervision (consolidated text of Journal of Laws 2023, item 753, as amended).

Act of 23 April 1964 - Civil Code (consolidated text of Journal of Laws 2023, item 1610, as amended).

Russian legal acts

Федеральный закон от 31.07.2020 N 259-ФЗ "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации", Kremlin.ru, http://www.kremlin.ru/acts/bank/45766/page/1 [accessed: 5 III 2024].

Федеральный закон от 14.07.2022 № 331-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации и о приостановлении действия отдельных положений статьи 5.1 Федерального закона «О банках и банковской деятельности»", http://publication.pravo.gov.ru/Document/View/0001202207140083?index=1 [accessed: 5 III 2024].

Федеральный закон от 24.07.2023 № 339-ФЗ "О внесении изменений в статьи 128 и 140 части первой, часть вторую и статьи 1128 и 1174 части третьей Гражданского кодекса Российской Федерации", http://publication.pravo.gov.ru/document/0001202307240009 [accessed: 5 III 2024].

Федеральный закон от 24.07.2023 № 340-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации", http://publication.pravo.gov.ru/Document/View/0001202307240024 [accessed: 5 III 2024].

Angela Pacholczak

Graduate of doctoral studies at the Faculty of Law and Administration of the University of Warsaw.

Contact: angelapacholczak@gmail.com

Yezhov's infiltration model and the Russian Federation's seizure of Crimea

MAREK ŚWIERCZEK

Internal Security Agency

https://orcid.org/0000-0002-0661-0315

Internal Security Review, 2024, no. 30: 385–411

https://doi.org/10.4467/20801335PBW.24.016.19618

ARTICLE

Abstract

The author analysed the scale of betrayal among the officers and officials of the Ukrainian state during the annexation of Crimea by the Russian Federation in 2014. The main research problem was an attempt to explain the anomaly in the activities of the special services in the form of recruiting 1,400 officers of the Ukrainian SBU to the Russian FSB. In an attempt to explain this phenomenon in the practice of secret services, the author used the theory of offensive intelligence and counterintelligence created and developed in the USSR from the early 1920s, as well as the findings of cognitive psychology regarding the phenomenon of projection as the main mechanism for explaining the behavior of other people. Thanks to the synthesis of psychology and the analysis of the theoretical achievements of the Soviet secret services, the author put forward a hypothesis about the mass recruitment of the SBU officers in the Crimea long before the annexation. According to the author, the main mechanisms of mass recruitment of agents in order to control the opponent's organisation were broadly understood corruption and cronyism characteristic to the post-Soviet area.

Keywords

annexation of Crimea, FSB, SBU, corruption as a factor of betrayal, offensive counterintelligence

On 21 February 2014, Ukrainian President Viktor Yanukovich signed an agreement with the opposition providing, among other things, for a return to the 2004 Constitution (which severely limited presidential powers) and the holding of early presidential elections by the end of 2014. Later the same day, Yanukovich left Kiev for Kharkiv to attend a congress of deputies of the south-eastern regions. He later maintained that there had been a failed attempt on the presidential column during this trip[1].

Under pressure from a demonstration of several thousand people with armed Right Sector militias, on 22 February the Verkhovna Rada of Ukraine adopted a resolution stating that, by leaving Kiev, Yanukovich had abandoned his presidential duties. A date for new elections for head of state was set for 25 May. 328 MPs voted in favour of the resolution (including MPs who had until recentlybeen part of the government majority). On 23 February, the Verkhovna Rada entrusted Chairman Oleksandr Turchinov with presidential duties.

From the perspective of the authorities of the Russian Federation (RF), this meant an almost complete loss of the possibility to influence the political situation in Ukraine and, militarily, a significant weakening of its position in the Black Sea basin. Russia expected the termination (by the new, anti-Russian-oriented Ukrainian government) of the agreement allowing the stationing of the Russian Black Sea Fleet in Crimea[2]. Although it consisted at the time of some 40 ships built back in the 1970s, the fleet remained fully operational[3] and was in the process of intensive modernisation and expansion[4]. Its stationing in Sevastopol gave the Russians access

[1] See: Viktor Yanukovich's interview with Nikolai Zyatkov: *Виктор Янукович: «Народ договорится, и Украина станет единой»*, "Аргументы и Факты" 2014, no. 52, online version: https://aif.ru/euromaidan/viktor_yanukovich_eksklusivnoe_interview [accessed: 6 VI 2023]. Later, the accusation that the opposition had attempted to assassinate Yanukovich was repeated by Vladimir Putin, who stressed that if it had not been for the help of the Russian secret services, Yanukovich would have been killed. See interview with Andrei Kandrashov in 2015: *Крым Путь на Родину Документальный фильм Андрея Кондрашова*, YouTube, 4 X 2020, https://www.youtube.com/watch?v=PGGNXIQXl-cU [accessed: 2 III 2023].

[2] In 2010, Yanukovich signed the so-called Kharkiv Agreement extending the agreement governing the stationing of the Black Sea Fleet in Crimea until 2042 in exchange for a reduction in the price of gas sold to Ukraine by the Russian Federation. A vote on this in the Verkhovna Rada led to a violent confrontation between representatives of the Party of Regions and the opposition. See: *Janukowycz podpisał umowę o stacjonowaniu rosyjskiej floty na Ukrainie* (Eng. Yanukovych signed agreement on stationing Russian fleet in Ukraine), Portal Spraw Zagranicznych, 29 IV 2010, https://psz.pl/162-wschod/janukowycz-podpisal-umowe-o-stacjonowaniu-rosyjskiej-floty-na-ukrainie [accessed: 7 VI 2023].

[3] This was confirmed by the effective blockade of Georgia during the 2008 war.

[4] In addition to modernising old ships, the plans at the time included the addition of six new submarines and six new frigates to the fleet, as well as the French Mistral-type helicopter carrier.

not only to the Black Sea but also to the Mediterranean, the South Atlantic and the Indian Ocean[5], despite the legal restrictions imposed by the Montreux Convention[6]. Crimea provided the Russian Federation with the opportunity to operate in the oceans and to dominate militarily in the Black Sea theatre of war through the option of expanding anti-ship and anti-aircraft missile systems (especially with the increased capabilities of the S-400 launcher)[7].

The abrupt change of power in Ukraine therefore meant very serious geopolitical problems for Russia, which were a significant reduction in the operational depth of its defences (the buffer of neutral states on its borders with North Atlantic Treaty Organisation) and the loss of its dominant position in the Black Sea basin, which greatly weakened the Russian southern flank. Russia, too weak at the time to risk open conflict, responded to this threat with hybrid action, using agent networks long built up in Ukraine[8] and masked kinetic force[9]. It annexed Crimea and embroiled Ukraine in a long-running conflict in the Donbass, effectively blocking the country's aspirations for NATO membership, and seized much of Ukraine's heavy industry and raw material resources, further exacerbating the country's difficult economic situation. The loss of Crimea (along with its almost 2 million inhabitants) and the mass emigration triggered by the eight-year conflict, which turned into a full-scale invasion in February 2022, left between 28 and 34 million people out of the 52 million Ukrainians in 1991 in the current Ukrainian territory[10].

---

5 *Crimea's Strategic Value to Russia*, Center for Strategic and International Studies, 18 III 2014, https://www.csis.org/blogs/post-soviet-post/crimeas-strategic-value-russia [accessed: 6 VI 2023].

6 *Convention concernant le régime des détroits* – agreement signed in 1936 regulating the law of the sea in the Black Sea straits. It concerns the right and rules of passage through the Black Sea straits of ships and vessels not belonging to Turkey, in whose territorial waters the Bosphorus and the Dardanelles are located.

7 *Crimea's Strategic Value to Russia*...

8 For more on the use of agents to achieve strategic objectives in Ukraine, see: M. Świerczek, *2014 takeover of the SBU headquarters in Lugansk as an example of the operation of the Russian special services*), "Internal Security Review" 2023, no. 28, pp. 278–312. https://doi.org/10.4467/20801335PBW.23.012.17662.

9 First it was the so-called green men in Crimea, and then the military groupings fighting in the Donbass against the Ukrainian army and posing as Donbass self-defence forces, despite the fact that, locked in successive encirclements, the Ukrainian troops were decimated with heavy equipment that the separatists were not allowed to have.

10 O. Danylov, *As of January 1, 2023, the population of Ukraine was 28-34 million*, Mezha.Media, 7 IV 2023, https://mezha.media/en/2023/04/07/as-of-january-1-2023-the-population-of-ukraine-was-28-34-million/ [accessed: 7 VI 2023]. Such a large margin of uncertainty is due to the fact that researchers cannot correctly assess whether emigrants will return to their country or stay permanently in their destination countries.

Russia's hybrid actions, even before they moved into the hot war phase, therefore had consequences of strategic importance for the entire Ukrainian state.

The annexation of Crimea and the attempted separation of Ukraine's eastern and southeastern regions as Russian special operations

The actions of the Russian Federation against Ukraine undertaken in 2014 had the character of a sequence of special operations, during which Russia pursued its geopolitical objectives. It achieved them through the annexation of Ukraine's economically and militarily most important territories[11], but - until 2022 - without the need for full-scale war[12]. The use of the army was spotty, always masked and on a small scale. This was made possible by the paralysis of Ukraine's decision-making centres (i.e. the newly formed government and the leadership of the power ministries) after the opposition seized power in February 2014. At the same time, passivity and lack of resistance on the part of Ukrainians, as well as their collaboration with the invaders (covert or overt), occurred at almost all levels of Ukrainian statehood. An examination of the course of successive Russian operations in Ukraine indicates that these processes were strongly influenced by Russian agents[13]. Russian intelligence networks were built both using political clientelistic networks in state institutions (especially in the power ministries) and among the Russian-speaking population, whose defence against alleged persecution was intended to provide cover for Russian actions.

Scale of infiltration

An objective indicator of the scale of Russian infiltration of Ukrainian state institutions is the number of Ukrainian soldiers and officers of the power ministries and officials who - after the annexation of Crimea - continued to serve and work for the occupiers, refusing to leave the peninsula and return to Ukraine. The first attempt to summarise the scale of the collaboration of Ukrainian state structures in Crimea with the Russians was made by the then deputy chairman of the Medjlis of Crimean

[11] As already mentioned, the attempt to take the whole of the east and south-east from Ukraine meant the threat of deindustrialisation and the cutting the country off from the ports through which grain was exported.

[12] It is irrational that, after two years of war, it has not been declared by any of the fighting parties.

[13] Cf.: M. Świerczek, *Szturm na siedzibę Służby Bezpieczeństwa Ukrainy w Ługańsku*...

Tatars[14] Ilmi Umerov[15]. In an interview given to the Ukrainian edition of the newspaper "Новое время" on 3 November 2017, he stated that 100% of Crimean militia and Security Service of Ukraine (SBU) officers, 80% of the military and 70% of prosecution staff had switched to the Russian side and continued their previous work, only that for the occupation forces[16]. According to Umerov, this proved that the Ukrainian state had not carried out any ideological work among the Crimean population for decades, and that the Russians had been preparing for the annexation for a very long time by expanding their agents and subjecting the population of the peninsula to intensive propaganda[17]. He stated that one of the elements of influencing society and state organs in Crimea was to be (in parallel with the long-standing building of pro-Russian sentiment) to portray the Tatars and their organisations as the main extremist factor and hostile to Ukrainian rule in Crimea[18]. This was a way of distracting the power ministries from Russian activity. Umerov pointed out that the clearest manifestation of the betrayal was that none of the 300 units of the Ukrainian army in Crimea resisted the Russian troops, who forcibly seized barracks and equipment[19].

Umerov's statement caused a storm in the Ukrainian media and fuelled long observed phenomena - espionage and the politicisation of widespread allegations of treason[20]. Some commentators accused Umerov of deliberately inflating statistics[21].

---

[14] Medjlis of Crimean Tatars (Къырымтатар Миллий Меджлиси) – an organisation of Crimean Tatars to represent the interests of this community in Crimea.

[15] Ilmi Umerov (born 1957) is a Ukrainian politician and social activist of Tatar nationality. In 2017, convictedin Crimea on charges of undermining the territorial integrity of the Russian Federation, after which he was handed over by the Russian authorities to Turkey in exchange for two detained FSB agents.

[16] *Замглавы Меджлиса Умеров: Сотрудники СБУ и милиции в Крыму оказались предателями на 100%, военнослужащие - на 80%, прокуратура - на 70%*, New Voice, 5 XI 2017, https://nv.ua/ukraine/politics/zamglavy-medzhlisa-umerov-sotrudniki-sbu-i-militsii-v-krymu-okazalis-predateljami-na-100-voennosluzhashchie-na-80-prokuratura-na-70-2135335.html [accessed: 7 V 2023].

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] In order to realise the scale of the phenomenon, it is worth tracing the ДЕРЖЗРАДА on Ukrinform. It contains a very large number of entries concerning real and alleged traitors. See: ДЕРЖЗРАДА, Ukrinform, https://www.ukrinform.ua/tag-derzzrada [accessed: 14 VI 2023]. The posts and articles on treason on the Myrotvorets portal are also a good example. See: https://myrotvorets.news/?s=%D0%B7%D1%80%D0%B0%D0%B4%D0%BD%D0%B8%D0%BA [accessed: 14 VI 2023].

[21] Cf.: *Официальная статистика: замглавы Меджлиса завысил количество предателей в Крыму на 10 %*, Inform Napalm, 7 XI 2017, https://informnapalm.org/41430-ofitsialnaya-statistika-zamglavy-medzhlisa-zavysil-protsent/ [accessed: 7 V 2023]; А. Круглов, *На измене*, Совершенно Секретно, 30 X 2014, https://www.sovsekretno.ru/articles/bezopasnost/na-izmene/ [accessed: 7 V 2023]; *«Предатели на 100%»: Умеров резко высказался о спецслужбах в Крыму*,

A parliamentary investigation was therefore conducted by the deputy of the Verkhovna Rada, Dmytro Tymchuk, who sent official parliamentary enquiries to the relevant ministries[22]. The responses containing officially confirmed data allowed to draw up a summary, including a division into individual service and armed forces[23].

Security Service of Ukraine

In all organisational units in Crimea served 1619 officers as at 1 March 2014. Of these, 1235 belonged to the officer corps. After the annexation, 217 officials, including 210 officers, left for Ukraine. The percentage of traitors was therefore 86.4% and 83% among officers[24].

OBOZ.UA, 5 XI 2017, https://news.obozrevatel.com/society/predateli-na-100-umerov-rezko-vyiskazalsya-o-spetssluzhbah-v-kryimu.htm [accessed: 7 V 2023]; O. Козаченко, *Умеров жалеет, что в Крыму не стали стрелять по русским*, Полит Навигатор, 3 XI 2017, https://m.politnavigator.net/umerov-zhaleet-chto-v-krymu-ne-stali-strelyat-po-russkim.html [accessed: 7 V 2023]; *Замглавы Меджлиса упрекнул Украину в сдаче Крыма без стрельбы*, Черноморская телерадиокомпания, 6 XI 2017, https://blackseatv.com/in-the-spotlight/zamglavy-medzhlisa-upreknul-ukrainu-v-sdache-kryma-bez-strelby/ [accessed: 7 V 2023]; *Теперь пишут записки в Москву: озвучены масштабы предательства крымчан*, From-UA, 30 XI 2017, https://from-ua.org/news/425623-teper-pishut-zapiski-v-moskvu-ozvucheni-masshtabi-predatelstva-krimchan.html [accessed: 7 V 2023]; *Более 10 тысяч солдат перешли на службу России*, Безформата, https://angarsk.bezformata.com/listnews/soldat-pereshli-na-sluzhbu-rossii/62518616/ [accessed: 7 V 2023]; *Сколько военных ВСУ и СБУ перешли на сторону России в 2014 году*, RF-SMI, 20 II 2022, https://rf-smi.ru/ykr/71072-skolko-voennyh-vsu-i-sbu-pereshli-na-storonu-rossii-v-2014-godu.html [accessed: 7 V 2023].

[22] A scan of the response from the Ukrainian Ministry of Defence. See: *Сколько военных из Крыма предали Украину: шокирующие цифры*, Panoptikon, 7 XI 2017, https://panoptikon.org/ukraine/98813-skolko-voennykh-iz-kryma-predali-ukrainu-shokirujushhie-cifry.html [accessed: 4 VI 2023].

[23] Data quoted from: Д. Тымчук, *Сколько крымских силовиков стали предателями Украины*, UA Info, 6 XI 2017, https://uainfo.org/blognews/1509980385-skolko-ukrainskiy-silovikov-v-krymu-stali-predatelyami.html [accessed: 4 VI 2023]; *Тымчук назвал число предателей среди украинских силовиков в Крыму после аннексии*, РБК-Україна, 6 XI 2017, https://www.rbc.ua/rus/news/tymchuk-nazval-chislo-predateley-sredi-ukrainskih-1509976026.html [accessed: 4 VI 2023]; *Нарден Тымчук назвал число изменивших присяге крымских силовиков*, Black Sea News, 6 XI 2017, https://www.blackseanews.net/read/136189 [accessed: 5 VI 2023].

[24] The calculations summarising the results of the deputy enquiries come from the official page of D. Tymchuk's Facebook page. See: https://www.facebook.com/dmitry.tymchuk/posts/1366726656789319 [accessed: 9 VI 2023].

Armed Forces of Ukraine

As of 1 March 2014, there were 13,468 soldiers of the Armed Forces of Ukraine (AFU) stationing in Crimea, including 4,737 officers. After the Russian takeover of Crimea, 3991 servicemen, including 1,649 officers, left the peninsula. The percentage of traitors in the AFU was thus 70.4%, and 65% among officers[25].

Ministry of the Interior

There is no data on the number of Ukrainian militiamen in Crimea. Only information on internal troops under the responsibility of the Ukrainian Ministry of Interior and Border Guard is available.

As of 1 March 2014, there were 2489 internal army soldiers in Crimea. 1398 returned to Ukraine. Thus, there were 44% traitors in the ranks of the internal troops. This low percentage was due to the fact that in the units stationed in Crimea there were 1265 basic military service soldiers from Ukraine proper who had returned home in full force. Among the officer cadre of the internal troops, usually from Crimea and living there, by contrast, the percentage of traitors was 86%[26].

As of 1 March 2014, there were 1869 Border Guard officers in Crimea, including 448 officers. 479, including 226 officers, returned to the country. The percentage of traitors was therefore 74% and 50% among officers[27].

The figures included in the above statistics may in fact be higher, as some officers may have returned to Ukraine to leave the service and retire, and then returned home to Crimea to take up service with the Russians, while retaining Ukrainian pension benefits.

Attempts to explain the scale of the betrayal

In the Ukrainian media discussing such a large scale betrayal, attempts were made to rationally explain why the mass betrayal of Ukrainian soldiers and officers occurred. The hypotheses put forward included several factors that could have been relevant.

- Firstly, those who stayed in Crimea had families, homes and property there. Leaving the occupied peninsula meant losing everything. The weakened

[25] Ibid.

[26] Ibid.

[27] Ibid.

Ukrainian state did not provide material security for people who remained faithful to their oath when they left Crimea[28].

- Secondly, according to the 2001 census, of the 2.4 million inhabitants of Crimea, 60.40% were ethnic Russians, 24.01% were of Ukrainian nationality and 10.11% were Tatars[29]. There is a lack of information on actual linguistic and cultural affiliation, i.e. data on how many of the Crimean Ukrainians and Tatars were Russian-speaking. It can be assumed that the ethnic structure of the Ukrainian services and military may have corresponded to these percentages, at least in terms of professional cadres, probably recruited mainly from peninsula residents looking for work close to home. Crimean Russians - loyal to their country of origin - may have rejected Ukrainian statehood, which was alien to them. A higher percentage of traitors than the statistics for the main nationalities would indicate may have been the result of, for example, a reluctance to accept Tatars (considered a subversive element) into service[30], so the choice to stay in service may have been derived from nationality. The ethnic factor may have played a major role due to Russian propaganda scaring the Russian and Russian-speaking population of Ukraine with the threat of ethnic cleansing by Right Sector activists[31].
- Thirdly, Russia in Crimea was not a foreign state. The Russian Black Sea Fleet worked closely with the AFU. Officers of these formations were friends, met, and were linked by comradeship and family ties. Thus, they were able to prioritise informal (i.e. family-friendship) relationships when making decisions. Eastern European societies - in contrast to the West -

[28] Ibid.

[29] *Про кількість та склад населення України за підсумками Всеукраїнського перепису населення 2001 року*, https://web.archive.org/web/20071124125111/http://www.ukrcensus.gov.ua/results/general/nationality/ [accessed: 12 VI 2023].

[30] This would change the nationality structure in Crimea's power ministries, as the proportion of Russians and Russified Ukrainians would be higher than in the population as a whole.

[31] Cf.: *Корсуньская трагедия - боевики Майдана пытают крымчан, поджёг автобусов. 20.02.2014*, YouTube, 20 II 2017, https://www.youtube.com/watch?v=s2TGeF-xbTc&list=PLeuqEf-NtM8zleTyjJ-n8DXE2Uz9OHm2Ty [accessed: 23 II 2023]; *Документальный фильм «Корсуньский погром»*, YouTube, 30 VII 2014, https://www.youtube.com/watch?v=7FfPTBQ4l38 [accessed: 22 II 2023]; *«Корсуньский погром»: зверства сторонников майдана*, YouTube, 21 VI 2014, https://www.youtube.com/watch?v=hlf_AdGbfjE [accessed: 22 II 2023]; *Корсуньская трагедия Убивали только за то, что они из Крыма 2014 весна*, YouTube, 27 V 2019, https://www.youtube.com/watch?v=bqUcM5YBWFw [accessed: 23 II 2023].

have a so-called communal character, i.e. they value loyalty to family members and friends more highly than to the state[32].

- Fourthly, the Crimean population was under the constant influence of the Russian mass media and generally supported the pro-Russian Party of Regions. Both Russia and Party of Regions activists intensively promoted the narrative that the opposition's seizure of power in Kiev was a forceful coup financed by the West. With this perception of these political events, the choice of Russia (to which the ousted Yanukovich had fled) could have been seen as the only option to fight the 'putschists' in a situation where the 'legitimate' president had obtained refuge in the Russian Federation.

Although the hypotheses presented are important in trying to explain the events described, they do not in any way explain the admission of 86.4% of Crimean SBU officers to the FSB. The militia, border guards, prosecutor's office or civil administration are non-political organs of the state (at least in theory), even purely technical and necessary for the administration of an area inhabited by a population[33]. This may result in their officers seeing the service as a profession and the state merely as an employer. This may encourage collaboration with the occupying power, especially if it forms the occupying administration on the basis of its own legal system[34]. The occupying forces may in turn use already existing institutions (with their personnel) with knowledge and experience in the area, treating them pragmatically as a necessary part of the administration, regardless of nationality.

Special services (all over the world) use very restrictive recruitment methods. They seek to identify as much as possible about the candidate's past and way of life (in order to eliminate the possibility of blackmail), as well as his or her possible links with groups potentially dangerous to the service. The most important thing is to establish whether the candidate is in contact with a foreign special service and whether there are indications of a real risk that such relations could be established in the future. In other words, the sine qua non conditions for admission to work in the special services are the candidate's lack of so-called counterintelligence risk and his or her loyalty to his or her own state. Consequently, even in peacetime and towards one's own

[32] On the differences between community and associative societies, see: F. Tönnies, *Wspólnota i stowarzyszenie* (Eng. Community and association), Warszawa 1988.

[33] An example drawn from history is the establishment of police units by the Germans in the General Government (Polnische Polizei im Generalgouvernement), which were armed and financed by Polish local governments. See in more detail: A. Hempel, *Policja granatowa w okupacyjnym systemie administracyjnym Generalnego Gubernatorstwa: 1939–1945* (Eng. Blue Police in the occupation administrative system of the General Government: 1939-1945), Warszawa 1987.

[34] This was the argument used by the so-called 'blue policemen' to defend themselves after the war. They pointed to their "service" role towards Polish society, which they protected from criminals.

citizens, extensive vetting procedures are applied. Under quasi-war conditions and with regard to citizens of a foreign state, the rigour of counter-intelligence checks should be much greater. Especially if the candidates have already once betrayed their service and their own state and broken the oath of allegiance taken by officers of the power ministries.

How, then, did the Russians accept 1,400 Crimean SBU officers into FSB service without vetting? This meant, after all, that they would have access to the FSB's IT systems, official and state secrets and the possibility of promotion in the hierarchy (not only in the Crimean units, but also in the headquarters). Such conduct is contrary to the elementary principles of the work of the special services. Looking for an explanation, one could assume that such a decision was taken by the Russians due to their inability to create security structures because of the lack of their own cadres. However, the FSB is estimated to have between 200,000[35] and 350,000[36] officers, of which around 100,000-120,000 serve in the Border Guard[37]. Thus, the internal service alone accounts for between 80,000 and 230,000 officers. With such a staff resource, the secondment of around 2,000 personnel to Crimea should not pose a problem[38].

Research hypothesis

The most plausible explanation for this phenomenon is the assumption that the Russians, when accepting former SBU officers, did not need to check their loyalty, as the Crimean SBU cadres had been in contact with the Russian special services for a long time. If this cooperation had been long and repeatedly positively verified, there was no need for additional confirmation of the new officers' loyalty. Russian agents in the SBU were simply taken over en masse by the FSB.

Such reasoning has the methodological weakness that no intelligence service in the world would recruit almost the entire personnel pool of an adversary to cooperate. This would be counter-productive, as new sources would provide the same information and receive remuneration for it, while generating the need to expand its own intelligence structures due to the handling of numerous agents. The aim, therefore, is to recruit only those ranked high enough in the adversary's structure

[35] *Численность ФСБ*, https://fsb.dossier.center/number/ [accessed: 12 VI 2023].

[36] B. Renz, *The Russian Force Structures*, "Russian Analytical Digest" 2007, no. 17, p. 6.

[37] *Численность ФСБ…*

[38] The one thousand four hundred officers of the Crimean SBU who took up service in Russian structures accounted for between 0.4 and 0.7% of the number of total posts in the FSB.

to be able to obtain information gathered from those at lower levels of the service hierarchy.

In attempting to explain the atypical modus operandi of the Russian services with regard to the Crimean SBU, reference can be made to the results of analyses that point to an important difference between the paradigm of operation of the Western and Russian secret services consisting in the different objectives and methods of the latter. These methods are referred to as offensiveness (Russian: наступательность)[39].

Offensive counterintelligence

It should be emphasised that the Soviet-Russian concept of counterintelligence differs radically from that of the West. According to the assumptions of the first concept, counterintelligence is not about passively protecting sensitive information from the actions of the enemy's intelligence services, but about actively controlling the enemy's intelligence and counterintelligence by placing its own agents ('moles') in these structures and planting double agents. However, the Russian concept of active counterintelligence does not stop there. Among the methods of operational counterintelligence work described by Russian authors dealing with the activities of the Soviet secret services[40] the term разложение противника always appears. Despite the frequent use of this term in the works of Russian historians, its definition is lacking, while at the same time such a modus operandi is treated as an obvious attribute of the Chekist operational workshop. Translating the term into Polish, one should speak of disorganisation, decomposition or systemic destabilisation of a hostile organisation. Sometimes this term is used in its developed form – разложение на корню, which should be understood as a complete, systemic paralysis

[39] "Наступательность – образ действий контрразведки обеспечивающий активность иинициативу, достижение максимальных успехов в борьбе с противником. Н. – представляет собой организационно-технический принцип, которым стремятся руководствоваться разведывательные и контр разведывательные органы в своей деятельности. В соответствии с ним сторона действующая наступательно, достигает при прочих равных условиях найлучших результатов" (Offensiveness is the counterintelligence modus operandi of seizing activity and initiative to achieve maximum success against the enemy. Offensiveness - represents the organisational and technical principle that intelligence and counterintelligence agencies try to follow in their operations. According to it, the best results are achieved by the side that plays offensively). See: *Контрразведывательный словарь*, Москва 1972, p. 171. Translations in the article are from the author (editor's note).

[40] In the context of agent infiltration, control over channels of communication.

of the enemy's military-intelligence organisation, making any effective offensive--defensive action impossible[41].

This approach to the work of the Soviet-Russian secret services stems from the theoretical assumptions formulated in the early 1920s by Aleksandr Kuk, deputy head of the agent department of the USSR's military intelligence service Razvyudpr. The main one stated that: *Secret intelligence has acquired an active character. This feature of clandestine intelligence, as bearing on terrorism, disorganisation of state life and the military system of the opposing side, turns out to be extremely important and shows intelligence in a completely different light from before the world war*[42]. According to this premise, intelligence ceased to consist merely of collecting military or political information about the opponent, but became a multi-faceted activity aimed at disorganising the opponent's state apparatus as fully as possible. In other words, the described *разложение противника* was a practical application of Kuk's theoretical considerations, which postulated active paralysis of the opponent's state structures instead of passive collection of information about it.

On the subject of Russian methods of disorganising the enemy - despite the lack of detailed descriptions in Russian literature - one can deduce from the 'interpretation' contained in a circular sent out on 11 August 1937 by the head of the People's Commissariat of Internal Affairs of the USSR (Народный комиссариат внутренних дел СССР, NKVD) Nikolai Yezhov[43]. The letter was a de facto death sentence for Polish communists working in the party-state apparatus of the USSR[44], accused of belonging to an intelligence network called the Polish Military Organisation (PMO). Characterising the (alleged) activities of the PMO to harm the interests of the USSR, Yezhov listed the following manifestations of activity:

- infiltration of the Soviet administration, political apparatus, economy, army (mainly middle and senior cadres), NKVD, party apparatus and Comintern;

---

[41] It is worth adding that 'dismantling' the enemy's organisation - as a connotation-neutral term - was a name reserved for offensive actions of the Soviet secret services. The same action of foreign services directed against the USSR was referred to by the pejoratively characterised word вредительство (pestering).

[42] A.I. Kuk, *Kanwa wywiadu agenturalnego* (Eng. The canvass of agent intelligence), Warszawa 1994, p. 16.

[43] Nikolai Ivanovich Yezhov (born 1895, executed 1940) - Soviet party and state activist, People's Commissar of State Security from 1936 to 1938, responsible for the implementation of Stalinist terror during the so-called Great Purge (named after him "Yezhovshchyna").

[44] *Оперативный приказ Народного комиссара внутренних дел Союза ССР Николая Ежова № 00485. 11 августа 1937 г. о польской национальной операции*, https://operacja-polska.pl/nkr/o--operacji-polskiej-nkw/dokumenty/966,00485-11-1937.html [accessed: 22 X 2019].

- locating agents in key positions in intelligence and counterintelligence (civilian and military) to paralyse the activities of bodies able to detect mass infiltration;
- organisation by Polish intelligence of systematic recruitment work using high positions in the USSR state apparatus, with the aim of weakening the USSR's defence capabilities in every possible field.

It is clear from the contents of Yezhov's letter that the tactic of dismantling the Soviet apparatus was to consist of three successive stages:

1) point infiltration of key places in the apparatus of the Soviet republic (these were mainly leadership positions in the secret services, the Workers' and Peasants' Red Army, administration, party and economy[45]);
2) support for further, almost massive infiltration at lower organisational levels by 'moles' positioned in sensitive locations[46];
3) creation of an extensive agent network entangling the economy and the political-military superstructure of the state, the members of which - by means of actions difficult to prove due to the use of camouflage - tried to harm the Soviet state by all means[47]. These activities consisted of corrupting and

[45] Cf.: "(…) уже определилось, что антисоветской работой организации были охвачены – система НКВД, РККА, Разведупр РККА, аппарат Коминтерна – прежде всего польская секция ИККИ, наркоминдел, оборонная промышленность, транспорт – преимущественно стратегические дороги западного театра войны, сельское хозяйство" (Eng. …it has already been established that the anti-Soviet work of this organisation included - the NKVD system, the Red Army, the Intelligence Department of the Red Army, the Comintern apparatus - above all the Polish section of the Comintern Executive Committee, the People's Commissariat of Foreign Affairs, the defence industry, transport - mainly strategic roads of the western theatre of warfare, agriculture). Quoted from: *Закрытое письмо*…

[46] Cf.: "Массовая фашистско-националистическая работа среди польского населения СССР в целях подготовки базы и местных кадров для диверсионно-шпионских и повстанческих действий" (Eng. Mass fascist-nationalist work among the Polish population in the USSR to prepare a base and local personnel for sabotage, espionage and insurgent activities). Quoted from: *Закрытое письмо*…

[47] Cf.: "Глубокое внедрение участников организации в компартию Польши, полный захват в свои руки руководящих органов партии и польской секции ИККИ, провокаторская работа по разложению и деморализации партии, срыв единого и народного фронта в Польше, использование партийных каналов для внедрения шпионов и диверсантов в СССР, работа, направленная к превращению компартии в придаток пилсудчины с целью использования ее влияния для антисоветских действий во время военного нападения Польши на СССР" (Eng. Deep penetration of members of the organisation into the Polish Communist Party, complete takeover of the party's leadership organs and the Polish section of the Comintern Executive Committee, provocative work for the decomposition and demoralisation of the party, breakdown of the united and popular front in Poland, use of party channels to introduce spies and saboteurs into the USSR, work to transform the Polish Communist Party into an appendage of Piłsudism in order

demoralising Soviet officials, promoting harmful solutions in industry and agriculture, leading to the dissipation and waste of budget resources, lobbying for ineffective or countereffective methods of operation of the secret services, administration and army (at both tactical and strategic levels[48]).

In historiography, Yezhov's circular was treated either as a manifestation of the widespread psychosis prevailing in the Soviet power apparatus, or as evidence of the cynicism of its author, who wanted to secure his career by means of mass executions of his more capable colleagues and thanks to recognition from Stalin, who was supposedly suffering from advanced paranoia. Sometimes a thesis was put forward about the alleged anti-Polonism of the Soviet authorities, which was said to be a legacy of tsarist times.

In the process of explanation, it is necessary to reach - without entering into considerations of Stalin's unproven (due to lack of diagnosis during his lifetime) madness and assuming that the sheer number of Poles occupying leadership positions in the USSR[49] falsifies the theories of Soviet anti-Polonism - to the carefully documented

to use its influence for anti-Soviet activities during the Polish military attack on the USSR). Quoted from: *Закрытое письмо…*

[48] Cf.: "Полный захват и парализация всей нашей разведывательной работы против Польши и систематическое использование проникновения членов организации в ВЧК–ОГПУ–НКВД и Разведупр РККА для активной антисоветской работы. Основной причиной безнаказанной антисоветской деятельности организации в течение почти 20 лет является то обстоятельство, что почти с самого момента возникновения на важнейших участках противопольской работы сидели проникшие в ВЧК крупные польские шпионы (…)" (Eng. The complete seizure and paralysis of all our intelligence work against Poland and the systematic infiltration of the Cheka-OGPU-NKVD and the Intelligence Board of the RKKA with the help of members of the organisation for active anti-Soviet work. The main reason for the unpunished anti-Soviet activity of this organisation for almost 20 years is the fact that, almost from the very beginning of its existence, significant Polish spies who had infiltrated the Cheka were active in the most important areas of anti-Polish work). Quoted from: *Закрытое письмо…*

[49] A minimum of 17% of the leadership apparatus (middle and senior levels) of the NKVD consisted of ethnic Poles. In reality, the Polish element in the NKVD was much more numerous, as there were a large number of people working in the Soviet state apparatus who came from Polishised Jewish, Belarusian-Lithuanian or Ukrainian families. In their personal questionnaires, however, to emphasise proletarian roots, they would enter their ethnic origin, remaining silent about their links with the Polish language and culture. The Soviets were aware of this. In the NKVD reports on the Polish 'operation', they scrupulously reported that 20,311 Poles and - as part of this operation - more than 17,000 representatives of other nations (mainly Belarusians and Jews) had been arrested. If these proportions were to be translated into the percentage of Poles in the NKVD leadership given above, it could mean that almost a third of the leadership apparatus of this institution had ties to the Polish language and culture. Quoted from: А. Зданович, *Польский крест советской контрразведки. Польская линия в работе ЧК-НКВД. 1918-1938*, Москва 2017, pp. 169–170, 311–312.

findings of cognitive psychology, within which the phenomenon of projection has been described as a possible explanation for the action against the PMO.

The mechanism of projection as a hypothesis explaining the actions of the NKVD

In psychology, projection is understood as a defence mechanism of personality consisting in attributing one's own motivations, views, traits and behaviours to others. The common occurrence of the phenomenon of projection results from the fact that the projecting individual usually has access only to his or her own thoughts, feelings and behaviours[50], with the help of which he or she explains other people's behaviours[51] (since in the process of understanding others, one cannot refer to emotions, beliefs and knowledge that one does not have[52]).

If one accepts that the Soviet services infiltrated foreign services en masse and paralysed their activities with the help of agents, then – in line with the availability heuristic[53] – NKVD officers were convinced that enemy intelligence was doing the same to them. The NKVD leadership, by dismantling the Western apparatuses of power with the help of 'moles', agents of influence and double agents, believed that it was the victim of symmetrical actions on the part of its opponents, carried out by similar methods and on a similar scale.

Yezhov's infiltration model as an explanation for mass betrayals in the Crimean SBU

If, on the basis of the above considerations, it is assumed that the Soviet services and then their continuators in the Russian Federation used the methods revealed by

[50] An attempt to avoid projection as a factor falsifying cognition in the social sciences is the rigorous application of methodology and the researcher's multiple cognitive perspectives. However, accessibility heuristics remain a major source of cognitive error. Cf.: D. Kahneman, P. Slovic, A. Tversky, *Judgment under uncertainty: heuristics and biases*, New York 1982.

[51] Cf.: T. Kobierzycki, *Filozofia osobowości* (Eng. Philosophy of personality), Warszawa 2001, p. 153. See in more detail: A. Freud, *Das Ich und die Abwehrmechanismen,* Wien 1936; O.F. Kernberg, *Borderline Conditions and Pathological Narcissism*, London 1990; K. König, *Abwehrmechanismen*, Göttingen–Zürich 2007; S. Mentzos, *Interpersonale und institutionalisierte Abwehr*, Frankfurt am Main 1994.

[52] This phenomenon is also known to so-called naïve psychology, e.g. as the belief that thieves believe that everyone steals.

[53] Habitual recourse to one's own experiences, emotions and beliefs.

Yezhov, the massive scale of betrayal in the Ukrainian state apparatus and the FSB's seamless absorption of the cadres of the Crimean secret services become understandable. Since the aim of the Russian services - according to the methodology described earlier - is not to obtain information, but to take control of the institutions of a hostile state in order to paralyse their activities through a network of agents penetrating almost all organisational levels, the mass scale of recruitment becomes logical.

The main infiltration mechanism, as described by Yezhov, was cronyism. Using corrupt mechanisms, agents could be introduced to lower levels with the help of 'moles' who had previously been placed high in the hierarchy. Established agents had to surround themselves with further agents or people who were fully controlled and lacked initiative in order to protect themselves from unmasking by subordinates and colleagues. Thus, agentisation and complicity (if only in passive form) descended to lower and lower levels of the organisation under attack.

The well-known phenomenon of mass administrative cliques in the post-Soviet area, accompanied by the passivity of those who do not belong to them but are fully loyal to them out of fear or self-interest, explains the effectiveness of the method outlined by Yezhov. It also explains the admission of almost 1500 former SBU officers to the FSB without vetting them. If one assumes that there were agent networks in the Crimean SBU reaching from the top to the bottom of the hierarchy, and that each level protected its own security by introducing new agents and by intimidating and making dependent employees formally uncooperative with the Russians, then the Russian takeover of an entire team, fully agent-controlled, did not involve a high degree of counterintelligence risk.

From this, it follows that the agentic model of capturing an adversary's institutions involves two key elements:

1) creation, through cronyism mechanisms, of branched agent networks composed mainly of management staff at all levels,
2) clientelistic dependence of rank-and-file employees on infiltrated cadres in order to gain full control over their actions and bind them to the established system.

The mechanism of dependency of subordinates by corrupt supervisory personnel is also common in the post-Soviet reality[54]. It consists of:

- negative selection of managed staff, removing from the team all independently thinking and autonomous employees who are not willing to accept implicit hierarchies and clientelistic dependencies;

[54] For more on the mechanisms of staff dependence on informal relationships in the secret services, see: Г.С. Водолеев, С.Ф. Сидоренко, *Спецнужды и спецслужбы*, Москва 2009.

- undermining subordinates' confidence in official regulations by developing unofficial, extra-legal networks of relationships and dependencies that fully regulate relations within the institution and replace the legal basis of its functioning;
- total paralysis of objective personnel policy, with the result that promotion depends solely on superiors and not on individual skills or work performance;
- corruption, which - through the complicity of subordinates - binds them to an unofficial structure both because they want to share in the profits and because they fear the legal consequences if they are exposed[55].

The last factor is the most important, as corruption (broadly understood as the use of a public function to pursue one's own interests) is a sine qua non for all other elements. Observations on the mechanisms operating in Ukrainian state structures during the recent conflict with the Russian Federation confirm the existence of a correlation between betrayal (i.e. entering into cooperation with Russian services) and prior corruption[56].

Corruption in the Crimean SBU

According to a study by Transparency International Ukraine (Трансперенсі Інтернешнл Україна, TIU), in 2022 Ukraine ranked 116th on the corruption scale out of 180 countries in the world[57]. In Europe, it was the most corrupt country. At the same time, it is worth noting that the results of the TIU study do not fully reflect

[55] Failing to report corruption is already a criminal offence, so passivity arising from powerlessness in the face of the system becomes an effective binding element to the informal, agent-created system.

[56] Cf.: *Генерал-коллекционер СБУ Свиридонов друг Куницына*, ОРД, 20 XII 2009, https://ord-ua.com/2009/12/29/general-kollektsioner-sbu-sviridonov-drug-kunitsyina/ [accessed: 15 VI 2022]; W. Samar, *Russian «moles» in the State Security Service of Ukraine: what is missing in the Kulinich-Sivkovych' case?*, Center of Journalistic Investigations, 26 IV 2023, https://investigator.org.ua/investigations/253973/ [accessed: 16 VI 2023]; *Генерал Кривонос: про зраду в 2014-му, Порошенка, Зеленського, «клоунів» у РНБО і силове звільнення Донбасу*, Радіо Свобода, 19 I 2020, https://www.radiosvoboda.org/a/rnbo-kryvonos-donbass-zrada-peremoga/30384758.html [accessed: 15 VI 2023]; *Корупція та зрада - це неприпустимі речі. І у професійному, і в людському плані. Це не можна пробачати», - Ігор Клименко*, 7 II 2023, https://mvs.gov.ua/uk/news/korupciia-ta-zrada-ce-nepripustimi-reci-i-u-profesiinomu-i-v-liudskomu-plani-ce-ne-mozna-probacati-igor-klimenko [accessed: 15 VI 2023]. See in more detail: A. Савченко, *Антиукраїнець: або Воля до боротьби, поразки чи зради*, Київ 2020.

[57] Transparency International Ukraine, https://www.transparency.org/en/countries/ukraine [accessed: 16 VI 2023].

the scale of the phenomenon, as many types of corruption (e.g. cronyism, favouritism or nepotism) are not perceived as such in Ukraine. They are treated as socially obvious phenomena[58]. One can therefore risk the hypothesis that the above surveys only show the scale of bribery and not corruption as a complex phenomenon.

Since its creation, on the basis of the republican Committee for State Security (Комитет государственной безопасности, KGB), the Security Service of Ukraine has been an institution with a predisposition to dysfunction[59]. On the one hand, it was subjected to politicisation (understood as the active support of political clans), and on the other, to the constant pressure of oligarchic capitalism, which drew the best officers to work in the private sector and with their help corrupted the entire structure. Crimea was remote from the Kiev headquarters and had a special status, while offering ample opportunities to join in the widespread looting of state assets[60], which encouraged corruption to flourish.

Only the period from 2000 onwards, when the anomie of the 1990s caused by the collapse of the USSR was slowly beginning to end, will be included in the analysis. During this period (i.e. from 2000 to 2014), the Crimean SBU was headed successively by Gen. Alexander Sviridonov, Gen. Vladimir Pshenichnyy, Gen. Alexander Yakimenko, Gen. Vladimir Totskiy and Gen. Gennady Kolachev. During the 14 years of their rule, there were many scandals related to the sale of SBU property for bribes[61], the expansion of corrupt relations with local business, organised crime, administration, as well as the so-called kryshevaniye[62] of profitable companies, the plundering of archaeological sites[63] and the running of security companies in collaboration

[58] The Ukrainians surveyed referred to corruption being treated as a bribe. The actual level of corruption is therefore significantly higher.

[59] The Security Service of Ukraine, due to the mass exodus of capable officers, consisted almost exclusively of people unable to find their way in the market reality and a handful of officers who were only a few years short of retirement. Low salaries and conditions resulting from the wild capitalism of the 1990s led to high levels of corruption. Cf.: *Генерал-коллекционер СБУ Свиридонов*…

[60] At the time of its separation from the USSR, Ukraine had the informal status of the world's tenth economy, with both fertile black soil and heavy industry. Three decades later it was the poorest country in Europe. See: *Map of sovereign states in Europe by projected 2023 GDP (PPP) per capita based on international dollars*, https://en.wikipedia.org/wiki/List_of_sovereign_states_in_Europe_by_GDP_(PPP)_per_capita [accessed: 12 III 2024].

[61] Including not only the polyclinic and nursery buildings, but also the contact flats used for operational work. From: *Генерал-коллекционер СБУ Свиридонов*…

[62] Kryshevaniye (Russian: крышевание) – protection in a broad sense, offered to companies in exchange for a bribe or share of the profits.

[63] In Crimea, so-called black archaeology has become a profitable business. The SBU leadership initially contented itself with stealing some of the seized artefacts and then moved on to illegal excavations with the help of soldiers from the ALFA unit. From: *Генерал-коллекционер СБУ Свиридонов*…

with bandits and the International Bodyguard Association, whose interests in the post-Soviet area were represented by former KGB colonel Josif Linder. The staffing of the Crimean SBU was subjected to constant negative selection, as not only the unruly but also competent officers who would be able to understand the nature of the illegal corruption schemes being set up were forced to leave[64]. Only officers who were passive and to some extent entangled in the illegal interests of the management were tried to be kept in the service.

There were reports in the press not only of widespread corruption and links (taken for granted[65]) of the Crimean SBU with the Russian services[66], but also of the strong influence of the Turkish secret services on the Crimean SBU to corrupt it through the leadership of the Tatarstan Medjlis[67]. There is a lack of information to resolve whether this was the result of multilateral sell-outs by Ukrainian officers to maximise profits, or whether the Russian special services used agents in the SBU to play operational games with Turkish intelligence.

Even a superficial review of media reports from the period in question indicates the complete anomie of the Crimean SBU[68], resulting from the intertwining of corrupt influences, infiltration by foreign special services, contact with organised crime and local political-economic networks. Thus, there was every indication that the cadres of the Crimean SBU, demoralised by corruption, subject to adverse selection and arbitrary superiors, should be fully controlled by the agent network created by the FSB.

---

64 Ibid.

65 All those heading the Crimean SBU had either been in the KGB or the Soviet army in the past. Consequently, contacts with colleagues from their former service (especially when they served in the Black Sea Fleet) were not questioned by anyone.

66 W. Samar, *Russian «moles»...*

67 Cf.: *Закрытый доклад СБУ: на турецкие деньги «меджлис» вел разведку для Анкары*, EADaily, 7 IV 2016, https://eadaily.com/ru/news/2016/04/07/zakrytyy-doklad-sbu-na-tureckie-dengi-medzhlis-vel-razvedku-dlya-ankary [accessed: 16 VI 2023].

68 Cf.: *Коррупция - СТОП! Прокуратура признала действия СБУ не соответствующими законодательству*, LB.ua, 23 V 2011, https://lb.ua/news/2011/05/23/97705_korruptsiya_stop_prokuratura_priz.html [accessed: 16 VI 2023]; М. Галеотти, *«Сейлем» и «Башмаки». Крым и криминал до и после российской аннексии*, Крым.Реалии, 27 X 2014, https://ru.krymr.com/a/26658454.html [accessed: 16 VI 2023]; *Агрессивный крымский боевик Самвел оказался спецагентом Кремля и мог работать в СБУ*, ТСН, 20 V 2014, https://tsn.ua/ru/politika/agressivnyy-krymskiy-boevik-samvel-okazalsya-specagentom-kremlya-i-mog-rabotat-v-sbu-366551.html [accessed: 16 VI 2023]; *Новые русские бандиты: кто контролирует Крым*, Україна Кримінальна, 24 III 2014, https://cripo.com.ua/investigations/?p=172293/ [accessed: 16 VI 2023]; *Милиция и СБУ закупили машин на 30 миллионов*, bigmir)net, 15 XII 2010, https://auto.bigmir.net/autonews/autoworld/5217854-miliciya-i-sbu-zakupili-masin-na-30-millionov [accessed: 16 VI 2023]; *Агенты национальной опасности*, dsnews.ua, 28 X 2013, https://www.dsnews.ua/economics/agenty-natsionalnoy-opasnosti-28102013090200 [accessed: 16 VI 2023].

Summary

The starting point of the considerations undertaken was the question of the possible reasons for the incredibly high percentage of Ukrainian state functionaries who switched to the side of the Russians in 2014. The main research problem was - contrary to the rules regulating the functioning of special services - the admission of 1,400 officers of the Crimean SBU to the Russian FSB. After all, no service would accept into its ranks hundreds of service officers of an enemy state (in addition, in a state of undeclared war with it), especially since they had broken the oath of allegiance they had taken at their previous location. All available procedures for checking the loyalty of so-called walk-ins (i.e. people spontaneously offering their services to the special services) should be applied to SBU officers declaring their willingness to work for the FSB[69]. The author considered that the only logically acceptable explanation for this phenomenon was that the Russians de facto did not accept neophytes of the Russkii mir into their service, but instead enlisted agents who had previously - by acting for Russia - fully proven their loyalty. Since the hypothetical mass enlistment was at odds with the economics of intelligence operations, the author drew, in the process of explanation, on the Soviet theorist's concept of active intelligence from the 1920s and - using the achievements of cognitive psychology - reconstructed the Soviet method of mass infiltration of an opponent's institution in order to paralyse its offensive and defensive actions early on and any attempt to improve and reform the agent-infested organisation.

From the analyses carried out, the explanation for the phenomenon indicated is most likely the massive infiltration of Ukrainian services in Crimea by the FSB. The author assumed that - in line with the described methodology of Soviet infiltration - the main mechanisms underlying such an attack were the widespread cronyism, nepotism and immanent corruption prevailing in the infested service. Indeed, by exploiting these pathologies, it is relatively easy to build vertical agent networks and at the same time (as a result of complicity in corruption and the removal of independently thinking individuals) to make the non-recruited part of the cadre dependent. All these factors occurred in great intensity in the Crimean SBU, which made it easy for the Russians to take control of this institution long before the annexation of the peninsula.

It can be presumed that the FSB's group takeover of Crimean SBU officers was carried out for propaganda purposes, since - from the point of view of operational logic - it would have been more advantageous for Russia to transfer agents

[69] See in more detail: I.A. Serov, *Work with Walk-ins*, "Studies in Intelligence" 1962, vol. 8, no. 1; F. Begoum, *You and Your Walk-In*, "Studies in Intelligence" 1962, vol. 6, no. 1.

from the Crimean SBU to the Kiev headquarters or regional SBU units, especially from areas adjacent to the kinetic action zone in the Donbass. Probably the fear of criminal trials against Ukrainian state functionaries working in Crimea, who could be accused, if not of treason, then of failing to fulfil their duties, also played a role. It was therefore preferable to leave the agents on the peninsula to use them for propaganda operations, while at the same time transferring to Ukraine the right agents positioned among the soldiers, officers and officials who were returning to their homeland in the halo of Ukrainian patriots[70].

If the hypothesis posed in the article is true, it must be assumed that the Crimean operation was a de facto special services operation, with only a subsidiary role for the armed forces. The kinetic action in the form of the intervention of the Russian army (first masked, then overt) could only have been the final chord of a multi-year process of mass infiltration and disintegration of the opponent's civil--military institutions. Taking into account the statistics quoted at the beginning of the article demonstrating the scale of the betrayal, one can risk the hypothesis that the army was used only to mask the real, hidden mechanism of the annexation. For Russia - relying on massively infiltrated Ukrainian state structures - could have staged the 'spontaneous' secession of Crimea in a situation of a forcible seizure of power by the opposition in Kiev. It would have been sufficient to carry out a *staging*[71] using mass protests, the local administration joining them and the Crimean parliament declaring secession. Thanks to Tymchuk's findings, it is known that all power institutions in Crimea were fully controlled by Russian agents. There was therefore no real force that could have stopped the 'people's referendum' if it had been carried out by a fully agent-controlled local parliament. The use of armed formations of the Russian Federation was even an obstacle to the legitimacy of the annexation, giving the West a pretext to declare the referendum invalid.

The most significant conclusion to be drawn from the above analysis is the finding that the Russians succeeded in seizing Crimea not through military intervention, but through systemic infiltration and agentic dismantling of the opponent's institutions. This tactic of aggression as an extension of policy is a development of the assumptions of Soviet theorists from the period of major disinformation operations and ancient Chinese military thought, indicating the possibility of achieving

[70] An identical method of operation was used by the Soviet GPU during major disinformation operations carried out in the 1920s and 1930s. See in more detail: M. Świerczek, *Jak Sowieci przetrwali dzięki oszustwu. Sowiecka decepcja strategiczna* (Eng. How the Soviets survived by deception. Soviet strategic deception), Warszawa 2021.

[71] Staging (Russian: инсценировка) – a game for the needs of foreign services conducted by agents and cadres of their own service.

strategic victory without military action, only by means of systemic corruption and recruitment of officers and officials of the enemy state[72].

The research problems arising from the above analysis can be put in the form of two questions: 1) why did the Russians - after the annexation of Crimea and the partial separation of the Donbass from Ukraine - decide to launch a full-scale military operation in 2022? and 2) what made their actions this time met with strong resistance from the Ukrainian state?

Bibliography

Begoum F., *You and Your Walk-In*, "Studies in Intelligence" 1962, vol. 6, no. 1.

Freud A., *Das Ich und die Abwehrmechanismen*, Wien 1936.

Hempel A., *Policja granatowa w okupacyjnym systemie administracyjnym Generalnego Gubernatorstwa: 1939–1945* (Eng. Blue police in the occupation administrative system of the General Government: 1939-1945), Warszawa 1987.

Kahneman D., Slovic P., Tversky A., *Judgment under uncertainty: heuristics and biases*, New York 1982.

Kernberg O.F., *Borderline Conditions and Pathological Narcissism*, London 1990.

Kobierzycki T., *Filozofia osobowości* (Eng. Philosophy of personality), Warszawa 2001.

König K., *Abwehrmechanismen*, Göttingen–Zürich 2007.

Kuk A.I., *Kanwa wywiadu agenturalnego* (Eng. The canvass of agent intelligence), Warszawa 1994.

Mentzos S., *Interpersonale und institutionalisierte Abwehr,* Frankfurt am Main 1994.

[72] Cf.: "Among the class of officials, there are always corrupt people whose office has tainted their character, and others who have experienced injustice and been wronged. There are multitudes of sycophants and servants who covet wealth. Those who remain too long in their comfortable positions, and those who have not, in their mind, occupied the office that suits them, and those whose only desire is to make good use of time and circumstances to fulfil their selfish aims, as well as those who are double-minded, fickle, ephemeral, and those who are still waiting for their opportunity. You can be sure that all of these people can be secretly recruited for service against their state, providing them with a decent salary in gold and silk. Then you can rely on viable informants from their country or attempts to thwart plans turned against you. They are also free to create conflict between the ruler and his advisers so that they do not act in concert". S. Tzu, *Sztuka wojny* (Eng. Art of War) elaborated by J. Paterczyk, p. 80, https://www.academia.edu/41929781/Sun_Tzu_SZTUKA_WOJNY_czyli_TRZYNA%C5%9ACIE_ROZDZIA%C5%81%C3%93W [accessed: 21 VI 2023].

Renz B., *The Russian Force Structures*, "Russian Analytical Digest" 2007, no. 17, pp. 5-7.

Serov I.A., *Work with Walk-ins*, "Studies in Intelligence" 1962, vol. 8, no. 1.

Świerczek M., *Jak Sowieci przetrwali dzięki oszustwu. Sowiecka decepcja strategiczna* (Eng. How the Soviets survived by deception. Soviet strategic deception), Warszawa 2021.

Świerczek M., *2014 takeover of the SBU headquarters in Lugansk as an example of the operation of the Russian special services*, "Internal Security Review" 2023, no. 28, pp. 278-312. https://doi.org/10.4467/20801335PBW.23012.17662.

Tönnies F., *Wspólnota i stowarzyszenie* (Eng. Community and association), Warszawa 1988.

Russian and Ukrainian literature

Водолеев Г.С., Сидоренко С.Ф., *Спецнужды и спецслужбы*, Москва 2009.

Зданович А., *Польский крест советской контрразведки. Польская линия в работе ЧК-НКВД. 1918-1938*, Москва 2017.

Контрразведывательный словарь, Москва 1972.

Савченко А., *Антиукраїнець: або Воля до боротьби, поразки чи зради*, Київ 2020.

Internet sources

Crimea's Strategic Value to Russia, Center for Strategic and International Studies, 18 III 2014, https://www.csis.org/blogs/post-soviet-post/crimeas-strategic-value-russia [accessed: 6 VI 2023].

Danylov O., *As of January 1, 2023, the population of Ukraine was 28-34 million*, Mezha.Media, 7 IV 2023, https://mezha.media/en/2023/04/07/as-of-january-1-2023-the-population--of-ukraine-was-28-34-million/ [accessed: 7 VI 2023].

Janukowycz podpisał umowę o stacjonowaniu rosyjskiej floty na Ukrainie (Eng. Yanukovych signed agreement on stationing Russian fleet in Ukraine), Portal Spraw Zagranicznych, 29 IV 2010, https://psz.pl/162-wschod/janukowycz-podpisal-umowe-o-stacjonowaniu-rosyjskiej-floty-na-ukrainie [accessed: 7 VI 2023].

Map of sovereign states in Europe by projected 2023 GDP (PPP) percapita based on international dollars, https://en.wikipedia.org/wiki/List_of_sovereign_states_in_Europe_by_GDP_(PPP)_per_capita [accessed: 12 III 2024].

Samar W., *Russian «moles» in the State Security Service of Ukraine: what is missing in the Kulinich-Sivkovych' case?*, Center of Journalistic Investigations, 26 IV 2023, https://investigator.org.ua/investigations/253973/ [accessed: 16 VI 2023].

Transparency International Ukraine, https://www.transparency.org/en/countries/ukraine [accessed: 16 VI 2023].

Tzu S., *Sztuka wojny* (Eng. Art of War), elaborated by J. Paterczyk, https://www.academia.edu/41929781/Sun_Tzu_SZTUKA_WOJNY_czyli_TRZYNA%C5%9ACIE_ROZDZIA%C5%81%C3%93W [accessed: 21 VI 2023].

Russian and Ukrainian Internet sources

Агенты национальной опасности, dsnews.ua, 28 X 2013, https://www.dsnews.ua/economics/agenty-natsionalnoy-opasnosti-28102013090200 [accessed: 16 VI 2023].

Агрессивный крымский боевик Самвел оказался спецагентом Кремля и мог работать в СБУ, ТСН, 20 V 2014, https://tsn.ua/ru/politika/agressivnyy-krymskiy-boevik-samvel-okazalsya-specagentom-kremlya-i-mog-rabotat-v-sbu-366551.html [accessed: 16 VI 2023].

Более 10 тысяч солдат перешли на службу России, Безформата, https://angarsk.bezformata.com/listnews/soldat-pereshli-na-sluzhbu-rossii/62518616/ [accessed: 7 V 2023].

Виктор Янукович: «Народ договорится, и Украина станет единой», "Аргументы и Факты" 2014, no. 52, online version: https://aif.ru/euromaidan/viktor_yanukovich_eksklusivnoe_interview [accessed: 6 VI 2023].

Галеотти М., *«Сейлем» и «Башмаки». Крым и криминал до и после российской аннексии*, Крым.Реалии, 27 X 2014, https://ru.krymr.com/a/26658454.html [accessed: 16 VI 2023].

Генерал-коллекционер СБУ Свиридонов друг Куницына, ОРД, 20 XII 2009, https://ord-ua.com/2009/12/29/general-kollektsioner-sbu-sviridonov-drug-kunitsyina/ [accessed: 15 VI 2022].

Генерал Кривонос: про зраду в 2014-му, Порошенка, Зеленського, «клоунів» у РНБО і силове звільнення Донбасу, Радіо Свобода, 19 I 2020, https://www.radiosvoboda.org/a/rnbo-kryvonos-donbass-zrada-peremoga/30384758.html [accessed: 15 VI 2023].

ДЕРЖЗРАДА, Ukrinform, https://www.ukrinform.ua/tag-derzzrada [accessed: 14 VI 2023].

Документальный фильм «Корсуньский погром», YouTube, 30 VII 2014, https://www.youtube.com/watch?v=7FfPTBQ4l38 [accessed: 22 II 2023].

Закрытый доклад СБУ: на турецкие деньги «меджлис» вел разведку для Анкары, EADaily, 7 IV 2016, https://eadaily.com/ru/news/2016/04/07/zakrytyy-doklad-sbu-na-tureckie-dengi-medzhlis-vel-razvedku-dlya-ankary [accessed: 16 VI 2023].

Замглавы Меджлиса Умеров: Сотрудники СБУ и милиции в Крыму оказались предателями на 100%, военнослужащие - на 80%, прокуратура - на 70%, New Voice, 5 XI 2017, https://nv.ua/ukraine/politics/zamglavy-medzhlisa-umerov-sotrudniki-sbu-i--militsii-v-krymu-okazalis-predateljami-na-100-voennosluzhashchie-na-80-prokuratura--na-70-2135335.html [accessed: 7 V 2023].

Замглавы Меджлиса упрекнул Украину в сдаче Крыма без стрельбы, Черноморская телерадиокомпания, 6 XI 2017, https://blackseatv.com/in-the-spotlight/zamglavy-medzhlisa-upreknul-ukrainu-v-sdache-kryma-bez-strelby/ [accessed: 7 V 2023].

Козаченко О., *Умеров жалеет, что в Крыму не стали стрелять по русским*, Полит Навигатор, 3 XI 2017, https://m.politnavigator.net/umerov-zhaleet-chto-v-krymu-ne-stali-strelyat-po-russkim.html [accessed: 7 V 2023].

Корупція та зрада - це неприпустимі речі. І у професійному, і в людському плані. Це не можна пробачати», - Ігор Клименко, 7 II 2023, https://mvs.gov.ua/uk/news/korupciia-ta--zrada-ce-nepripustimi-reci-i-u-profesiinomu-i-v-liudskomu-plani-ce-ne-mozna-probacati-igor-klimenko [accessed: 15 VI 2023].

Коррупция - СТОП! Прокуратура признала действия СБУ не соответствующими законодательству, LB.ua, 23 V 2011, https://lb.ua/news/2011/05/23/97705_korruptsiya_stop_prokuratura_priz.html [accessed: 16 VI 2023].

Корсуньская трагедия - боевики Майдана пытают крымчан, поджёг автобусов. 20.02.2014, YouTube, 20 II 2017, https://www.youtube.com/watch?v=s2TGeF=-xbTc&list-PLeuqEfNtM8zleTyjJ-n8DXE2Uz9OHm2Ty [accessed: 23 II 2023].

Корсуньская трагедия Убивали только за то, что они из Крыма 2014 весна, YouTube, 27 V 2019, https://www.youtube.com/watch?v=bqUcM5YBWFw [accessed: 23 II 2023].

«Корсуньский погром»: зверства сторонников майдана, YouTube, 21 VI 2014, https://www.youtube.com/watch?v=hlf_AdGbfjE [accessed: 22 II 2023].

Круглов А., *На измене*, Совершенно Секретно, 30 X 2014, https://www.sovsekretno.ru/articles/bezopasnost/na-izmene/ [accessed: 7 V 2023].

Крым Путь на Родину Документальный фильм Андрея Кондрашова, YouTube, 4 X 2020, https://www.youtube.com/watch?v=PGGNXIQXlcU [accessed: 2 III 2023].

Милиция и СБУ закупили машин на 30 миллионов, bigmir)net, 15 XII 2010, https://auto.bigmir.net/autonews/autoworld/5217854-miliciya-i-sbu-zakupili-masin-na-30-millionov [accessed: 16 VI 2023].

Myrotvorets, https://myrotvorets.news/?s=%D0%B7%D1%80%D0%B0%D0%B4%D0%B-D%D0%B8%D0%BA [accessed: 14 VI 2023].

Нардеп Тымчук назвал число изменивших присяге крымских силовиков, Black Sea News, 6 XI 2017, https://www.blackseanews.net/read/136189 [accessed: 5 VI 2023].

Новые русские бандиты: кто контролирует Крым, Україна Кримінальна, 24 III 2014, https://cripo.com.ua/investigations/?p=172293/ [accessed: 16 VI 2023].

Официальная статистика: замглавы Меджлиса завысил количество предателей в Крыму на 10 %, Inform Napalm, 7 XI 2017, https://informnapalm.org/41430-ofitsialnaya--statistika-zamglavy-medzhlisa-zavysil-protsent/ [accessed: 7 V 2023].

Оперативный приказ Народного комиссара внутренних дел Союза ССР Николая Ежова № 00485. 11 августа 1937 г. о польской национальной операции, https://operacja-polska.pl/nkr/o-operacji-polskiej-nkw/dokumenty/966,00485-11-1937.html [accessed: 22 X 2019].

«Предатели на 100%»: Умеров резко высказался о спецслужбах в Крыму, OBOZ.UA, 5 XI 2017, https://news.obozrevatel.com/society/predateli-na-100-umerov-rezko-vyiskazal-sya-o-spetssluzhbah-v-kryimu.htm [accessed: 7 V 2023].

Про кількість та склад населення України за підсумками Всеукраїнського перепису населення 2001 року, https://web.archive.org/web/20071124125111/http://www.ukrcensus.gov.ua/results/general/nationality/ [accessed: 12 VI 2023].

Сколько военных ВСУ и СБУ перешли на сторону России в 2014 году, RF-SMI, 20 II 2022, https://rf-smi.ru/ykr/71072-skolko-voennyh-vsu-i-sbu-pereshli-na-storonu-rossii-v-2014-godu.html [accessed: 7 V 2023].

Сколько военных из Крыма предали Украину: шокирующие цифры, Panoptikon, 7 XI 2017, https://panoptikon.org/ukraine/98813-skolko-voennykh-iz-kryma-predali-ukrainu--shokirujushhie-cifry.html [accessed: 4 VI 2023].

Теперь пишут записки в Москву: озвучены масштабы предательства крымчан, From--UA, 30 XI 2017, https://from-ua.org/news/425623-teper-pishut-zapiski-v-moskvu-ozvucheni-masshtabi-predatelstva-krimchan.html [accessed: 7 V 2023].

Тымчук Д., *Сколько крымских силовиков стали предателями Украины*, UA Info, 6 XI 2017, https://uainfo.org/blognews/1509980385-skolko-ukrainskiy-silovikov-v-krymu-stali-predatelyami.html [accessed: 4 VI 2023].

Тымчук Д., a Facebook post, https://www.facebook.com/dmitry.tymchuk/posts/1366726656789319 [accessed: 9 VI 2023].

Тымчук назвал число предателей среди украинских силовиков в Крыму после аннексии, РБК-Україна, 6 XI 2017, https://www.rbc.ua/rus/news/tymchuk-nazval-chislo-predateley--sredi-ukrainskih-1509976026.html [accessed: 4 VI 2023].

Численность ФСБ, https://fsb.dossier.center/number/ [accessed: 12 VI 2023].

Marek Świerczek, PhD

Officer of the Internal Security Agency.

Contact: m.swierczek@abw.gov.pl