

TERRORYZM

studia
analizy
prewencja



**TERRORISM
PREVENTION**
Centre of Excellence



COS CENTRALNY OŚRODEK
SZKOLENIA I EDUKACJI ARW
ul. gen. dyw. Włocławca Bema 10/11 01-614 Warszawa

Zespół redakcyjny dr Damian Szlachter (redaktor naczelny)
Agnieszka Dębska (sekretarz redakcji, skład)
Aleksandra Dąbała, Aneta Olkowska, Izabela Paczesna,
Monika Sikora (redakcja językowa, korekta)

Projekt okładki Aleksandra Bednarczyk

© Copyright by Agencja Bezpieczeństwa Wewnętrznego 2024

ISSN 2720-4383

e-ISSN 2720-6351

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

Artykuły wyrażają poglądy autorów

Deklaracja o wersji pierwotnej:

Wersja drukowana czasopisma jest jego wersją pierwotną

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

Czasopismo jest dostępne w Portalu Czasopism Naukowych Uniwersytetu
Jagiellońskiego pod adresem: <https://www.ejournals.eu/Terroryzm/>

Materiały do czasopisma należy składać przez panel redakcyjny dostępny
pod adresem: <https://ojs.ejournals.eu/Terroryzm/about/submissions>

Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota”
ul. Nadwiślańczyków 2, 05-462 Wiązowna

Kontakt

tel. (+48) 22 58 58 671

e-mail: wydawnictwo@abw.gov.pl

www.abw.gov.pl/wyd/



Numer zamknięto i oddano do druku w marcu 2024 r.

Druk

Biuro Logistyki Agencji Bezpieczeństwa Wewnętrznego

ul. Rakowiecka 2A, 00-993 Warszawa

tel. (+48) 22 58 57 657

Rada naukowa

prof. dr hab. Sebastian Wojciechowski
Uniwersytet im. Adama Mickiewicza w Poznaniu,
Instytut Zachodni w Poznaniu

prof. dr hab. Waldemar Zubrzycki
Akademia Policji w Szczytnie

dr hab. Aleksandra Gasztold, prof. UW
Uniwersytet Warszawski

dr hab. Ryszard Machnikowski, prof. UŁ
Uniwersytet Łódzki

dr hab. Agata Tyburska
Akademia Policji w Szczytnie

dr hab. Barbara Wiśniewska-Paź, prof. UW
Uniwersytet Wrocławski

dr Piotr Burczaniuk
Agencja Bezpieczeństwa Wewnętrznego

dr Jarosław Jabłoński
Siły Zbrojne RP

dr Anna Matczak
Uniwersytet Nauk Stosowanych w Hadze

dr Paulina Piasecka
Collegium Civitas w Warszawie

Recenzenci numeru 5

dr Magdalena Adamczuk

dr Tomasz Białek

dr Daniel Boćkowski

dr Wojciech Grabowski

dr Marek Jeznach

dr Adam Krawczyk

dr Katarzyna Maniszewska

dr Anna Polak

dr Karolina Wojtasik

dr Jakub Zięty

SPIS TREŚCI

7 Wstęp redaktora naczelnego

ARTYKUŁY

13 **Krzysztof Izak**

*Dwadzieścia lat od ataków w Madrycie.
Problematyka bezpieczeństwa antyterrorystycznego Hiszpanii*

53 **Aleksander Olech**

*Grupa Wagnera w Afryce.
Pozorowana walka rosyjskich najemników z terroryzmem*

91 **Mariusz Cichomski**

*Między konfliktem zbrojnym a terroryzmem państwowym –
szczególne indywidualne środki ograniczające przyjęte w Polsce
w kontekście wojny w Ukrainie i sytuacji w Białorusi. Perspektywa prawna*

133 **Julia Puczyńska, Marcin Podhajski, Karolina Wojtasik, Tomasz P. Michalak**

*Duże modele językowe i możliwości ich wykorzystania
w terroryzmie dżihadystycznym i przestępczości*

ARTYKUŁY RECENZYJNE / RECENZJE

167 **Jędrzej Łukasiewicz**

*Recenzja książki: Rafał Miętiewicz, Systemy autonomiczne
w działaniach na morzu*

VARIA

175

Adam Tatarowski

*Budowanie odporności infrastruktury krytycznej
w świetle zagrożeń asymetrycznych i terroryzmu.
Tendencje legislacyjne w polskiej implementacji dyrektywy CER
ze szczególnym uwzględnieniem aspektów standaryzacji
i certyfikacji rozwiązań organizacyjno-technicznych*

195

Jarosław Przyjemczak, Nina Czyżewska

*Projekt APPRAISE.
Budowanie systemu bezpieczeństwa przestrzeni publicznych*

207

Wierzę, że poradzimy sobie z nowymi zagrożeniami!
Wywiad z płk. rez. Christopherem P. Costą, byłym doradcą
prezydenta USA do spraw walki z terroryzmem,
dyrektorem Międzynarodowego Muzeum Szpiegostwa w Waszyngtonie

221

English language version

Szanowni Państwo!

Piąty numer czasopisma „Terroryzm – studia, analizy, prewencja” (T-SAP) ukazuje się w dwudziestą rocznicę ataków terrorystycznych na madrycki system transportu miejskiego. Tragiczne wydarzenia z 11 marca 2004 r. pozostają dotychczas największym pod względem liczby ofiar śmiertelnych i rannych zamachem na terytorium Unii Europejskiej. Ich zaistnienie przyczyniło się do opracowania unijnych ram polityki antyterrorystycznej. Utworzono wówczas m.in. stanowisko europejskiego koordynatora do spraw zwalczania terroryzmu oraz przyjęto pierwszy plan działania UE w zakresie zwalczania terroryzmu. Kilkanaście miesięcy po tych atakach w Agencji Bezpieczeństwa Wewnętrznego powstał Departament Przeciwdziałania Terroryzmowi – odrębny pion do spraw walki z terroryzmem. Co roku dzień 11 marca przypomina o konieczności kontynuowania działań przeciwko ekstremizmowi i terroryzmowi oraz potrzebie zwiększania w społeczeństwie świadomości na temat tych zagrożeń. W celu upamiętnienia ofiar zamachu w Madrycie, wśród których było czworo Polaków, 11 marca jest obchodzony Europejski Dzień Pamięci o Ofiarach Terroryzmu. Przypomnieniem tych wydarzeń rozpoczynamy kolejne wydanie T-SAP. W artykule pt. *Dwadzieścia lat od ataków w Madrycie. Problematyka bezpieczeństwa antyterrorystycznego Hiszpanii* znajdują Państwo opis przebiegu ataków oraz analizę ich skutków politycznych i społecznych.

W tym numerze została również omówiona działalność Grupy Wagnera w Afryce oraz jej wpływ na walkę z terroryzmem na tym kontynencie z uwagi na to, że w ostatnich latach obecność rosyjskich najemników znacznie się tam zwiększyła. Liczymy, że opracowanie ponownie wywoła dyskusję

o zasadności umieszczania tego typu podmiotów na unijnej liście organizacji terrorystycznych.

Kolejny artykuł, do którego lektury chcielibyśmy Państwa zaprosić, to pierwsza w Polsce naukowa analiza szczególnych indywidualnych środków ograniczających przyjętych w RP w kontekście wojny w Ukrainie i sytuacji w Białorusi. W tekście zostały omówione relacje między krajowymi a unijnymi środkami ograniczającymi oraz przesłanki do wpisu podmiotów wspierających rosyjskie działania w Ukrainie na obowiązującą w Polsce listę sankcyjną.

Ostatnie miesiące przyniosły najbardziej dynamiczny rozwój technologii sztucznej inteligencji. W artykule poświęconym dużym modelom językowym, takim jak ChatGPT, autorzy opisują nowe możliwości, jakich dostarczają tego typu nowoczesne technologie, oraz wskazują, jak mogą zostać wykorzystane w terroryzmie dżihadystycznym i przestępczości.

Zachęcamy także do zapoznania się z recenzją monografii pt. *Systemy autonomiczne w działaniach na morzu*. Jest to pierwsze opracowanie w języku polskim, które tak wyczerpująco omawia wyzwania związane z ochroną portów morskich oraz morskiej infrastruktury strategicznej przed wrogim wykorzystaniem autonomicznych pojazdów pływających do działań sabotażowych i aktywności terrorystycznej.

Dzięki stworzeniu w ramach T-SAP przestrzeni do dyskursu o tym, jak zapobiegać oraz przeciwdziałać zagrożeniom o charakterze terrorystycznym i zwalczać je, czasopismo służy inicjowaniu rzeczowych dyskusji wśród ekspertów do spraw bezpieczeństwa. Zapraszamy do lektury tekstu na temat konieczności wypracowania nowego podejścia do oceny ryzyka w odniesieniu do infrastruktury krytycznej w świetle zagrożeń asymetrycznych i terroryzmu. Szczególną rolę w tych działaniach odegra standaryzacja i certyfikacja rozwiązań organizacyjno-technicznych wynikających z dyrektywy CER, w tym technicznych środków zapewnienia bezpieczeństwa fizycznego.

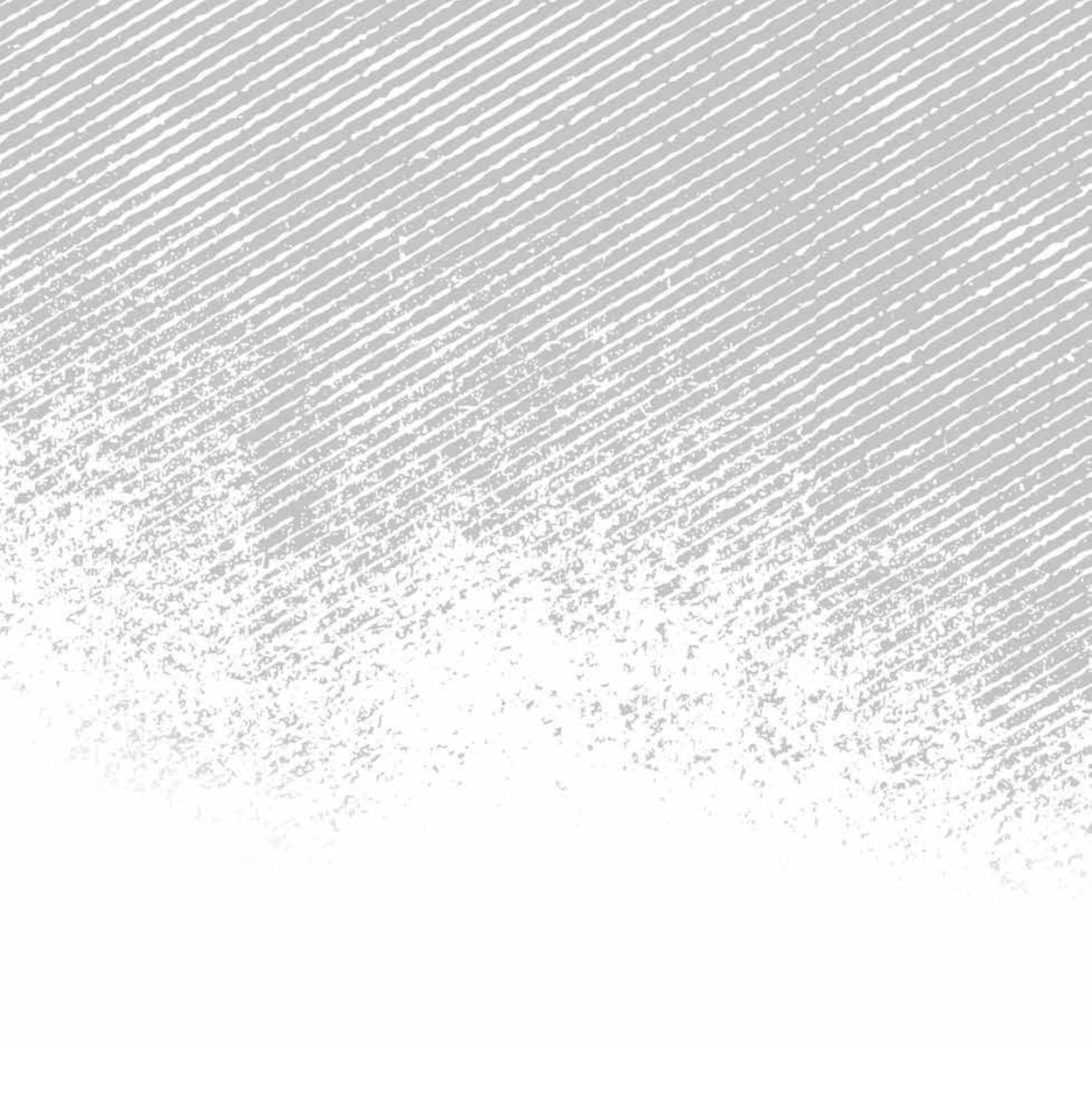
Polskie instytucje państwowe, ośrodki badawcze czy think tanki biorą udział w wielu inicjatywach antyterrorystycznych finansowanych ze środków UE i NATO. Chcielibyśmy, aby efekty tych przedsięwzięć były prezentowane również na łamach

T-SAP. Jednym z nich jest projekt APPRAISE będący elementem budowania systemu bezpieczeństwa przestrzeni publicznych.

W ostatniej części czasopisma publikujemy wywiad z byłym doradcą prezydenta USA do spraw terroryzmu, który opowiedział o zmianach w walce z terroryzmem w Stanach Zjednoczonych wprowadzonych po zamachach z 11 września 2001 r. oraz podzielił się ponadtrzydziestoletnim doświadczeniem zdobytym w czasie służby.

Zapraszając do lektury piątego numeru T-SAP, wyrażam nadzieję, że prezentowane w nim materiały będą miały wpływ na dyskusję dotyczącą polskich priorytetów w zakresie walki z terroryzmem, które zostaną przyjęte do realizacji w trakcie kolejnej prezydencji Polski w Radzie UE w pierwszej połowie 2025 r. Poprzednie polskie przewodnictwo w antyterrorystycznych grupach roboczych zostało uznane przez ekspertów w obszarze bezpieczeństwa wewnętrznego z krajów UE za jedno z najlepszych w latach 2010–2020.

Redaktor naczelny
dr Damian Szlachter



ARTYKUŁY

Dwadzieścia lat od ataków w Madrycie. Problematyka bezpieczeństwa antyterrorystycznego Hiszpanii

Twenty years since the Madrid attacks.
Spain's anti-terrorist security issues

KRZYSZTOF IZAK

Autor niezależny



<https://orcid.org/0000-0001-9815-6035>

Abstrakt

Celem artykułu jest przedstawienie przyczyn, chronologicznego przebiegu i skutków ataków przeprowadzonych 11 marca 2004 r. w Madrycie, z uwzględnieniem różnic i sprzeczności w doniesieniach na temat tych wydarzeń. Autor analizuje działania podejmowane przez władze Hiszpanii dla zapewnienia bezpieczeństwa antyterrorystycznego w kraju, w tym utworzenie struktur do walki z islamskim terroryzmem i muzułmańskim ekstremizmem. Omawia ponadto problemy i wyzwania wpływające na stan bezpieczeństwa państwa, z którymi mierzą się hiszpańskie służby walczące z przemocą polityczną i nielegalną migracją ludności z państw podwyższonego ryzyka.

Słowa kluczowe

Al-Kaida, ekstremizm muzułmański, ETA, imigranci, służby specjalne, terroryzm, zamachy

Abstract

The aim of the article is to present the causes, chronological course and effects of the attack carried out on March 11, 2004 in Madrid, taking into account differences and contradictions in reports about these events. The author analyses the actions taken by the Spanish authorities to ensure anti-terrorist security in the country, including the creation of structures to fight Islamic terrorism and Muslim extremism. He also discusses the problems and challenges faced by Spanish services fighting political violence and illegal migration of people from high-risk countries, which affect the state of state security.

Keywords

Al-Qaeda, Muslim extremism, ETA, immigrants, secret services, terrorism, attacks

Hiszpania należy do krajów najdłużej walczących z terroryzmem. Separatystyczna organizacja Kraj Basków i Wolność (Euskadi Ta Askatasuna, ETA) prowadziła ataki terrorystyczne nieprzerwanie przez ponad 50 lat. W 2011 r. baskijscy nacjonalisci ogłosili zakończenie działalności zbrojnej. Dwa lata później doszło do samorozwiązania Batasuny – politycznego skrzydła ETA, a w 2018 r. samej ETA. Od 1960 r., czyli początku istnienia organizacji, zginęło – według różnych publikacji prasowych i książek – od 830 do 857 osób, m.in. wojskowych, funkcjonariuszy Gwardii Obywatelskiej (Guardia Civil), policjantów, polityków, sędziów i przypadkowych ludzi. Ponadto ETA dokonała 84 porwań.

W pierwszej dekadzie XXI w. Hiszpania zmagła się z dwoma odmiennymi obliczami terroryzmu: nacjonalistyczno-separatystycznym oraz islamskim. Po atakach z 11 września 2001 r. Hiszpania wzięła udział w operacji przeciwko talibom w Afganistanie. Była również inicjatorem i sygnatariuszem tzw. listu ośmiu podpisanego 30 stycznia 2003 r. przez premierów Hiszpanii, Polski, Portugalii, Włoch, Wielkiej Brytanii, Węgier, Danii oraz prezydenta Czech. Pismo było wyrazem solidarności ze Stanami Zjednoczonymi we wspólnej walce w obronie demokracji przeciwko reżimowi Saddama Husajna. List ten dowodził powstałego w Europie podziału dotyczącego kwestii irackiej. Rząd Hiszpanii konsekwentnie popierał interwencję w Iraku. Wynikało to z tego, że reżim Husajna nie wypełniał rezolucji ONZ i nie przejawiał najmniejszej woli współpracy z inspektorami

Międzynarodowej Agencji Energii Atomowej, którzy mieli sprawdzić, czy zlikwidowano zapasy uzbrojenia i wstrzymano prace nad bronią masowego rażenia¹.

Stan zagrożenia terrorystycznego w Hiszpanii w okresie poprzedzającym ataki

Zanim doszło do ataków w Madrycie, hiszpańskie służby obserwowały miejscową sieć Al-Kaidy oraz komórki terrorystyczne powiązane z organizacjami ekstremistycznymi w Algierii i Maroku. W ich utworzeniu na terenie Hiszpanii w latach 90. XX w. pomogła budowa sieci meczetów finansowanych przez Arabię Saudyjską i organizacje charytatywne pozostające pod jej wpływem. W meczetach pracowali często imamowie i kaznodzieje wyznający najbardziej radykalną, salaficką doktrynę islamu, zakazującą integracji muzułmanów ze społeczeństwem zachodnim i propagujący koncepcję dżihadu jako walki zbrojnej z „niewiernymi”.

W latach 90. XX w. w Hiszpanii aktywnie działał Syryjczyk Imad Ed-din Barakat alias Abu Dahdah, jeden z założycieli komórki Al-Kaidy w tym kraju i jej domniemany przywódca. Z portu lotniczego Adolfo Suárez Madryt-Barajas odprawiał ochotników dżihadu do walk w Bośni, Czeczenii i Afganistanie. Rannym bojownikom zapewniał leczenie w hiszpańskich szpitalach. W pierwszej połowie lat 90. XX w. w Hiszpanii mieszkał także inny Syryjczyk – uważany za jednego z najbliższych współpracowników Osamy bin Ladena – Mustafa Setmariam Nasar alias Abu Musab al-Suri. Po zawarciu przez niego małżeństwa z Hiszpanką, która przeszła na islam, otrzymał obywatelstwo tego kraju². W Hiszpanii działała również siatka Marokańskiej Islamskiej Grupy Walczącej (Al-Dżama’a al-Islamijja

¹ Później USA i inne państwa poinformowały, że żadnej broni masowego rażenia w Iraku nie znaleziono, a doniesienia na temat jej posiadania przez to państwo były fałszywe, propagowane w celu stworzenia casus belli.

² Abu Musab al-Suri jest uznawany za najbardziej elokwentnego ideologa współczesnego dżihadu i wyrafinowanego stratega. Jego dzieło pt. *Dawa al-mukawama al-islamijja al-alamijja* (pol. Wezwanie do islamskiego światowego oporu) opublikowane w cyberprzestrzeni w 2004 r. i liczące 1604 strony było najczęściej cytowane na islamistycznych stronach. W 2005 r. Al-Suri został aresztowany w Pakistanie i przekazany Syrii, w której był poszukiwany za działalność ekstremistyczną w latach 80. XX w. Nie wiadomo, gdzie przebywa obecnie. Zob. S. Grześkowiak, *Poczet islamskich ideologów i ekstremistów*, Warszawa 2023, s. 307–318.

al-Mukatila fi al-Maghrib) oraz algierskiej Islamskiej Grupy Zbrojnej (Al-Dżama'a al-Islamijja al-Musallaha). Warto wiedzieć, że pięciu spośród terrorystów, którzy 11 września 2001 r. skierowali samoloty na cele w USA, przebywało w Hiszpanii, dopracowując szczegóły zamachu z łącznikiem Al-Kaidy Ramzim bin asz-Szibhem.

W październiku 2001 r. Bin Laden w telewizji Al-Dżazira mówił o Hiszpanii jako arabskiej Andaluzji: *Niechaj cały świat wie, że nigdy nie zaakceptujemy, aby tragedia Al-Andalus mogła się powtórzyć*³. Podczas operacji „Daktyl” („Dátíl”) prowadzonej w listopadzie 2001 r. oraz w kwietniu i lipcu 2002 r. policja rozbiła hiszpańską sieć Al-Kaidy, w której znaczącą rolę odgrywała tzw. grupa syryjska. Zatrzymano wtedy Abu Dahdaha i dziesięć osób należących do tej grupy, w większości Syryjczyków. Aresztowano wówczas także kilkadziesiąt osób, z których 25 w 2003 r. stanęło przed sądem w Madrycie⁴. Jednocześnie zarówno obywatele Hiszpanii, jak i obiekty należące do tego kraju były celami ataków terrorystycznych w Iraku, Algierii i Maroku.

W maju 2003 r. dowództwo sił USA powierzyło Polsce organizację w Iraku Wielonarodowej Dywizji Centrum-Południe (Multinational Division Central-South, MND C-S), a następnie dowodzenie nią. Oficjalnie MND C-S rozpoczęła działania 3 września 2003 r. W pierwszej fazie⁵ składała się z trzech wielonarodowych brygad: polskiej, liczącej 2400 żołnierzy w prowincjach Babilon i Karbała; ukraińskiej, w której skład wchodziło 1800 żołnierzy odpowiadających za prowincję Wasit; hiszpańskiej w liczbie 1300 żołnierzy, którym zostały przydzielone do kontroli bezpieczeństwa prowincje Al-Kadisijja i An-Nadżaf⁶. José Maria Aznar z prawicowej Partii Ludowej (Partido Popular, PP) postrzegał interwencję w Iraku jako element wojny z terroryzmem i uznawał go za największe zagrożenie we współczesnym świecie. Twierdził, że zadaniem NATO jest rozwinięcie odpowiednich instrumentów politycznych i militarnych do walki z nim. Stanowisko to

³ *What's Osama Talking About?*, Slate, 8 X 2001 r., <https://slate.com/news-and-politics/2001/10/what-s-osama-talking-about.html> [dostęp: 8 X 2001].

⁴ R. Gunaratna, *Spain: An Al Qaeda Hub?*, „UNISCI Discussion Papers” 2004, nr 5, <https://www.redalyc.org/pdf/767/76712467002.pdf>, s. 1–8 [dostęp: 22 II 2014]; Fernando Reinales, *experto en terrorismo internacional, advierte: “Al Qaeda está hoy más extendida de lo que ha estado nunca”*, Universidad Internacional Menéndez Pelayo, <https://www.uimp.es/actualidad-uimp/fernando-reinales-experto-terrorismo-internacional.html> [dostęp: 21 VI 2021].

⁵ Więcej o MND C-S w dalszej części artykułu (przyp. red.).

⁶ M. Brylew, *Irak 2006–2012. Stabilizacja czy konflikt?*, Toruń 2013, s. 50.

odzwierciedlało jego osobisty stosunek do terroryzmu, wyrażany wielokrotnie wcześniej także w kontekście zagrożeń ze strony ETA⁷.

Przeciwnikami wysłania sił hiszpańskich do Iraku była większość społeczeństwa i opozycyjna Hiszpańska Socjalistyczna Partia Robotnicza (Partido Socialista Obrero Español, PSOE) kierowana przez José Luisa Rodríguez Zapaterę. W 2003 r. organizowano masowe protesty przeciwko wyjazdowi żołnierzy do Iraku. W październiku tego samego roku Bin Laden oskarżył USA o realizację imperialnych interesów. Zagroził także Włochom, Turcji, Wielkiej Brytanii, Japonii, Australii, Holandii, Polsce i Hiszpanii, że jeśli nie wycofają swoich wojsk z Iraku, to zostaną podjęte przeciwko nim właściwe kroki odwetowe⁸.

W końcu listopada 2003 r. w zasadzce zginęło siedmiu członków grupy zadaniowej hiszpańskiego Narodowego Centrum Wywiadu (Centro Nacional de Inteligencia, CNI), a jeden został ranny. Do zdarzenia doszło na ruchliwej szosie, 30 km na południe od Bagdadu⁹. Na początku grudnia 2003 r. Instytut Islamskiego Centrum Mediów Dżihadu (Markaz al-Islam al-Dżihadi Media Institut) kontrolowany przez Organizację Al-Kaidy na Półwyspie Arabskim (Tanzim Al-Kaida fi Dżazirat al-Arab) opublikował w internecie czterostronicowe „Przesłanie do narodu hiszpańskiego” oraz czterdziestosiedmiostronicową analizę sytuacji w Iraku i roli mudżahediniów walczących w imię islamu¹⁰. W tym drugim dokumencie jeden rozdział poświęcono szczegółowemu omówieniu realiów politycznych, gospodarczych i społecznych Wielkiej Brytanii, Polski i Hiszpanii, które poparły USA w wojnie w Iraku. Pomijając obszerne wątki odnoszące się do Iraku i USA, za szczególnie interesujący można uznać fragment dotyczący Hiszpanii, której poświęcono sześć stron. Autor lub autorzy wysunęli tezę, że władze tego kraju można zmusić do wycofania wojska z Iraku przez przeprowadzenie kilku dotkliwych ataków. Takie działanie miałyby wpływ

⁷ P. Domejko-Kozera, *Polityka bezpieczeństwa w Hiszpanii w latach 1992–2004*, Warszawa 2006, s. 46.

⁸ A. Wejkszner, *Ewolucja terroryzmu motywowanego ideologią religijną na przykładzie salafickiego ruchu globalnego dżihadu*, Poznań 2010, s. 338.

⁹ *Siedmiu hiszpańskich agentów zginęło w Iraku*, Wirtualna Polska, 29 XI 2003 r., <https://wiadomosci.wp.pl/siedmiu-hiszpańskich-agentow-zginelo-w-iraku-6036492925121665a> [dostęp: 30 XI 2003].

¹⁰ H.A. Fernández, *Does al-Qaeda have a global strategy?*, Elcano Royal Institute, 4 V 2004 r., <https://www.realinstitutoelcano.org/en/analyses/does-al-qaeda-have-a-global-strategy/> [dostęp: 6 V 2004].

na wybory. Można bowiem przewidzieć, że rząd nie utrzyma się w następstwie dwóch, trzech uderzeń, a pod wpływem presji społeczeństwa wycofa część sił. Prognozowano, że pewne zwycięstwo odniesie wówczas partia socjalistyczna, która sprzeciwiała się wysłaniu żołnierzy do Iraku i że to właśnie ona doprowadzi do wyjazdu stamtąd hiszpańskiego kontyngentu. Taka decyzja Madrytu, w połączeniu z podjęciem podobnej przez Rzym, wywołałaby społeczną i polityczną presję w Wielkiej Brytanii. W jej wyniku premier Tony Blair utraciłby władzę. Nie ulega wątpliwości, że autor lub autorzy dokumentów byli doskonale zorientowani w sytuacji politycznej Europy, w tym Polski jako lojalnego sojusznika Stanów Zjednoczonych¹¹.

W dniu 24 grudnia 2003 r. został udaremniony zamach bombowy na dworcu kolejowym Chamartin w północnej części Madrytu. W pociągu Intercity z Irún w Kraju Basków do Madrytu terroryści z ETA zamierzali umieścić dwie walizki zawierające ładunki wybuchowe o łącznej masie ok. 50 kg. Policja zapobiegła tragedii – jedną bombę zdołano przechwycić, ponieważ aresztowano w San Sebastián terrorystę Garikoitza Arruarte'a Santacruza, który niósł walizkę z 25 kg materiału wybuchowego. Drugą bombę odnaleziono w przedziale bagażowym pociągu. Zatrzymano go na stacji kolejowej w Burgos i – po uprzedniej ewakuacji pasażerów – ładunek zdetonowano. Został on umieszczony w pociągu w San Sebastián przez Gorce Lorana, którego następnie aresztowano. Bomby miały eksplodować w Chamartin w popołudniowych godzinach szczytu. Według ekspertów godziny ustawione na zapalnikach sugerowały, że ETA nie tyle chciała dokonać masakry, ile wywołać panikę i chaos. Wszystkich pasażerów i pracowników kolei zdołano by ewakuować, ponieważ ETA miała zwyczaj ostrzegać przed zamachami bombowymi. Nagranie z takim ostrzeżeniem policja znalazła w kryjówce aresztowanych terrorystów¹². Dnia 26 grudnia 2003 r. na torach linii Zaragoza–Caspe–Barcelona znaleziono bombę, która miała wybuchnąć 31 grudnia 2003 r.

W dniu 29 lutego 2004 r. funkcjonariusze Gwardii Obywatelskiej zatrzymali młodych terrorystów należących do ETA: Gorkę Vidala Álvarę i Irkusa Badillo Borde'a, którzy w furgonetce wieźli 536 kg materiałów wybuchowych. W samochodzie znajdowała się również mapa Madrytu

¹¹ Tamże.

¹² *ETA pretendía volar la estación de Chamartín con un „tren bomba” y provocar una masacre*, ABC España, 26 XII 2003 r., https://www.abc.es/espana/abci-pretendia-volar-estacion-chamartin-tren-bomba-y-provocar-masacre-200312260300-228547_noticia.html [dostęp: 26 XII 2003].

z zaznaczonym okręgiem obejmującym Park Handlowy NII, lotnisko i fragment miejscowości Alcalá de Henares. Celem kolejnego ataku miała być stacja metra Avenida de América w Madrycie. Jeden z terrorystów przyznał, że ETA planowała podczas przerwy świątecznej przeprowadzić zamach na króla¹³. Służby specjalne spodziewały się również wielkiego zamachu w Madrycie przed wyborami 14 marca, jako pokazu siły ze strony separatystów baskijskich w momencie kryzysu, który nastąpił w organizacji. Aby uniemożliwić terrorystom realizację planów, postawiono w stan gotowości wszystkie służby strzegące bezpieczeństwa państwa¹⁴.

Przygotowania do ataków terrorystycznych w Madrycie

Według hiszpańskiej policji pomysłodawcą ataków był Rabei Osman Ahmed alias Muhammad al-Masri (Muhammad Egipcjanin), wcześniejszy oficer armii Egiptu i specjalista od materiałów wybuchowych. W latach 90. XX w. przebywał w Afganistanie, gdzie nawiązał kontakt z Al-Kaidą. W 1999 r. dotarł nielegalnie do Niemiec. Następnie został aresztowany w pociągu podczas podróży do Francji, ponieważ jechał bez dokumentów. Podał przy tym fałszywą tożsamość – zapewniał, że jest Palestyńczykiem. Po odbyciu w więzieniu trafił do obozu dla uchodźców w Lebach, gdzie uzyskał roczne zezwolenie na pobyt. W tym czasie stał się aktywnym kaznodzieją, głoszącym nienawiść do Żydów. Tuż przed zamachami z 11 września 2001 r. pojawił się w Hiszpanii. W Madrycie nawiązał z nim kontakt obywatel Tunezji Serhan Abdel Madżid Fakhit (Sirhan bin Abdelmadżid Fakhit) alias El Tunecino (Tunezyjczyk), który przyjechał do Hiszpanii w 1996 r. w ramach programu stypendialnego. Podjął studia doktoranckie z ekonomii, ale ich nie ukończył. Głosił za to coraz bardziej radykalne poglądy, aż stał się fanatykiem religijnym. Zradyzalizował się pod wpływem imama Munira Mahmuda al-Masariego z meczetu M-30 w Madrycie. Zasługą Tunezyjczyka była odbudowa w stolicy Hiszpanii komórki Al-Kaidy. W jej skład weszli głównie Marokańczycy, którzy dotąd nie stanowili zagrożenia i pozostawali na wolności po operacji „Daktyl”. Aresztowani wówczas obywatele Syrii, Algierii i Tunezji byli doświadczonymi bojownikami, mającymi za sobą

¹³ *Actividad Terrorista de ETA 2004*, Ministerio del Interior, <https://www.statewatch.org/media/documents/news/2005/jan/mirbal2004acteta.pdf> [dostęp: 12 III 2005].

¹⁴ Tamże.

wojenną przeszłość w Bośni, Czeczenii i Afganistanie. Fakhret zaprzyjaźnił się z Algierczykiem Ahmedem Brahimem, domniemanym skarbnikiem Al-Kaidy w Hiszpanii, a po jego aresztowaniu – w związku z zamachami na ambasadę USA w Kenii i Tanzanii 7 sierpnia 1998 r. – z rodziną Brahima. Tunezyjczyk prawdopodobnie utrzymywał kontakty z innymi grupami ekstremistów działającymi w Hiszpanii, niezwiązanymi bezpośrednio z jego komórką, ale funkcjonującymi w ramach międzynarodowych struktur dżihadu¹⁵. Znajomość z Al-Masrim, który w Hiszpanii często zmieniał tożsamość i dokumenty, przyczyniła się do tego, że Fakhret został organizatorem i koordynatorem ataków na pociągi w Madrycie. Jeszcze przed tym wydarzeniem Al-Masri opuścił Hiszpanię. Wyjechał do Włoch, gdzie zatrudnił się jako murarz i planował duży zamach w Europie oraz rekrutował islamskich ochotników do walki z siłami NATO w Iraku. Po ucieczce Al-Masriego z Hiszpanii Fakhret przejął jego bazę logistyczną i kontakty. O pomoc w przeprowadzeniu ataków zwrócił się do Amera Aziziego alias Osmana al-Andalusiego, uznawanego za prawą rękę Abu Dahdaha. Po jego aresztowaniu Azizi przejął kierownictwo nad hiszpańską komórką Al-Kaidy. Po atakach w USA w 2001 r. ukrył się na tydzień przed madrycką policją. Po powrocie do stolicy Hiszpanii szybko sprzedał swój samochód i uciekł z kraju. W listopadzie 2001 r. podczas likwidacji hiszpańskiej komórki Al-Kaidy policja odnalazła w domu Aziziego dokumenty wskazujące na jego kontakty z tą organizacją, werbowanie młodych muzułmanów do szkolenia w Afganistanie i powiązania z niektórymi zamachowcami z 11 września 2001 r., którym wraz z Abu Dahdahem zorganizował spotkanie w Tarragonie. Utrzymywał również kontakty z organizatorami zamachów w Casablance w nocy z 16 na 17 maja 2003 r.¹⁶ Azizi był także łącznikiem między Al-Kaidą a Marokańską Islamską Grupą Walczącą i tę okoliczność próbował wykorzystać Tunezyjczyk. Spotkanie obu ekstremistów odbyło się w Turcji na przełomie 2002 i 2003 r. Fakhret zwrócił się do Aziziego z prośbą o przydzielenie mu do przeprowadzenia operacji terrorystycznej bojowników gotowych umrzeć jako męczennicy. Azizi odmówił, ponieważ tacy ludzie zostali aresztowani. Pozwolił mu natomiast działać w imieniu Al-Kaidy.

¹⁵ F. Reinares, *Al-Qaeda's Revenge. The 2004 Madrid Train Bombings*, New York 2016, s. 56–59.

¹⁶ W maju 2003 r. grupa 14 terrorystów należących do organizacji Salaficki Dżihad (As-Salafijja al-Dżihadijja) zaatakowała w Casablance dwie restauracje, hotel Farah, konsulnat belgijski, ośrodek i cmentarz żydowski. Zginęło 31 osób, a ok. 100 zostało rannych. Zob. K. Izak, *Leksykon organizacji i ruchów islamistycznych*, Warszawa 2014, s. 117.

Polecił również Marokańczyka Dżamala Zugama, który mógłby pomóc w zorganizowaniu sprawnie działającej grupy terrorystycznej¹⁷.

Według koncepcji Fernando Reinaresa, hiszpańskiego eksperta w zakresie terroryzmu, to Azizi był inicjatorem ataków w Madrycie. Jego nazwisko występuje w 149 z 271 tomów akt sądowych dotyczących wydarzeń z 11 marca 2004 r.¹⁸ Decyzja o atakach w Hiszpanii zapadła podobno w Karaczi w południowym Pakistanie. Plan zatwierdzono w lutym 2002 r. na spotkaniu Al-Kaidy w Turcji, w którym wziął udział także Azizi. W 2005 r. zginął on w wyniku amerykańskiego nalotu w Waziristanie Północnym na terenie zachodniego Pakistanu¹⁹. Reinares podważył przede wszystkim propagowaną przez środowiska lewicowe tezę wiążącą madrycki zamach z wojną w Iraku. Zgodnie z jego koncepcją ataki w Madrycie miały być zemstą Al-Kaidy za rozbitcie w latach 2001–2002 przez policję jej hiszpańskiej siatki. Ataki te nie miały natomiast nic wspólnego z przebywaniem hiszpańskich żołnierzy w Iraku, ponieważ rozpoczęli oni misję w 2003 r. Ich obecność dopiero wówczas stała się doskonałym pretekstem do przeprowadzenia ataków²⁰. Do wczesnych przygotowań serii zamachów w Madrycie przyznał się Al-Masri w rozmowie telefonicznej ze swoim „podopiecznym” Palestyńczykiem²¹. Została ona podsłuchana przez włoską policję w maju 2004 r. Al-Masri stwierdził w niej m.in., że przygotowania do ataków zajęły mu dwa i pół roku. Mimo że w kluczowym momencie nie było go w Madrycie, to utrzymywał kontakt z zamachowcami²². Wśród organizatorów zamachu

¹⁷ F. Reinares, *Al-Qaeda's Revenge...*, s. 118–120; Z. Jakubowska, *Madryt 11 marca*, Warszawa 2005, s. 116–117.

¹⁸ *Madrid bombings 'probably al Qaeda'*, Stuff, 21 I 2010 r., <https://www.stuff.co.nz/vl-push/world/3226277/Madrid-bombings-probably-al-Qaeda> [dostęp: 21 I 2010].

¹⁹ A. Hernández, *11M: quién fue el autor intelectual y otras claves que plantea el documental de Netflix sobre el mayor atentado yihadista en Europa*, BBC, 11 III 2022 r., <https://www.bbc.com/mundo/noticias-60693476> [dostęp: 11 III 2022]; W. Maclean, *New evidence of Qaeda tie to Madrid blast: expert*, Reuters, 13 I 2010 r., <https://www.reuters.com/article/cnews-us-security-spain-qaeda-idCATRE60B52020100112> [dostęp: 13 I 2010]; A. Martin Plaza, *Los atentados del 11M que sacudieron España*, RTVE, 11 III 2014 r., <https://www.rtve.es/noticias/20140311/atentados-del-11m-sacudieron-espana/893543.shtml> [dostęp: 11 III 2014].

²⁰ F. Reinares, *The Evidence of Al-Qa`ida's Role in the 2004 Madrid Attack*, „CTC Sentinel” 2012, t. 5, nr 3, <https://ctc.westpoint.edu/the-evidence-of-al-qaidas-role-in-the-2004-madrid-attack/> [dostęp: 18 IV 2012].

²¹ Z. Jakubowska, *Madryt 11 marca...*, s. 114–115.

²² *Llega a España "El Egipcio" para ser juzgado por el 11-M*, 20 minutos, 17 XI 2006 r., <https://www.20minutos.es/noticia/173755/0/egipcion/11-m/italia/> [dostęp: 17 XI 2006].

znajdował się również Marokańczyk Hasan al-Haski, uznawany za przywódcę komórki Marokańskiej Islamskiej Grupy Walczącej w Hiszpanii, w której pojawił się po dłuższym pobycie w Belgii²³.

Korzystając z rady Aziziego, Fakheta nawiązał kontakt z Zugamem. Był on wraz z rodakami Muhammadem Chaouim i Muhammadem Bekkalim współwłaścicielem sklepu z telefonami komórkowymi Nuevo Siglo (Nowy Wiek) w madryckiej dzielnicy Lavapiés. Zugam był znany policji od 2001 r., kiedy rozpracowywano siatkę Al-Kaidy w Hiszpanii. Został aresztowany, a następnie zwolniony z więzienia – mimo jego wiadomych powiązań z algierską Islamską Grupą Zbrojną, z wieloma ludźmi Abu Dahdaha, z Azizim i Muhammadem al-Fizazim, jednym z najbardziej radykalnych kaznodziejów z Maroka. Inną osobą pomagającą Fakhetowi werbować ochotników do komórki terrorystycznej i najprawdopodobniej finansującą przygotowania do zamachu był Marokańczyk Dżamal Ahmidan, zwany „Chińczykiem” lub „Mowglim” – bogaty właściciel sklepu z ubraniami i handlarz narkotyków, który został zastępcą Tunezyjczyka. Kolejną postacią z grupy zamachowców był Marokańczyk Rafa Zuhier, współpracownik „Chińczyka” w handlu narkotykami. Utrzymywał on również kontakty z osobami mającymi dostęp do materiałów wybuchowych. Relacje te nawiązał podczas pobytu w więzieniu, w którym odsiadywał wyrok za napad z użyciem broni palnej. Poznał tam Hiszpana Antonia Toro Castrę, handlarza narkotykami i materiałami wybuchowymi, którego szwagier Jose Emilio Suárez Trashorras był górnikiem w Avilés (miejscowości położonej w Asturii na północnym zachodzie Hiszpanii). Po opuszczeniu zakładu karnego Zuhier nadal utrzymywał znajomość z Castrą i jego współpracownikami. Skontaktował ich z marokańskimi handlarzami narkotyków. Zażyłość między muzułmanami i Hiszpanami była tak duża, że ci pierwsi zostali nawet zaproszeni na ślub Trashorrasa z siostrą Castry, który odbył się w lutym 2004 r. W tym czasie toczyły się już negocjacje dotyczące zakupu przez Marokańczyków ok. 200 kg materiału wybuchowego goma-2 eco wytwarzanego na bazie dynamitu, używanego w hiszpańskim przemyśle budowlanym i górnictwie. Był on również oprócz tytadyny produkowanej we Francji stosowany przez ETA. Zakup przez Hiszpanów materiału wybuchowego za 6000 euro i 25 kg haszyszu uzasadniano wykorzystaniem zarówno w Maroku, jak i do wysadzania sejfów podczas napadów w Madrycie. Materiał pochodził z kopalni kaolinu „Conchita” należącej do firmy Caolines de Merilles, w której

²³ F. Reinares, *The Evidence of Al-Qa`ida's Role...*, s. 51–52.

poprzednio pracował Trashorras. Gomeę-2 eco wywiózł z zakładu Emilio Llano Álvarez, nadzorca w kopalni „Conchita”²⁴.

Materiał wybuchowy był najpierw przesyłany w niewielkich ilościach w luku bagażowym autokarów liniowych kursujących między Asturią i Madrytem. Towar wysyłał szesnastoletni chłopiec, którego nazywano „Cyganek” („Gitano”)²⁵. Po największą część gomy Marokańczycy osobiście przyjechali do Aviles, gdzie odebrali ją bezpośrednio od Trashorrasa. Przygotował on również gwoździe i śruby, które miały wzmocnić śmiertcioną moc materiału wybuchowego. Z Avilés do Madrytu Marokańczycy wracali dwoma samochodami: własnym volkswagenem golfem, w którego bagażniku przewozili gomeę-2 eco, i pożyczoną od Hiszpanów toyotę. Kierował nią „Chińczyk”, który jechał jako pierwszy i miał ostrzegać przed patrolami policji. Był on już wcześniej trzykrotnie zatrzymywany i karany mandatami za różne wykroczenia. Materiał wybuchowy bezpiecznie dowieziono do wiejskiego domu w Morata de Tajuña w okolicach Chinchón na przedmieściach Madrytu. Był to rejon mało uczęszczany, a budynek całkowicie ogrodzony zasłaniającym parkanem. Nieruchomość służyła wcześniej za schronienie dla nielegalnych imigrantów, którzy sympatyzowali z muzułmańskimi ekstremistami. Należała ona do Syryjczyka aresztowanego w 2001 r. pod zarzutem przynależności do Al-Kaidy. Pierwszym najemcą był Marokańczyk zatrzymany w 2003 r. w związku z zamachem w Casablance, drugim zaś „Chińczyk”. Miesiąc przed atakiem w wiejskim domu rozpoczął się wzmożony ruch związany z wytwarzaniem bomb na bazie materiałów wybuchowych przywiezionych z Avilés. Jako zapalników użyto aluminiowych detonatorów i telefonów komórkowych. Telefony do sklepu Nuevo Siglo dostarczyli dwaj Hindusi: Vinay Kohly i Suresh Kumar. Następnie Zugam zawiózł je do domu na wsi, gdzie zostały przerobione na zapalniki czasowe. Dokonali tego prawdopodobnie wspomniani wyżej Chaoui i Bekkali. Bomby skonstruował Marokańczyk Abderrahman Zbakin zwany „Chemikiem”. Częstymi gośćmi byli również Zugam, „Chińczyk” i Trashorras. Przez cały czas w domu przebywał Osman al-Ghanut, młody Marokańczyk pracujący jako murarz i pomagający w przygotowaniu ładunków wybuchowych. Skonstruowano łącznie 13 bomb, które umieszczono w plecakach i torbach. Gotowe ładunki wybuchowe przewieziono skradzionym furgonem marki Renault Kangoo

²⁴ Z. Jakubowska, *Madryt 11 marca...*, s. 126.

²⁵ Ze względu na młody wiek chłopca nie podawano jego nazwiska do publicznej wiadomości.

i samochodem osobowym firmy Škoda do domu w madryckiej dzielnicy Alcalá, zamieszkaney przez imigrantów z Afryki Północnej, oraz do wynajętego trzy dni przed atakiem mieszkania w dzielnicy Leganés. Znajdowało się ono na pierwszym piętrze budynku i liczyło prawie 100 m² powierzchni. W dniu 10 marca terroryści zaangażowani w umieszczenie bomb w pociągach dokonali rytualnego oczyszczenia w zakładzie fryzjerskim należącym do Marokańczyka Abdeluaida Berraka, przyjaciela Abu Dahdaha. Łącznie w przygotowaniach do zamachu uczestniczyło ponad 40 osób²⁶.

Przebieg ataków

Rankiem w czwartek 11 marca 2004 r. siedmiu terrorystów: Tunezyjczyk Fakhet oraz Marokańczycy – Ahmidan, Abd an-Nabi Kundża, Allakema Lamari, Muhammad Ulad Akcha, jego brat Rachid Oulad Akcha i Asri Rifat Anuar – przyjechało samochodami marek Renault Kangoo i Škoda do Alcalá de Henares, miasta oddalonego ok. 30 km na wschód od Madrytu, aby podłożyć bomby w wagonach kolei miejskiej Cercanias. Zarówno w samym Madrycie, jak i jego okolicach znajduje się dziesięć głównych linii tych pociągów. Składy kolejowe, oprócz jednej linii, zatrzymują się lub kończą bieg na dworcu Atocha – centralnej, węzłowej stacji kolejowej w stolicy Hiszpanii. W Alcalá de Henares znajdują się trzy linie Cercanias. Jedna biegnie z Guadalajary, a dwie pozostałe mają tu swój początek. W godzinach porannego szczytu zatłoczone pociągi w kierunku Madrytu odjeżdżają stąd co pięć minut²⁷.

Furgonetkę zaparkowano niedaleko dworca. Mieszkający w pobliżu dozorca Luis Garrudo zauważył, że wysiadły z niej trzy osoby. Zostały one sfilmowane przez kamery monitoringu wraz z czterema pozostałymi, gdy wchodziły i wychodziły z pociągów stojących na peronach. Sprawcy ulokowali ładunki wybuchowe w czterech pociągach. Składy pełne pasażerów odjeżdżały z Alcalá de Henares do Madrytu między godz. 7.01 a 7.14²⁸.

²⁶ F. Reinares, *Al-Qaeda's Revenge...*, s. 71–74; Z. Jakubowska, *Madryt 11 marca...*, s. 127–129.

²⁷ Opracowano na podstawie szczytkowych informacji. Zob. Z. Jakubowska, *Madryt 11 marca...*, s. 56–57, 74, 129, 207–208, 212–214.

²⁸ A. Martin Plaza, *Los atentados del 11M que sacudieron España...*; *Atentados Terroristas del Dia 11 del Marzo de 2004 de Madrid*, Juzgado Central de Instrucción N° 6 Audiencia Nacional Madrid, <https://e00-elmundo.uecdn.es/documentos/2006/04/11/auto11m/01.pdf>, s. 1 [dostęp: 11 IV 2006]; Z. Jakubowska, *Madryt 11 marca...*, s. 55–56.

Dworzec Atocha, skład nr 21431

Pociąg zatrzymał się na peronie nr 2. Wielu pasażerów opuściło skład i zaczęli do niego wsiadać ludzie, którzy chcieli jechać w kierunku Alcobendas, 13 km na północ od Madrytu. O godz. 7.37 (według innych źródeł o godz. 7.39)²⁹ eksplodowała pierwsza bomba, a dwie kolejne wybuchły w odstępie czterech sekund. Eksplozje nastąpiły w wagonach nr 4, 5 i 6³⁰. Zginęło 29 pasażerów, a 115 zostało rannych. Siła wybuchu została w pewnym sensie ograniczona w wyniku otwartych drzwi pociągu, ale eksplozja bomb umieszczonych w koszach po prawej stronie spowodowała, że fala uderzeniowa rozeszła się po peronie, na którym znajdowało się dużo pasażerów. Zapanował wśród nich chaos. Ich celem było wydostanie się ze szczątków pociągu. Ludzie wpadali na siebie, starając się dobiec do ruchomych schodów, co nie było łatwe, biorąc pod uwagę, że o tej godzinie dworzec Atocha przypominał stację w tokijskim metrze. W momencie gdy eksplodowały bomby, do dworca Atocha zbliżał się drugi pociąg³¹.

Dworzec Atocha, ulica Téllez, skład nr 17305

Pociąg, który z Atochy miał jechać do stacji Chamartin, był nieco spóźniony. Skład zwalniał, aby zatrzymać się na wysokości ulicy Téllez, biegnącej równoległe do torowiska, ok. 800 m od Atochy³². Tu miał oczekiwać na odjazd składu nr 17393. O godz. 7.39 wybuchły cztery bomby w wagonach: 1, 4, 5 i 6³³. Siła eksplozji była tak duża, że wielu z 65 zabitych zostało wyrzuconych na zewnątrz. Gdyby nie opóźnienie pociągu, ofiar mogło być znacznie więcej. Rannych zostało 165 osób. Według świadków zdarzenia najbardziej zaskakujące były cisza i spokój, z jakimi ranni pasażerowie, niektórzy w bardzo ciężkim stanie, wysiadali ze zniszczonych wagonów, pomagając sobie wzajemnie, jeszcze bez wsparcia służb medycznych. Zgłoszenie o wybuchu na dworcu Atocha pogotowiu ratunkowe otrzymało bezpośrednio

²⁹ W publikacjach jest podawany różny czas eksplozji pierwszej bomby w pociągu na dworcu Atocha, np. godz. 7.37, 7.38 lub 7.39. Rozbieżności dotyczą także czasu eksplozji w pozostałych pociągach, przy czym wszystkie miały nastąpić w odstępie od trzech do pięciu minut, a nie jak podano na grafikach (rysunek 1, rysunek 2). Zob. *The Terror Attacks in Madrid...*, s. 28–30 [dostęp: 11 III 2008]; F. Reinares, *Al-Qaeda's Revenge...*, s. xxiii.

³⁰ Zob. F. Reinares, *Al-Qaeda's Revenge...*, s. xxiii.

³¹ *The Terror Attacks in Madrid...*, s. 27.

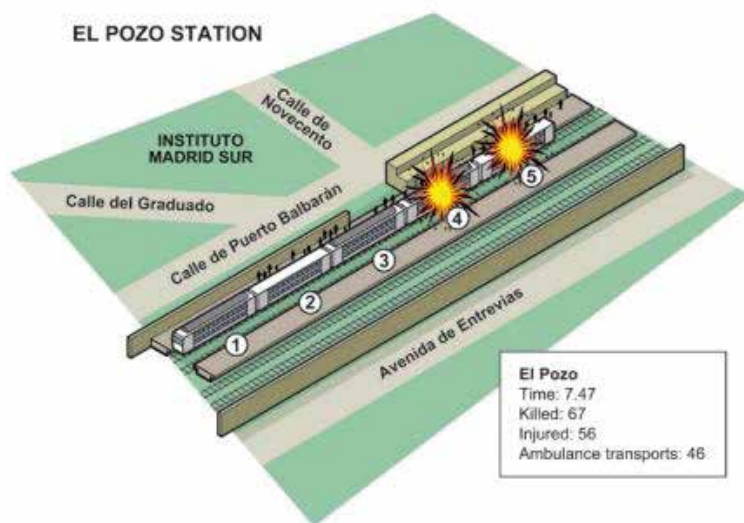
³² Zob. *Atentados Terroristas del Día 11 del Marzo de 2004 de Madrid...*; F. Reinares, *Al-Qaeda's Revenge...*, s. xxiii; Z. Jakubowska, *Madryt 11 marca...*, s. 57, 205.

³³ Zob. F. Reinares, *Al-Qaeda's Revenge...*, s. xxiii.

po eksplozji. Osiem minut później przyjechała pierwsza karetka. Na dworzec Atocha wysłano ich najwięcej³⁴.

Dworzec El Pozo del Tio Raimundo, skład nr 21435

Na dworzec przyjechał przepełniony pociąg piętrowy z Guadalajary przez Alcalá de Henares (rysunek 1). Wysiedli z niego studenci i uczniowie, a wsiedli pracownicy, w tym wielu rodziców, którzy o tej porze pozostawiali dzieci w pobliskich przedszkolach. O godz. 7.38 (7.40) skład ruszył do odległego o trzy przystanki dworca Alcobendas. Nie minął jeszcze peronu, gdy w dwóch wagonach nr 4 i 5 doszło do potężnych eksplozji, w wyniku których zginęło 67 osób, a 56 – głównie znajdujących się na peronie – zostało rannych. Atak na dworcu El Pozo był trzecim z kolei, co oznaczało, że mobilizacja i skierowanie służb zajmie więcej czasu. Pierwsze zgłoszenie zarejestrowano o godz. 7.47, a 15 minut później przyjechała karetka pogotowia. W ciągu 1 godz. i 10 minut wszystkich rannych przewieziono do szpitali³⁵.



Rysunek 1. Skład nr 21435 na dworcu El Pozo del Tio Raimundo.

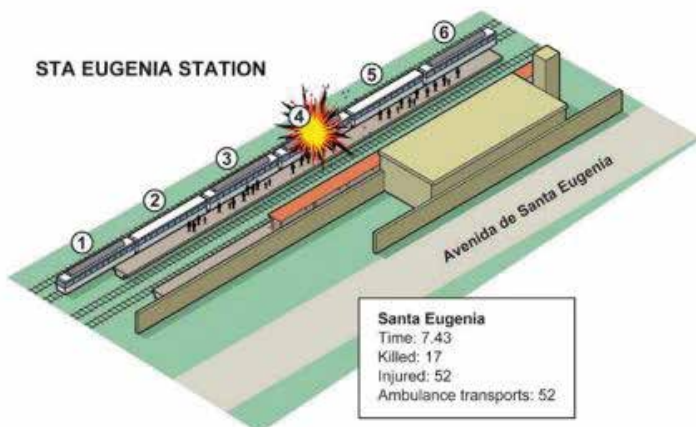
Źródło: *The Terror Attacks in Madrid, Spain, 2004, Kamedo-report 90*, Socialstyrelsen 2007, https://www.socialstyrelsen.se/globalassets/sharepoint-dokument/artikelkatalog/ovrigt/2007-12336_200712336.pdf, s. 30 [dostęp: 11 III 2008].

³⁴ *The Terror Attacks in Madrid...*, s. 30.

³⁵ Tamże, s. 29.

Dworzec Santa Eugenia, skład nr 21713

O godz. 7.40 (7.42) nastąpiła ostatnia z serii eksplozji (rysunek 2)³⁶. Stało się to w momencie, gdy pociąg ruszał z dworca. Wybuch materiału umieszczonego w torbie podróźnej spowodował olbrzymie spustoszenie. Zginęło 17 osób, a 52 zostały ranne. Szczątki ludzkie były rozrzucone w promieniu 50 metrów. Poważnym uszkodzeniom uległy budynki stacji³⁷.



Rysunek 2. Skład nr 21713 na dworcu Santa Eugenia.

Źródło: *The Terror Attacks in Madrid, Spain, 2004, Kamedo-report 90*, Socialstyrelsen 2007, https://www.socialstyrelsen.se/globalassets/sharepoint-dokument/artikkelkatalog/ovrigt/2007-12336_200712336.pdf, s. 29 [dostęp: 11 III 2008].

Natychmiast po atakach w Madrycie zmobilizowano wszystkie siły. W miejscach katastrofy powstały szpitale polowe, służby medyczne zapelowały o oddawanie krwi, ponieważ zapasy kończyły się w szybkim tempie. Przed mobilnymi punktami krwiodawstwa ustawiały się tłumy ludzi. Równoległe z akcją ratunkową rozpoczęło się śledztwo i operacja antyterrorystyczna pod kryptonimem „Klatka” („Jaula”), której celem było uniemożliwienie terrorystom ucieczki z miasta. Stolicę ogarnął paraliż komunikacyjny. O godz. 10.00 prawie wszyscy ranni zostali przewiezieni do ok. 20 szpitali. Ponad 300 osób trafiło do szpitala Gregorio Marañón,

³⁶ Eksplozję w pociągu na dworcu Santa Eugenia wymienia się w *The Terror Attacks in Madrid, Spain, 2004, Kamedo-report 90* jako drugą w kolejności, tymczasem nastąpiła ona równocześnie z wybuchem w pociągu na dworcu El Pozo lub jako ostatnia.

³⁷ Tamże, s. 28.

który wcześniej nie był tak obciążony. Nigdy też nie ćwiczone awaryjnego planu działania na wypadek wielkich katastrof, a sytuacja z rana 11 marca 2004 r. wręcz przypominała wojnę³⁸. Policja zwlekała z publikacją nazwisk zabitych. Tragiczny bilans został w końcu podany do publicznej wiadomości. W czterech pociągach jechało ponad 6000 ludzi. W wyniku ataków zginęły 192 osoby, a ponad 1400 zostało rannych³⁹. Wśród ofiar z 16 państw było czworo Polaków: dwie kobiety, mężczyzna i jego siedmiomiesięczna córka, którzy dzień po atakach zmarli w szpitalu⁴⁰. Następnie uaktualniono statystykę rannych, których ostateczna liczba wyniosła 1858⁴¹. Był to drugi pod względem liczby ofiar śmiertelnych atak terrorystyczny w Europie po zamachu na samolot linii Pan American nad Lockerbie w Szkocji z 21 grudnia 1988 r. Zginęło w nim 259 pasażerów i członków załogi oraz 11 mieszkańców tego miasta.

W śledztwie prowadzonym przez policję odkryto, że plecaków podłożonych w pociągach było więcej. Z trzynastu wybuchło dziesięć bomb. Jedną z nich znaleziono w pociągu na dworcu Atocha, a drugą w składzie na dworcu El Pozo del Tio Raimundo. Obydwie zostały zdetonowane przez saperów z Regionalnej Brygady Operacyjno-Rozpoznawczej (Técnico Especialista en Desactivación de Artefactos Explosivos, TEDAX). Trzeci ładunek wybuchowy odkryto wśród bagaży wyniesionych z pociągu w El Pozo, gdy w jednym z plecaków zadzwonił telefon komórkowy. Specjaliści rozbili tę bombę. Składała się z materiału wybuchowego typu goma-2 eco, śrub i gwoździ mających zwiększyć siłę rażenia, dwóch detonatorów i wspomnianego telefonu na kartę z alarmem zaprogramowanym na godzinę, o której miał nastąpić wybuch. Nie doszło do niego z powodu wady zapalnika. Ustalono, że karta pochodziła ze sklepu należącego do Zugama. Ujawnione połączenia pozwoliły zidentyfikować wielu terrorystów⁴². W dniu

³⁸ Z. Jakubowska, *Madryt 11 marca...*, s. 64.

³⁹ Ostatnia ranna osoba zmarła w 2014 r. po dziesięciu latach pozostawania w śpiączce. Liczba wszystkich ofiar śmiertelnych wyniosła zatem 193 osoby. Zob. B. Cedeira, *La víctima que entró en coma el 11M hasta morir 10 años después*, *El Español*, 11 III 2017 r., https://www.elespanol.com/reportajes/20170310/199730525_0.html [dostęp: 11 III 2017].

⁴⁰ *Zmarła czwórka Polaków rannych w Madrycie*, *Gazeta Wyborcza*, 12 III 2004 r., <https://web.archive.org/web/20091214225052/http://wyborcza.pl/1,75248,1961962.html> [dostęp: 12 III 2004].

⁴¹ *Zamachy w Madrycie – odwet za Irak*, *Polskie Radio*, 11 III 2014 r., <https://www.polskieradio.pl/106/246/Artykul/1071933%2CZamachy-w-Madrycie---odwet-za-Irak> [dostęp: 11 III 2014].

⁴² A. Martin Plaza, *Los atentados del 11M que sacudieron España...*

zamachu mieszkańcy Alcalá de Henares poinformowali policję o podejrzanej furgonetce zaparkowanej w pobliżu dworca. Została ona odholowana na policyjny parking. Funkcjonariusze znaleźli w niej m.in. siedem detonatorów, resztki materiału wybuchowego i kasetę magnetofonową z nagraniem recytacją fragmentu Koranu, koc, szalik i rękawice⁴³.

Politycy rządzącej partii chwilę po zamachach oskarżyli o ich przeprowadzenie baskijską organizację ETA, która rzekomo chciała wpłynąć na przebieg wyborów. Premier Aznar powiedział: *ETA stoi za tymi zamachami*⁴⁴. Wtórował mu minister spraw wewnętrznych Ángel Acebes, który stwierdził: *Nie ma wątpliwości, że odpowiedzialność ponosi ETA*. W przemówieniu telewizyjnym o godz. 14.30 Aznar stanowczo oskarżył organizację o przeprowadzenie ataków. Zapowiedział również zorganizowanie następnego dnia manifestacji przeciwko baskijskim separatystom. Także inni politycy PP bez jakichkolwiek wątpliwości wskazywali na ETA jako sprawcę ataków. Takie same sygnały płynęły początkowo od służb specjalnych, mimo że organizacja odrzucała te oskarżenia⁴⁵. Wieczorem Brygada Abu Hafs al-Masri wysłała do arabskojęzycznego dziennika „Al-Quds al-Arabi” („Arabska Jerozolima”) wydawanego w Londynie e-mail, w którym przyznała się do dokonania zamachów⁴⁶. W tym samym czasie policja odnalazła we wskazanym przez tę brygadę miejscu kasetę video. Nagrano na niej przedstawiciela Al-Kaidy w Europie, Abu Dudżana al-Afghaniego, który w imieniu organizacji przyznał się do zamachów dokonanych dokładnie dwa i pół roku po 11 września, w odpowiedzi na współpracę Hiszpanii z „kryminalistą Bushem”. Miał to być odwet za zło wyrządzane w świecie przez Zachód, zwłaszcza w Iraku i Afganistanie⁴⁷.

⁴³ *Atentados Terroristas del Dia 11 del Marzo de 2004 de Madrid...*, s. 147–149.

⁴⁴ M. Catalán, *Prensa, verdad y terrorismo: la lección política del 14-M*, „El Argonauta Español” 2005, nr 2. <https://doi.org/10.4000/argonauta.1191> [dostęp: 26 VIII 2023].

⁴⁵ Tamże.

⁴⁶ Nazwa organizacji pochodzi od Muhammada Atefa alias Abu Hafs al-Masri, jednego z najbliższych współpracowników Bin Ladena i działacza Egipskiego Islamskiego Dżihadu (Al-Dżihad al-Islami al-Misri). Brygada dała znać o sobie ponownie 17 marca 2004 r., deklarując zawieszenie broni w Hiszpanii, jeśli nowy rząd spełni swą obietnicę i wycofa wojska z Iraku. Przy okazji nazwała Aznara „ogonem Stanów Zjednoczonych”, który został „wyrzucony na śmietnik historii”. Ta sama organizacja wzięła odpowiedzialność za zamachy w Stambule w listopadzie 2003 r. i Londynie w lipcu 2005 r. Publikowała również dziesiątki odezw, oświadczeń i komunikatów. Okazało się jednak, że brygada istniała jedynie w sferze wirtualnej. Zob. K. Izak, *Leksykon organizacji i ruchów islamistycznych...*, s. 413.

⁴⁷ Z. Jakubowska, *Madryt 11 marca...*, s. 82.

W sobotę 13 marca aresztowano trzech współwłaścicieli sklepu z telefonami Nuevo Siglo, z którego pochodziły komórki przerobione na zapalniki. Agentom wywiadu udało się też zlokalizować kryjówkę terrorystów w wynajętym mieszkaniu w dzielnicy Leganés. Pomogły w tym karty z telefonów komórkowych i karta przedpłacona znaleziona 2 kwietnia w torbie z materiałem wybuchowym, umieszczonej na torach kolei dużych prędkości (Alta Velocidad Española, AVE). Następnego dnia policjanci i funkcjonariusze Grupy Operacji Specjalnych (Grupo Especial de Operaciones, GEO) przystąpili do oblężenia budynku, w którym znajdowała się kwatera terrorystów. Początek operacji i sprzeczne informacje na temat jej przebiegu wzbudziły wiele kontrowersji. Około godz. 18.00 jeden z terrorystów wyszedł na zewnątrz, aby wyrzucić śmieci. Zobaczył policjantów, po czym ostrzegł kolegów i uciekł⁴⁸. Według innej wersji wydarzeń uciekł bez ostrzeżenia towarzyszy, którzy sami zobaczyli policjantów w pobliżu⁴⁹. Wtedy przez okno terroryści otworzyli ogień, wznosząc po hiszpańsku okrzyki na cześć Allaha. Po ewakuacji mieszkańców zdecydowano, że grupa funkcjonariuszy GEO wysadzi drzwi do mieszkania i wpuści do środka gaz łzawiący. Gdy antyterroryści znaleźli się na klatce schodowej obok mieszkania, w drzwiach wejściowych stanął nagi mężczyzna. W tym momencie doszło do potężnej eksplozji, w wyniku której zginął jeden funkcjonariusz, a 15 innych zostało rannych, kilku ciężko. Duża część fasady budynku została zniszczona. Siła eksplozji materiałów wybuchowych zgromadzonych w mieszkaniu była tak wielka, że nie można było doliczyć liczby zmasakrowanych ciał terrorystów, którzy popełnili zbiorowe samobójstwo. Najpierw poinformowano, że zginęło ich czterech. Dopiero po trzech dniach ustalono, że było ich siedmiu⁵⁰. Byli to ci sami terroryści, którzy podkładali bomby w pociągach na dworcu w Alcalá de Henares.

⁴⁸ Tamże, s. 130.

⁴⁹ *Los terroristas del 11-M se inmolan y matan a un geo al volar su «piso franco» en Leganés*, ABC España, 4 IV 2004 r., https://www.abc.es/espana/abci-terroristas-inmolan-y-matan-volar-piso-franco-leganes-200404040300-962802830594_noticia.html [dostęp: 4 IV 2004].

⁵⁰ Z. Jakubowska, *Madryt 11 marca...*, s. 82; R. Becares, O. Cernuda, *Cuatro terroristas islámicos se inmolan en un piso de Leganés y matan a un agente de policía*, elmundo.es, 4 IV 2004 r., <https://www.elmundo.es/elmundo/2004/04/03/enespecial/1081016920.html> [dostęp: 4 IV 2004]; *La policía eleva a siete los terroristas muertos en Leganés*, Cadenaser, 7 IV 2004 r., https://cadenaser.com/ser/2004/04/07/espana/1081295423_850215.html [dostęp: 7 IV 2004].

Polityczne skutki wydarzeń z 11 marca 2004 roku

Do zamachów w Madrycie doszło trzy dni przed wyborami parlamentarnymi. W przypadku gdyby to ETA faktycznie przeprowadziła ataki, wyborcy z pewnością poparliby partię Aznara, który realizował politykę twardego postępowania z baskijskimi terrorystami i odrzucił wszelkie możliwości negocjacji z nimi. Przy czym Aznar już wcześniej zadeklarował, że nie będzie ubiegał się o ponowny wybór na premiera, w związku z tym PP na swojego lidera w kampanii wyborczej wybrała Mariano Rajoya. Gdyby jednak ataki w Madrycie przeprowadzili islamscy ekstremiści, sytuacja mogłaby się diametralnie zmienić, ponieważ 80% społeczeństwa było przeciwne wysłaniu hiszpańskich żołnierzy do Iraku. Z pewnością politycy PSOE wykorzystaliby ten fakt do zdyskredytowania ówczesnego rządu. Z tego względu Aznar i Acebes cały czas oskarżali ETA o przeprowadzenie ataków, mimo że fakty ujawniane w kolejnych godzinach temu przeczyły. Analiza dowodów rzeczowych badanych przez ekspertów kryminalistyki wymuszała przynajmniej zachowanie powściągliwości w wypowiedziach ludowców. Tymczasem 11 marca ok. godz. 21.30 Zapatero zatelefonował do redaktora naczelnego dziennika „El Mundo” i poinformował go, że w świetle nowych dowodów jest przekonany o winie Al-Kaidy, a co więcej – według jego opinii – rząd również ma tę wiedzę. Gdy następnego dnia opozycja kwestionowała słowa członków prawicowego rządu, głos zabrali przedstawiciele ETA. Do redakcji skrajnie nacjonalistycznego dziennika „Gara” zadzwonił anonimowy rozmówca i oświadczył, że baskijska organizacja nie ponosi żadnej odpowiedzialności za czwartkowe zamachy. Kilkanaście minut później Acebes w imieniu rządu ogłosił, że nie wierzy w autentyczność tej informacji. W piątek wieczorem ok. 11 mln Hiszpanów, w tym ok. 2,3 mln w samym Madrycie, wzięło udział w demonstracjach przeciwko przemocy ETA, a także jako wyraz upamiętnienia ofiar oraz wsparcia dla ich rodzin. Pokaz tej jedności został zakłócony, gdy śledztwo policyjne zaczęło koncentrować się na Al-Kaidzie. W sobotę 13 marca, kiedy nastąpiły pierwsze aresztowania islamskich radykałów związanych z zamachem, rzecznik rządu i minister spraw wewnętrznych nadal obwiniali ETA. W związku ze sprzecznościami między pojawiającymi się nowymi dowodami z wypowiedziami przedstawicieli władz opozycja zdecydowała się działać mimo obowiązującej ciszy wyborczej. Przedwyborczy zakaz agitacji został złamany okrzykami tłumu, który zebrał się przy siedzibie PP w Madrycie. Mieszkańcy domagali się poznania prawdy, zanim wezmą udział w wyborach. Antyrządowe protesty wybuchły także w Barcelonie i innych dużych

miastach Hiszpanii. Tego samego wieczora i w nocy toczyła się walka na słowa między PP i PSOE, która oskarżyła rząd o kłamstwa w trakcie trwającego śledztwa⁵¹.

W dniu 14 marca zwyciężyła lewica, zdobywając 11 mln głosów, PP zaś 9,7 mln. Frekwencja w wyborach parlamentarnych wyniosła 77,26% i była jedną z najwyższych w Hiszpanii⁵². Następnego dnia, po ogłoszeniu zwycięstwa socjalistów, Zapatero poinformował, że zamierza zaprosić pozostałe partie polityczne do dialogu na temat walki z terroryzmem. Zapowiedział też powrót do sojuszu z Francją i Niemcami, czyli prowadzenia polityki proeuropejskiej zamiast proamerykańskiej poprzedniego rządu. Oznajmił, że jego pierwszym krokiem będzie wycofanie wojsk z Iraku. Wojnę z reżimem Husajna nazwał błędem, ponieważ w Iraku nie znaleziono żadnej broni masowego rażenia. Okazało się ponadto, że w USA i Wielkiej Brytanii manipulowano raportami służb specjalnych, by uwiarygodnić konieczność interwencji. Nowy premier Hiszpanii stwierdził również, że jego zwycięstwo w głosowaniu jest sygnałem zmian dla innych krajów, w których wkrótce odbędą się wybory, włączając w to Stany Zjednoczone, gdzie w listopadzie prezydent George W. Bush miał zmierzyć się z senatorem z Massachusetts Johnem Kerryem. Jeżeli wyborcy nie zaakceptują wojny w Iraku i jego okupacji, mogą wyrazić swój protest w sondażach i przy urnach, zmieniając w ten sposób kierunek polityki. Ostateczną decyzję o wycofaniu hiszpańskiego kontyngentu podjęto 19 kwietnia 2004 r.⁵³

W maju 2004 r. 1300 hiszpańskich żołnierzy opuściło Irak⁵⁴. Do kraju wrócili także żołnierze stacjonujący na Dominikanie i w Hondurasie. Latem tego samego roku MND C-S licząca 9000 żołnierzy dowodzonych przez Polaków zmniejszyła się do ok. 7000. Ich obecność w Iraku nie miała istotnego znaczenia militarnego, ale zakończenie misji zostało odebrane jako gest o charakterze politycznym, będący konsekwencją reorientacji stanowiska Hiszpanii, w którym nowy rząd wyraźnie dystansował się od taktyki wojny

⁵¹ J. Cieszko, *Tragedia w Madrycie, 11–14 marca 2004 roku*, w: *Hiszpania: Media masowe i wybory w obliczu terroryzmu*, B. Dobek-Ostrowska, M. Kuś (red.), Wrocław 2007, s. 51–54; J.L. Gonzalez Esteban, *Kronika 11 marca: terroryzm i polityczna zmiana w Hiszpanii*, w: *Hiszpania: Media masowe i wybory...*, s. 67–70.

⁵² J. Cieszko, *Tragedia w Madrycie...*, s. 56–57.

⁵³ A. Martin Plaza, *Los atentados del 11M que sacudieron España...*; J. Cieszko, *Tragedia w Madrycie...*, s. 54–55.

⁵⁴ M. Brylew, *Irak 2006–2012...*, s. 50.

z terroryzmem głoszonej przez USA⁵⁵. Międzynarodowe media donosiły wówczas, że Hiszpanie zawiedli. Polskie Ministerstwo Obrony Narodowej miało nadzieję, że Hiszpanie przejmą dowodzenie w strefie za którą odpowiadała dywizja MND C-S. Ówczesny premier Polski, Leszek Miller, apelował do Hiszpanów o lojalność wobec międzynarodowej koalicji antyterrorystycznej, jednak bezskutecznie⁵⁶. Stanowisko nowego rządu hiszpańskiego spotkało się z ostrą krytyką Waszyngtonu i innych stolic. Administracja Busha nie ukrywała swojego gniewu na Zapaterę, porównując obecną sytuację z podpisaniem układu monachijskiego w 1938 r. Wówczas dla uspokojenia sytuacji Francja i Wielka Brytania zgodziły się na przyłączenie części terytorium Czechosłowacji do Niemiec. W podobny sposób w 2004 r. postąpiła Hiszpania, która chcąc „uspokoić” terrorystów, wycofała z Iraku swój kontyngent wojskowy. W polskich mediach pojawiały się złośliwe komentarze, że wybory w Hiszpanii wygrała Al-Kaida⁵⁷. Wydarzenia z 11 marca oraz ich konsekwencje miały wpływ zarówno na ogólne stosunki międzynarodowe, jak i dwustronne między Hiszpanią i Stanami Zjednoczonymi. Zmiana rządu w Hiszpanii nie spotkała się z przychylnym przyjęciem administracji Busha. W trakcie wizyty w państwach UE ówczesna przewodnicząca Narodowego Komitetu Bezpieczeństwa USA, Condoleezza Rice, zignorowała Madryt. Nie zatrzymała się tam, uznając, że nie usłyszy w Madrycie nic z tego, czego nie mogłaby usłyszeć w Paryżu. Zamachy w stolicy Hiszpanii wykorzystał prezydent Bush w trakcie kampanii wyborczej w 2004 r. Uzasadniał nimi konieczność kontynuowania polityki militarnej w Iraku oraz utrzymania ograniczenia swobód obywatelskich mieszkańców USA. Wskazywał

⁵⁵ Kontyngent hiszpański pozostał natomiast w Afganistanie. Zapatero wyrażał bowiem przekonanie, że obydwie te interwencje zasadniczo różniły się pod względem przesłanek i legalności.

⁵⁶ *Po pięciu latach koniec polskiej misji w Iraku*, money.pl, 29 X 2008 r., https://www.money.pl/archiwum/wiadomosci_agencyjne/pap/arttykul/po;pieciu;latach;koniec;polskiej;misji;w;iraku,188,0,381372.html [dostęp: 29 X 2008]. Jesienią 2014 r. hiszpańskie Ministerstwo Obrony podjęło decyzję o wysłaniu do Iraku 300 żołnierzy. Tym razem wspierali oni międzynarodową koalicję w walce z Państwem Islamskim. Szkolili irackie wojsko w przeprowadzaniu akcji specjalnych oraz w wykrywaniu i rozbrajaniu min. Hiszpanie nie brali czynnego udziału w walkach, ale musieli stawiać opór w przypadku ataków. Zob. *Hiszpański parlament zgodził się na wysłanie żołnierzy do Iraku*, Wirtualna Polska, 22 X 2014 r., <https://wiadomosci.wp.pl/hiszpanski-parlament-zgodzil-sie-na-wyslanie-zolnierzy-do-iraku-6027730872366209a> [dostęp: 22 X 2014].

⁵⁷ B. Łódzki, *Reakcja polskich mediów masowych na atak terrorystyczny w Madrycie 11 marca 2004 r.*, w: *Hiszpania: Media masowe i wybory w obliczu terroryzmu*, B. Dobek-Ostrowska, M. Kuś (red.), Wrocław 2007, s. 126.

ponadto, że terroryzm to rzeczywiście największe zagrożenie dla świata, a więc kontynuowanie tej polityki jest priorytetem w jego polityce zagranicznej⁵⁸. Innym skutkiem wydarzeń w Madrycie mającym międzynarodowe znaczenie było przyjęcie przez Radę Europejską w marcu 2004 r. deklaracji w sprawie zwalczania terroryzmu. Dwa miesiące później utworzono stanowisko koordynatora UE ds. zwalczania terroryzmu.

Skazanie sprawców ataków w Madrycie

W dniu 14 marca 2005 r. Al-Kaida przyznała się do ataków w Madrycie. Mówca przedstawiający się jako rzecznik tej organizacji w Europie oświadczył, że zamachy były zemstą za (...) *współpracę Hiszpanii z kryminalistą Bushem i jego sojusznikami*⁵⁹. Informacja ta nie wywołała większej reakcji społecznej, ponieważ śledztwo i tak wykazało, że za ataki odpowiedzialna była organizacja Bin Ladena. Polityczna i społeczna debata związana z wydarzeniami w Madrycie powróciła w 2007 r. w związku z kontrowersyjnymi wyrokami wydanymi na organizatorów i pomocników ataku terrorystycznego. W jego przygotowanie i realizację bezpośrednio było zaangażowanych 29 osób, w większości Marokańczyków. Proces trwał od 15 lutego do 2 lipca 2007 r. Przed sądem stanęło 15 Marokańczyków, dziewięciu Hiszpanów, dwóch Syryjczyków, Algierczyk, Libańczyk i Egipcjanin. Wyrok odczytano 31 października 2007 r. – 21 z 29 oskarżonych o udział w zamachach, z których żaden nie przyznał się do winy, zostało skazanych na ponad 40 000 lat pozbawienia wolności. Ośmiu sąd uniewinnił. W tej samej sprawie wymienia się też 28 oskarżonych, z których siedmiu uniewinniono. Wśród nich znajdował się Al-Masri, uznawany przez niektórych autorów za inicjatora zamachów w Madrycie. W 2004 r. został zatrzymany w Mediolanie po tym, jak policja podsłuchiwała jego rozmowę, w której przyznał się do zaplanowania ataków. Uniewinniono też Muhammada Egipcjanina, co pokretnie tłumaczono tym, że odbywa on już we Włoszech karę 10 lat więzienia (zredukowaną do 8) za przynależność do organizacji

⁵⁸ T. Płudowski, *Reakcje prasy amerykańskiej na madrycki atak terrorystyczny z 11 marca 2004 r.*, w: *Hiszpania: Media masowe i wybory w obliczu terroryzmu*, B. Dobek-Ostrowska, M. Kuś (red.), Wrocław 2007, s. 156–157.

⁵⁹ A. Mroczek, *Zamach w Madrycie 11 III 2004 – minuta po minucie*, terroryzm.com, 25 IX 2005 r., <http://www.terroryzm.com/zamach-w-madrycie-11-iii-2004-minuta-po-minucie/> [dostęp: 25 IX 2005].

terrorystycznej. Inny organizator ataków, Al-Haski, będący również szefem hiszpańskiej komórki Marokańskiej Islamskiej Grupy Walczącej, został skazany na 15 lat pozbawienia wolności zamiast ponad 40 000, czego domagał się prokurator. Najcięższe kary otrzymali Zugam i Al-Ghanut: po 30 lat za każdego ze 191 zabitych, po 20 lat za każdego z 1858 rannych (próba zabójstwa) i po 12 lat za przynależność do organizacji terrorystycznej. Wśród skazanych znalazł się również Trashorras, któremu zarzucono współudział w wydarzeniach poprzez sprzedaż materiałów wybuchowych islamskim terrorystom. Jego wyrok to 34 715 lat więzienia. Jednak zgodnie z hiszpańskim systemem prawnym żaden ze skazanych w więzieniu nie będzie przebywał dłużej niż 40 lat. Pozostali oskarżeni otrzymali wyroki od 3 do 23 lat pozbawienia wolności. Prokuratura oraz stowarzyszenia skupiające bliskich ofiar odwołały się od wyroków do Sądu Najwyższego, który w sentencji z 17 lipca 2008 r. podtrzymał większość z nich. Społeczeństwo, a przede wszystkim rodziny ofiar zamachów, przyjęły wyroki, zwłaszcza te najniższe i uniewinniające, z niedowierzaniem, oburzeniem i złością⁶⁰. Hiszpanom trudno było pogodzić się z tym, że masakry dokonali muzułmanie, którzy mieszkali w Madrycie, pracowali tu i często przyjaźnili się z miejscową społecznością. Politycy rządzącej PSOE raczej nie komentowali wyroku. Wciąż natomiast oskarżali poprzedni prawicowy rząd, że próbował ukryć prawdę o rzeczywistych sprawcach ataków i zrzucić winę na ETA, by Hiszpanie nie pomyśleli, że był on odwetem za wysłanie hiszpańskich wojsk do Iraku⁶¹.

Problemy z bezpieczeństwem antyterrorystycznym w Hiszpanii

Wraz z wynikami toczącego się śledztwa nasuwały się pytania i wątpliwości dotyczące nie tylko sprawców ataków, lecz także stanu bezpieczeństwa antyterrorystycznego w Hiszpanii. W kraju, w którym w latach 1960–2011 walczono z terroryzmem separatystów baskijskich, doszło do zamachu motywowanego dżihadystyczną ideologią. Z jednej strony

⁶⁰ M. Tryc-Ostrowska, *Kontrowersyjny wyrok za zamachy w Madrycie*, „Rzeczpospolita”, 2 XI 2007 r.

⁶¹ C. Taracha, *Wybory w cieniu zamachu. Kilka uwag na temat wydarzeń z marca 2004 roku w Madrycie*, w: *Terroryzm wczoraj i dziś. Wybrane problemy*, P. de la Fuente, W. Gizicki, C. Taracha (red.), Lublin 2015, s. 80; *El final del principio en la investigación del 11-M*, elmundo.es, 1 XI 2007 r., <https://www.elmundo.es/elmundo/2007/11/01/espana/1193885319.html> [dostęp: 1 XI 2007]; M. Tryc-Ostrowska, *Kontrowersyjny wyrok...*

wyrażano uznanie dla sprawności i profesjonalizmu służb ratownictwa medycznego oraz ekspertów kryminalistyki i medycyny sądowej. Z drugiej strony śledztwo ujawniło wiele błędów i zaniedbań związanych z inwigilacją najbardziej zradykalizowanych osób oraz postępowaniem policji i Gwardii Obywatelskiej wobec informatorów. W grupie osób związanych z atakiem znajdowało się aż pięciu informatorów tych służb. Policja odrzuciła np. informacje przekazane przez jednego z nich, że to nie ETA przeprowadziła atak, ponieważ były one sprzeczne z linią polityczną⁶². Także proces sądowy pozostawił wiele pytań i wątpliwości zarówno co do autorstwa zamachu, jak i jego sprawców i pomysłodawców. Nic więc dziwnego, że ten gorący temat stał się przedmiotem rozważań o charakterze naukowym i publicystycznym. Do opinii publicznej docierały różne interpretacje i spekulacje dotyczące wydarzeń z 11 marca 2004 r. Autorem oficjalnej koncepcji przyjmowanej przez rządzący Hiszpanią establishment polityczny i znaczną część społeczeństwa jest Reinares. Przyjęła się również opinia Luisa del Piny, który w zamachach dopatrywał się śladów obecności służb specjalnych, nie wskazując ich konkretnie⁶³.

W celu zwiększenia skuteczności w walce z krajowym i międzynarodowym terroryzmem dwa miesiące po zamachach utworzono w Hiszpanii Narodowe Centrum Koordynacji Antyterrorystycznej (Centro Nacional de Coordinación Antiterrorista, CNCA). W Polsce jego odpowiednikiem jest Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego. W skład CNCA weszli najlepsi funkcjonariusze Krajowego Korpusu Policji (Cuerpo Nacional de Policía, CNP), Gwardii Obywatelskiej, CNI i zakładów karnych. Narodowe Centrum Koordynacji Antyterrorystycznej podlegało Sekretarzowi Stanu ds. Bezpieczeństwa w Ministerstwie Spraw Wewnętrznych (Ministerio del Interior). W departamentach zajmujących się terroryzmem islamskim i radykalizmem muzułmańskim znalazło się wielu specjalistów. Była to instytucja o charakterze analitycznym. Jej podstawowym celem było przyjmowanie, przetwarzanie i ocena dostępnych informacji strategicznych na temat wszystkich rodzajów terroryzmu stanowiących zagrożenie dla Hiszpanii, bez podejmowania działań operacyjnych, które znajdowały się w gestii Sił i Organów Bezpieczeństwa Państwa (Fuerzas y Cuerpos de Seguridad del Estado, FCSE). W skład FCSE wchodziły: wywiad, policja, Gwardia Obywatelska oraz katalońska policja Mossos d'Esquadra.

⁶² Z. Jakubowska, *Madryt 11 marca...*, s. 173–175.

⁶³ C. Taracha, *Wybory w cieniu zamachu...*, s. 81–85.

Nowa instytucja do walki z terroryzmem stale aktualizowała ocenę zagrożenia terrorystycznego, starała się utrzymać inicjatywę w walce z terrorystami, wybierać najlepsze scenariusze ewentualnej interwencji i planować reakcję. Wprowadzono zmiany legislacyjne. Zainicjowano modyfikację i rozbudowę systemu prewencji terrorystycznej, obejmujące m.in. usprawnienie sił szybkiego reagowania i wykorzystanie wojska. Zacieśniono współpracę wywiadowczą w ramach UE z USA i państwami muzułmańskimi⁶⁴.

W związku z powstaniem organizacji Al-Kaidy w Krajach Islamskiego Maghrebu (Tanzim al-Kaida fi Bilad al-Maghrib al-Islami) w 2007 r. nastąpił wzrost zagrożenia terrorystycznego w Hiszpanii. Internetowy organ medialny organizacji „Al-Andalus” głosił m.in., że jego celem jest rekrutowanie zwolenników pod hasłem walki o kalifat na Półwyspie Iberyjskim. Oświadczenia i materiały propagandowe zamieszczane na portalu przyczyniały się do radykalizacji hiszpańskich muzułmanów. Zastępca Bin Ladena w Al-Kaidzie Ajman az-Zawahiri wzywał do (...) *odzyskania Al-Andalus, co jest powinnością naszego ludu w ogóle, a was* (krajów Maghrebu – dop. aut.) – *w szczególności. Ten cel będzie można osiągnąć jedynie pozbywając się z islamskiego Maghrebu synów Francji i Hiszpanii*⁶⁵. Hiszpania zajęła też szczególne miejsce w ideologii Państwa Islamskiego, przez które była postrzegana jako naturalna część kalifatu obecnie okupowana przez „niewiernych”. Aby zminimalizować rosnące zagrożenie, zwiększono liczbę funkcjonariuszy zajmujących się problematyką ekstremizmu muzułmańskiego. W CNCA zatrudniono więcej tłumaczy języka arabskiego. W kwietniu 2004 r.⁶⁶ było ich 11, a w listopadzie 2007 r. – 86. Przeprowadzono wiele operacji, podczas których aresztowano miejscowych radykałów oraz imigrantów z Afryki Północnej i Bliskiego Wschodu. Przyjechali oni do Hiszpanii, w ojczystrych krajach zaś byli ścigani za terroryzm. Rozbito ponadto wiele komórek terrorystycznych o międzynarodowych powiązaniach, w tym komórkę przygotowującą atak na Sąd Najwyższy w Madrycie (październik 2004 r.). Istniało realne zagrożenie płynące z aktywności radykałów przebywających w więzieniach, którzy starali się tam rekrutować muzułmanów do prowadzenia działań terrorystycznych po opuszczeniu zakładu karnego. Policyjna operacja pod kryptonimem „NOVA” miała przeciwdziałać tym

⁶⁴ Centro Nacional de Coordinación Antiterrorista CNCA, La Pagina de ASR, <https://intelpage.info/centro-nacional-de-coordinacion-antiterrorista.html> [dostęp: 12 XII 2015].

⁶⁵ K. Izak, *Leksykon organizacji i ruchów islamistycznych...*, s. 469.

⁶⁶ S. Kosmyńska, *Święta wojna w Al-Andalus. Przeobrażenia aktywności dżihadystycznych komórek terrorystycznych w Hiszpanii w latach 1995–2012*, Łódź 2015, s. 304.

tendencjom. Po zamachach w Madrycie duża aktywność ekstremistów muzułmańskich koncentrowała się w Katalonii. Do 2009 r. przeprowadzono tam 14 operacji antyterrorystycznych, większość w Barcelonie i okolicach, m.in. „Tygrys” („Tigris”), „Szakal” („Chacal”) czy „Kameleon” („Camaleon”)⁶⁷. W ciągu 10 lat działalności CNCA zrealizowało w Hiszpanii ponad 50 operacji skierowanych przeciwko międzynarodowym strukturalnym terrorystycznym oraz luźnym komórkom bez szerszych powiązań organizacyjnych. W tym czasie aresztowano ponad 500 osób, ale tylko 14% z nich zostało skazanych, pozostałych zwolniono z braku dowodów⁶⁸. Władze zezwalały jednak na organizowanie spotkań islamskich radykałów, w których uczestniczyło po kilka tysięcy osób. W 2010 r. w Hiszpanii odbyło się co najmniej dziesięć kongresów salafitów, w których wzięło udział od 2000 do 3000 osób. Dwa lata wcześniej zorganizowano tylko jeden taki kongres⁶⁹. Polityka wielokulturowości, tolerowania, a nawet wspierania aktywności mniejszości religijnych, lansowana przez władze, które bagatelizowały płynące z zagranicy finansowanie organizacji, meczetów i centrów muzułmańskich, zderzała się z działaniami służb specjalnych, mających coraz większe problemy z inwigilowaniem środowisk radykalnych.

Po ogłoszeniu przez ETA w 2011 r. zakończenia działalności zbrojnej służby specjalne skoncentrowały się na walce z terroryzmem islamskim i przeciwdziałaniu muzułmańskiemu ekstremizmowi, co korelowało w czasie z tworzeniem nowego frontu walki dżihadystów w Iraku i Syrii. W związku ze wzrostem zagrożenia ze strony terrorystów związanych z Państwem Islamskim w połowie października 2014 r. CNCA zostało połączone z Centrum Wywiadu przeciwko Przestępczości Zorganizowanej (Centro de Inteligencia contra el Crimen Organizado, CICO), tworząc Centrum Wywiadu ds. Zwalczania Terroryzmu i Przestępczości Zorganizowanej (Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, CITCO). Celem fuzji była optymalizacja wysiłków i lepsze wykorzystanie zasobów ekonomicznych obu agencji w obliczu narastających zagrożeń i powiązań między ekstremistami, organizacjami terrorystycznymi i przestępczością zorganizowaną. Oprócz wymienionych już działań prowadzonych wcześniej przez CNCA, zadaniem CITCO jest m.in. przekazywanie FCSE istotnych informacji i prognoz, koordynowanie działań FCSE,

⁶⁷ Tamże, s. 259, 262.

⁶⁸ Tamże, s. 310.

⁶⁹ J. Loredo, *Marzenie o Al Andalus*, „Nasz Dziennik”, 19 XI 2011 r.

sporządzanie rocznych raportów na temat przestępczości zorganizowanej, terroryzmu i radykalizmu w Hiszpanii oraz okresowej oceny zagrożenia w tych obszarach. W gestii CITCO znajduje się opracowywanie i rozpowszechnianie statystyk związanych z powyższymi zagadnieniami, jak również utrzymywanie kontaktów z odpowiednimi instytucjami w Brukseli i podobnymi jednostkami w krajach członkowskich UE. Stworzono specjalny zespół do monitorowania działań w internecie. To właśnie w sieci werbowano 80% dżihadystów do udziału w walkach w Iraku i Syrii. Przystąpiono również do realizacji programu deradykalizacji środowisk młodych muzułmanów⁷⁰.

Celem hiszpańskich służb było podejmowanie interwencji na możliwie jak najwcześniejszym etapie, aby zapobiec zamachom. W przypadku islamskich terrorystów udawało się to przez 13 lat (z różnym powodzeniem w przypadku ETA, która ostatniego zamachu dokonała w 2009 r.). W raporcie hiszpańskiego ministerstwa spraw wewnętrznych z 2016 r. zauważono, że liczba wiadomości wysyłanych przez dżihadystów, wzywających tzw. samotne wilki do przeprowadzenia ataków na Hiszpanię i do „wyzwolenia” takich miast, jak Toledo, Kordoba czy Sewilla, podwoiła się w porównaniu z poprzednimi latami⁷¹. Stało się oczywiste, że dżihadyści będą starali się przeprowadzić kolejne ataki. Realnym celem była Katalonia. Już w październiku 2007 r. CIA przekazała władzom w Madrycie raport, z którego wynikało, że region autonomiczny Katalonii przekształcił się w zaplecze operacyjne i werbunkowe terrorystów. Pojawiały się nawet alarmujące opinie, że Katalonia stała się nowym centrum globalnego dżihadu⁷². Nie można zapominać, że nawoływanie Państwa Islamskiego do podejmowania wszelkich działań terrorystycznych w Europie trafiło na podatny grunt w Hiszpanii, gdzie zwiększył się napływ nielegalnych imigrantów z Afryki, a miejscowi muzułmanie mocno się radykalizowali. Gdy w 2016 r. UE zawarła umowę z Turcją o odsyłaniu nielegalnych imigrantów, znaczenia nabrały

⁷⁰ Interior cesa al jefe del CITCO y nombra a un comisario al frente del Gabinete de Estudios y Coordinación, elDiario.es, 7 VII 2018 r., https://www.eldiario.es/politica/interior-citco-gabinete-estudios-coordinacion_1_2035094.html [dostęp: 7 VII 2018].

⁷¹ J. Badcock, *The Long Shadow of al-Andalus. Spain is on the periphery of Europe, but central to modern jihad*, Foreign Policy, 21 VIII 2017 r., <https://foreignpolicy.com/2017/08/21/the-long-shadow-of-al-andalus-spain-islamic-state-terrorism-al-qaeda/> [dostęp: 21 VIII 2017].

⁷² K. Haahr, *The Growth of Militant Islamist Micro-Diaspora Communities*, „CTC Sentinel” 2008, t. 1, nr 4, <https://ctc.westpoint.edu/wp-content/uploads/2010/06/Vol1Iss4-Art6.pdf> [dostęp: 18 IV 2008].

szlaki przerzutu migrantów z Libii i Tunezji do Włoch oraz z Maroka przez Cieśninę Gibraltarską do Hiszpanii. Niemniej jednak hiszpańskie służby zostały uznane za jedne z najskuteczniejszych w Europie pod względem wykrywania terrorystów, a hiszpańscy eksperci do walki z terroryzmem zyskali miano najlepszych na świecie. W uznaniu ich zasług zorganizowano w lipcu 2015 r. w Madrycie posiedzenie Komitetu Antyterrorystycznego ONZ⁷³. Wizerunku tego nie nadszarpnął zamach w Barcelonie, do którego doszło dwa lata później.

W dniach 17 i 18 sierpnia 2017 r. Katalonia stała się celem ataków dżihadystów z Ripoll. Zginęło wówczas 16 osób, a 128 zostało rannych⁷⁴. Ponadto siedmiu terrorystów zostało zabitych przez policję podczas zamachów lub krótko po nich, a trzech stanęło przed sądem. Terroryci zaatakowali w Barcelonie i Cambrils przy użyciu samochodów oraz noży. W ich zamierzeniu atak miał przebiegać zupełnie inaczej. Do zmiany planów przyczynił się wybuch w bazie terrorystów w Alcanar, w wyniku którego zginęli radykalny imam Abdelbaki (Abdel Baki) As-Satty, inicjator ataku, oraz terrorysta przygotowujący materiał wybuchowy⁷⁵. Jeden z terrorystów został ranny. Śledztwo wykazało, że pierwotny plan zamachowców przewidywał umieszczenie w furgonetce 200 kg materiału wybuchowego wykonanego na bazie TATP (z ang. *triacetone triperoxide*, trimeryczny nadtlenek acetonu), zwanego też matką szatana, obłożonego butlami z gazem, aby zwiększyć siłę eksplozji. Celem była prawdopodobnie Sagrada Família. W wielu opiniach

⁷³ *Madryt: posiedzenie Komitetu Antyterrorystycznego ONZ*, Dziennik Gazeta Prawna, 27 VII 2015 r., <https://www.gazetaprawna.pl/wiadomosci/artykuly/885271,madryt-posiedzenie-komitetu-antyterrorystycznego-onz.html> [dostęp: 27 VII 2015].

⁷⁴ *Hiszpania: Rozpoczął się proces dżihadysty zatrzymanego w Warszawie*, Dziennik Gazeta Prawna, 11 VI 2018 r., <https://www.gazetaprawna.pl/wiadomosci/artykuly/1132741,proces-dzihadysty-zatrzymanego-w-warszawie.html> [dostęp: 11 VI 2018].

⁷⁵ Abdelbaki As-Satty był Marokańczykiem. W 2014 r. sąd nakazał wydalenie go z Hiszpanii, tuż po zakończeniu odsiadania przez niego wyroku za przemyt narkotyków. Mimo tej decyzji As-Satty pozostał w Hiszpanii, co więcej w 2015 r. sąd wyższej instancji nakazał cofnięcie decyzji o jego wydaleniu. Mógł więc legalnie przebywać w tym kraju. Zamieszkał w katalońskim mieście Ripoll, gdzie do czerwca 2017 r. w miejscowym meczecie wygłaszał kazania nawołujące do radykalizmu, nauczał i werbował do walki po stronie Państwa Islamskiego w Iraku i Syrii. Sam został zwerbowany podczas pobytu w więzieniu, gdzie poznał Raszida Aglifa, odbywającego wyrok za współudział w zamachach w Madrycie 11 marca 2004 r. Ukazuje to braki w działaniach prewencyjnych służby penitencjarnej, przede wszystkim niedostateczną kontrolę nad relacjami, jakie skazani nawiązywali w więzieniach. System uszczelniono jesienią 2018 r. Zob. J. Dziedzina, *Imam kazał zabijać*, gość.pl, 7 IX 2017 r., <https://www.gosc.pl/doc/4166327.Imam-kazal-zabijac> [dostęp: 7 IX 2017].

wyrażano tezę, że atak można było udaremnić, gdyby nie arogancja władz Katalonii, które zlekceważyły ostrzeżenia i sabotowały współpracę z siłami bezpieczeństwa państwa, uchylając się od przekazywania Madrytowi istotnych informacji o dżihadystach⁷⁶. Odmówiły też postawienia przy wjeździe na deptak Las Ramblas betonowych zapór, mających zapobiec wjechaniu tam samochodów. To właśnie w tym miejscu rozpedzony pojazd zabił najwięcej ludzi. Bezpieczeństwo mieszkańców Barcelony i turystów zostało podporządkowane miejscowym politykom, którzy dopuścili się wielu zaniechań w imię polityki uniezależnienia się Katalonii od Hiszpanii, a jednym z jej elementów było zjednanie sobie sympatii muzułmanów przed referendum secesyjnym 1 października 2017 r.⁷⁷

Tydzień po wydarzeniach w Katalonii Państwo Islamskie przyznało się do ataków i ostrzegło przed kolejnymi zamachami. W upublicznionym nagraniu wideo Muhammad Jasin Ahram Pérez, obywatel Hiszpanii, który w 2014 r. wyjechał do Syrii, groził: *Hiszpańscy chrześcijanie, nie zapominajcie o muzułmańskiej krwi, która została przelana, i o hiszpańskiej inkwizycji. Pomścimy dokonane przez was masakry i te, które przeprowadzacie teraz przeciwko Państwu Islamskiemu. Al-Andalus znowu będzie tym, czym było, krainą kalifatu*⁷⁸. Wobec nowych wyzwania ówczesna wicepremier Hiszpanii Soraya Sáenz de Santamaria przekazała CNI dodatkowo 20 mln euro na działania antyterrorystyczne oraz zatrudnienie 600 nowych agentów. W systemie wymiaru sprawiedliwości wprowadzono reformy prawne, które ułatwiły stawianie podejrzanych przed sądem. Dotąd można było ich zatrzymać, przesłuchać, a jeśli nie znaleziono wystarczających dowodów potwierdzających winę podejrzanych, należało ich zwolnić⁷⁹. Po ataku terrorystycznym w Barcelonie hiszpańskie służby wspierane przez CNI przeprowadziły osiemnastomiesięczną tajną operację pod kryptonimem „Alexandra”. Jej zwieńczeniem było aresztowanie w styczniu 2019 r. 17 osób, wśród których znajdowało się pięciu obywateli Algierii, Libii oraz Iraku. Oskarżono ich o przynależność

⁷⁶ *Zamachy terrorystyczne w Hiszpanii. Można było im zapobiec*, Magazyn TVN24, <https://archiwum.tvn24.pl/magazyn-tvn24/114/tvn24.pl/magazyn-tvn24/willa-na-uboczu-matka-szata-na-i-plan-a-zamach-na-niespotykana-skale,114,2082.html> [dostęp: 22 VIII 2017].

⁷⁷ K. Izak, *Sieć ekstremistów religijnych i politycznych. Sojusznicy i wrogowie*, „Przegląd Bezpieczeństwa Wewnętrznego” 2019, nr 21, s. 107; *Zamachy terrorystyczne w Hiszpanii...*

⁷⁸ J. Martin-Arroyo, *El Cordobés, the Spanish face of Islamic State*, El Pais, 25 VIII 2017 r., https://english.elpais.com/elpais/2017/08/25/inenglish/1503659430_853709.html [dostęp: 25 VIII 2017]. Tłumaczenie pochodzi od autora (dop. red.).

⁷⁹ T. Skowronek, *Hiszpania walczy ze światowym terroryzmem*, „Przegląd” 2019, nr 46, s. 29.

do Państwa Islamskiego. Realizowano ponadto operacje „Minerwa” i „Neptun”, których celem było śledzenie tras podróży terrorystów wracających ze stref walki w Iraku i Syrii po upadku Państwa Islamskiego. Do Hiszpanii przybywali oni najczęściej wmieszani w grupy afrykańskich migrantów, pokonując w łodziach Cieśninę Gibraltarską. Okazało się również, że wprowadzony w 2014 r. program deradykalizacji więźniów był nieskuteczny. Po dwóch latach od jego wdrożenia w hiszpańskich więzieniach przebywało prawie 100 radykałów muzułmańskich, czyli dwukrotnie więcej niż przed rozpoczęciem tego programu. W październiku 2018 r. ujawniono, że w 17 więzieniach, w których znajdowali się islamscy ekstremiści, w proces radykalizacji było zaangażowanych łącznie 25 osób, m.in. niektórzy skazani za ataki w Madrycie w marcu 2004 r., w tym Al-Haski. Z tej grupy aż 21 osób przebywało w odosobnieniu. Pomimo to prowadziły one działalność propagandową za pomocą listów przekazywanych innym więźniom wychodzącym na spacer, a także przy udziale członków ich rodzin. W lutym 2018 r. hiszpański rząd uruchomił nowy program służący przeciwdziałaniu radykalizacji więźniów. W ramach jego realizacji wszyscy funkcjonariusze w więzieniu mieli obowiązek codziennej obserwacji zachowań osadzonych wyznających islam, a także osób uznawanych za podatne na radykalizację. W październiku 2018 r. w 28 zakładach karnych przebywało łącznie 140 dżihadystów, z których część znajduje się już na wolności⁸⁰.

Rok 2018 był krytyczny dla hiszpańskich służb z powodu nienotowanej wcześniej liczby nielegalnych migrantów, którzy przybyli z Maroka, pokonując Cieśninę Gibraltarską. Tą drogą dotarło wtedy ponad 57 500 imigrantów na ogólną liczbę ponad 64 000, co stanowiło ponadczterokrotny wzrost w porównaniu z 2017 r.⁸¹ W większości nie posiadali oni żadnych dokumentów tożsamości, by utrudnić ewentualną ekstradycję. Zjawisku nielegalnej migracji do Hiszpanii towarzyszą handel fałszywymi dokumentami i kradzieże danych osobowych. W tym procederze Hiszpania znajduje się w czołówce krajów UE⁸². Przystępczość ta umożliwia imigrantom legalizację pobytu z fałszywą tożsamością, co stanowi dodatkowe wyzwanie dla

⁸⁰ A. Kłos, *Fikcja walki z radykalizmem*, „Gazeta Polska Codziennie”, 13 X 2018 r.; „El Mundo”: *zamachowcy z Madrytu radykalizowali młodych muzułmanów w więzieniach*, TVN24, 11 X 2018 r., <https://tvn24.pl/swiat/zamachowcy-z-madrytu-radykalizowali-mlydych-muzulmanow-w-wiezieniach-ra875396-2384538> [dostęp: 11 X 2018].

⁸¹ K. Izak, *Hiszpania i Francja walczą z nielegalną imigracją i fałszerstwami dokumentów*, „Człowiek i Dokumenty” 2021, nr 62, s. 68.

⁸² Tamże, s. 69.

służb specjalnych. Tą drogą dotarł do Hiszpanii m.in. Abdel Madzid Abdel Bary, znany jako raper Państwa Islamskiego, który w mediach społecznościowych zamieszczał liczne groźby po adresem państw zachodnich⁸³.

Władze Maroka wykorzystują w celach politycznych i ekonomicznych presję migracyjną na granice Hiszpanii, wysuwając kolejne żądania i domagając się ustępstw od Madrytu. Dnia 22 maja 2021 r. władze Rabatu wezwały Hiszpanię do wszczęcia dochodzenia w sprawie przybycia na leczenie do tego kraju siedemdziesięcioletniego Brahima Ghaliego, przywódcy Frontu Polisario. Decyzja Madrytu o przyjęciu Ghaliego bez poinformowania Rabatu nadszarpięła stosunki między obu krajami i spowodowała rozluźnienie ochrony granicy przez marokańskich pograniczników. Zachęciło to koczujących przy granicy migrantów do jej przekroczenia. W ciągu 35 godzin przybyło do Ceuty, hiszpańskiej enklawy w Maroku, ponad 8000 migrantów, w tym ponad 2000 nieletnich⁸⁴.

W latach 2020–2027 UE wypłaci Rabatowi 3,5 mld euro za powstrzymanie własnych obywateli przed przekraczaniem lądowych i morskich granic Maroka z Hiszpanią. Z tego wynika, że umowa nie obejmuje migrantów z innych państw Afryki, którzy nadal forsują hiszpańską granicę⁸⁵. Ich celem są również Wyspy Kanaryjskie. W 2020 r. przyplłynęło tu 23 000 migrantów, dziesięciokrotnie więcej niż w roku poprzednim. Ten kierunek Rabat również wykorzystuje, rozluźniając kontrolę wybrzeża. Celem jest skłonienie Hiszpanii do uznania marokańskiej zwierzchności nad Saharą Zachodnią i uzyskanie największego dostępu do podwodnych złóż telluru, rud rzadkiego półmetalów, które znajdują się u wybrzeży Wysp Kanaryjskich⁸⁶.

Innym czynnikiem negatywnie wpływającym na bezpieczeństwo w Hiszpanii jest sytuacja w Katalonii, gdzie nadal są obecne separatystyczne dążenia. W październiku odbywają się tam burzliwe manifestacje w celu uczczenia rocznicy referendum niepodległościowego z 2017 r. W 2019 r. rocznicowa manifestacja w Barcelonie zamieniła się w gwałtowne zamieszki i strajk generalny w Katalonii, co jak nigdy wcześniej

⁸³ K. Izak, *Oryginalne paszporty w rękach terrorystów i oszustów*, „Człowiek i Dokumenty” 2019, nr 54, s. 51; J. Wójcik, „Raper ISIS” wrócił do Europy po azyl, euroislam.pl, 20 V 2020 r., <https://euroislam.pl/rapper-isis-do-europy-powrocil-jako-szukajacy-azylu/> [dostęp: 20 V 2020].

⁸⁴ K. Izak, *Migranci jako element nacisku w stosunkach międzynarodowych. Dokumenty dowodem przestępczej działalności państw*, „Człowiek i Dokumenty” 2021, nr 63, s. 59.

⁸⁵ Tamże.

⁸⁶ G. Lindenberg, *Czy Maroko gra z Hiszpanią imigrantami?*, euroislam.pl, 14 II 2021 r., <https://euroislam.pl/czy-maroko-gra-z-hiszpania-imigrantami/> [dostęp: 14 II 2021].

naruszyło politykę regionu i całej Hiszpanii. Należy zaznaczyć, że władze Katalonii, w której mieszka 1/4 wszystkich muzułmanów w Hiszpanii, prowadzą własną politykę migracyjną.

W latach 2019–2023 hiszpańskim służbom udało się udaremnić kilka poważnych zamachów, w tym podczas katolickiej procesji w Sewilli w kwietniu 2019 r. Odnotowano też kilka zdarzeń o charakterze terrorystycznym, m.in. w styczniu 2023 r. Marokańczyk zaatakował ludzi w dwóch kościołach w Algeciras. Zginęła jedna osoba, a cztery zostały ranne. Sprawcę aresztowano, gdy wchodził do trzeciej świątyni. Z kolei w sierpniu 2023 r. w Madrycie 11 osób zostało rannych w wyniku ataku niezidentyfikowanych napastników uzbrojonych w noże. Obecnie w Hiszpanii obowiązuje czwarty stopień zagrożenia terrorystycznego w pięciostopniowej skali. Madryt nie zmienił poziomu zagrożenia od 2015 r., po atakach terrorystycznych w Paryżu⁸⁷.

Podsumowanie

Dwadzieścia lat po atakach terrorystycznych w Madrycie Hiszpania zмага się z nielegalną imigracją ludności z Afryki, ruchami nacjonalistycznymi oraz ekstremizmem i terroryzmem islamskim. Autor artykułu nie znajduje jednoznacznej odpowiedzi na pytanie, czy od 2004 r. kraj stał się bardziej bezpieczny. Można by tak sądzić, biorąc pod uwagę zamknięcie działalności terrorystycznej baskijskich separatystów z ETA i samorozwiązanie tej organizacji, jak również sukcesy hiszpańskich służb w eliminowaniu kolejnych komórek terrorystycznych i aresztowaniach ekstremistów. Za tymi osiągnięciami służb antyterrorystycznych kryją się jednak konkretne liczby aresztowanych, które nie napawają optymizmem, ponieważ od lat utrzymują się na wysokim poziomie przy okresowych tendencjach spadkowych. Świadczą one o tym, że mimo podejmowanych wysiłków poziom radykalizacji muzułmanów nie maleje, co stanowi zagrożenie bezpieczeństwa kraju. Przyczyną tego jest nielegalna migracja z Maroka i Algierii oraz innych krajów muzułmańskich. Dla Arabów Hiszpania jest krajem wyjątkowym w Europie, stanowi bowiem w ich świadomości zmitologizowany Al-Andalus przodków (arab. *dar al-islam*, pol. ziemia islamu). Po atakach terrorystycznych

⁸⁷ La Policía Nacional advierte: «estamos en nivel 4 de alerta terrorista». *Estas son las claves*, Hipertextual, 30 V 2023 r., <https://hipertextual.com/2023/05/la-policia-nacional-advierte-estamos-en-nivel-4-de-alerta-terrorista-estas-son-las-claves> [dostęp: 30 V 2023].

z 11 września 2001 r. w USA oraz w obliczu lawinowo rosnącej migracji z krajów muzułmańskich temat islamu w Hiszpanii stał się przedmiotem debaty, artykułów prasowych i opracowań naukowych. W 2001 r. w Hiszpanii żyło 324 000 cudzoziemców wyznających islam⁸⁸. Statystykę dopełniała liczna, zwłaszcza w Andaluzji, grupa konwertytów na islam, szacowana na 20 000–25 000 członków, oraz nielegalni imigranci wyznania muzułmańskiego, którzy sprawiali, że szacunkowa liczba wyznawców islamu w Hiszpanii wynosiła ok. 600 000⁸⁹. Obecnie mieszka ich tam 2 350 000, w tym ponad 640 000 w Katalonii, a więc cztery razy więcej niż 20 lat wcześniej⁹⁰.

Młodzi ludzie przybywający do Hiszpanii z krajów muzułmańskich wnoszą własne idee i wartości, a te w ostatnich latach ukierunkowują się na zwiększoną religijność i pragnienie coraz większego udziału religii w życiu politycznym⁹¹. Stąd tylko krok do roszczeń oraz walki o ustępstwa i przywileje. W zależności od tego, kto sprawuje władzę w Madrycie – socjaliści czy prawicowa Partia Ludowa – polityka migracyjna państwa zaostrza się lub luzuje. Ten sam trend jest widoczny w stosunku do separatystycznych dążeń Katalonii i Baskonii oraz wzmacniania terytorialnej jedności kraju. W latach 2021–2023 udało się władzom Madrytu wyciszyć problemy z Katalonią, co przełożyło się na złagodzenie sporu politycznego i zmniejszenie w Barcelonie zainteresowania władzami regionu. Nie dotyczy to służb specjalnych, które nie mogą liczyć na współpracę z katalońską policją Mossos d'Esquadra, muszą angażować własne siły i środki do inwigilacji tamtejszych środowisk muzułmańskich, które dzięki władzom w Barcelonie cieszą się dużą autonomią.

Hiszpańskie służby specjalne walczące z religijnym terroryzmem i politycznym ekstremizmem nie mają więc łatwego zadania. W niedalekiej przyszłości staną wobec jeszcze poważniejszych wyzwań związanych z szybko zwiększającą się liczbą muzułmanów, w tym radykałów i konserwatywnych wyznawców islamu zamkniętych na integrację z chrześcijańską większością. Ta rosnąca liczba przekłada się bowiem na ich społeczne

⁸⁸ R. Stryjewski, *Muzułmanie w Hiszpanii*, w: *Muzułmanie w Europie*, A. Parzymies (red.), Warszawa 2005, s. 466.

⁸⁹ Tamże.

⁹⁰ R. Fernández, *Número total de musulmanes por comunidad autónoma de España en 2022*, Statista, 11 IV 2023 r., <https://es.statista.com/estadisticas/552893/musulmanes-en-espana-por-comunidad-autonoma/> [dostęp: 11 IV 2023].

⁹¹ J. Wójcik, *Czy polityczny islam wraca na Bliski Wschód?*, euroislam.pl, 22 VIII 2023 r., <https://euroislam.pl/czy-polityczny-islam-wraca-na-bliski-wschod/> [dostęp: 22 VIII 2023].

żądania i polityczne dążenia. W 2018 r. muzułmanie zapowiedzieli utworzenie własnych partii na wzór marokańskich Partii Sprawiedliwości i Rozwoju (Hizb al-Adala wa at-Tanmijja), Sprawiedliwości i Dobroczyńności (Al-Adl wa al-Ihsan) i tunezyjskiej Partii Odrodzenia (Hizb an-Nahda), wywodzących się z ruchu Braci Muzułmanów (Al-Ichwan al-Muslimin)⁹². Należy mieć nadzieję, że wzrost sił i środków przeznaczanych na działalność hiszpańskich służb specjalnych i dobra współpraca z ich odpowiednikami w Maroku, niezależnie od politycznych zawirowań między Madrytem i Rabatem, pozwoli skutecznie przeciwstawiać się zagrożeniom bezpieczeństwa antyterrorystycznego Hiszpanii.

Bibliografia

Brylew M., *Irak 2006–2012. Stabilizacja czy konflikt?*, Toruń 2013.

Cieszek J., *Tragedia w Madrycie, 11–14 marca 2004 roku*, w: *Hiszpania: Media masowe i wybory w obliczu terroryzmu*, B. Dobek-Ostrowska, M. Kuś (red.), Wrocław 2007, s. 39–60.

Domejko-Kozera P., *Polityka bezpieczeństwa w Hiszpanii w latach 1992–2004*, Warszawa 2006.

Gonzalez Esteban J.L., *Kronika 11 marca: terroryzm i polityczna zmiana w Hiszpanii*, w: *Hiszpania: Media masowe i wybory w obliczu terroryzmu*, B. Dobek-Ostrowska, M. Kuś (red.), Wrocław 2007, s. 61–72.

Grześkowiak S., *Poczet islamskich ideologów i ekstremistów*, Warszawa 2023.

Izak K., *Hiszpania i Francja walczą z nielegalną imigracją i fałszerstwami dokumentów*, „Człowiek i Dokumenty” 2021, nr 62, s. 67–75.

Izak K., *Leksykon organizacji i ruchów islamistycznych*, Warszawa 2014.

Izak K., *Migranci jako element nacisku w stosunkach międzynarodowych. Dokumenty dowodem przestępczej działalności państw*, „Człowiek i Dokumenty” 2021, nr 63, s. 56–65.

Izak K., *Oryginalne paszporty w rękach terrorystów i oszustów*, „Człowiek i Dokumenty” 2019, nr 54, s. 44–55.

⁹² K. Izak, *Sieć ekstremistów...*, s. 108.

Izak K., *Sieć ekstremistów religijnych i politycznych. Sojusznicy i wrogowie*, „Przegląd Bezpieczeństwa Wewnętrznego” 2019, nr 21, s. 96–134.

Jakubowska Z., *Madryt 11 marca*, Warszawa 2005.

Kłos A., *Fikcja walki z radykalizmem*, „Gazeta Polska Codziennie”, 13 X 2018 r.

Kosmyńska S., *Święta wojna w Al-Andalus. Przeobrażenia aktywności dżihadystycznych komórek terrorystycznych w Hiszpanii w latach 1995–2012*, Łódź 2015.

Loredo J., *Marzenie o Al Andalus*, „Nasz Dziennik”, 19 XI 2011 r.

Łódzki B., *Reakcja polskich mediów masowych na atak terrorystyczny w Madrycie 11 marca 2004 r.*, w: *Hiszpania: Media masowe i wybory w obliczu terroryzmu*, B. Dobek-Ostrowska, M. Kuś (red.), Wrocław 2007, s. 123–137.

Pludowski T., *Reakcje prasy amerykańskiej na madrycki atak terrorystyczny z 11 marca 2004 r.*, w: *Hiszpania: Media masowe i wybory w obliczu terroryzmu*, B. Dobek-Ostrowska, M. Kuś (red.), Wrocław 2007, s. 140–159.

Reinares F., *Al-Qaeda's Revenge. The 2004 Madrid Train Bombing*, New York 2016.

Skowronek T., *Hiszpania walczy ze światowym terroryzmem*, „Przegląd” 2019, nr 46, s. 28–30.

Stryjewski R., *Muzułmanie w Hiszpanii*, w: *Muzułmanie w Europie*, A. Parzymies (red.), Warszawa 2005, s. 453–493.

Taracha C., *Wybory w cieniu zamachu. Kilka uwag na temat wydarzeń z marca 2004 roku w Madrycie*, w: *Terroryzm wczoraj i dziś. Wybrane problemy*, P. de la Fuente, W. Gizicki, C. Taracha (red.), Lublin 2015, s. 77–85.

Tryc-Ostrowska M., *Kontrowersyjny wyrok za zamachy w Madrycie*, „Rzeczpospolita”, 2 XI 2007 r.

Wejkszner A., *Ewolucja terroryzmu motywowanego ideologią religijną na przykładzie salafickiego ruchu globalnego dżihadu*, Poznań 2010.

Źródła internetowe

Actividad Terrorista de ETA 2004, Ministerio del Interior, <https://www.statewatch.org/media/documents/news/2005/jan/mirbal2004acteta.pdf> [dostęp: 12 III 2005].

Atentados Terroristas del Dia 11 del Marzo de 2004 de Madrid, Juzgado Central de Instruccion Nº 6 Audiencia Nacional Madrid, <https://e00-elmundo.uecdn.es/documentos/2006/04/11/auto11m/01.pdf> [dostęp: 11 IV 2006].

Badcock J., *The Long Shadow of al-Andalus. Spain is on the periphery of Europe, but central to modern jihad*, Foreign Policy, 21 VIII 2017 r., <https://foreignpolicy.com/2017/08/21/the-long-shadow-of-al-andalus-spain-islamic-state-terrorism-al-qaeda/> [dostęp: 21 VIII 2017].

Becares R., Cernuda O., *Cuatro terroristas islámicos se inmolan en un piso de Leganés y matan a un agente de policía*, elmundo.es, 4 IV 2004 r., <https://www.elmundo.es/elmundo/2004/04/03/enespecial/1081016920.html> [dostęp: 4 IV 2004].

Catalán M., *Prensa, verdad y terrorismo: la lección política del 14-M*, „El Argonauta Español” 2005, nr 2. <https://doi.org/10.4000/argonauta.1191> [dostęp: 26 VIII 2023].

Cedeira B., *La víctima que entró en coma el 11M hasta morir 10 años después*, El Español, 11 III 2017 r., https://www.elespanol.com/reportajes/20170310/199730525_0.html [dostęp: 11 III 2017].

Centro Nacional de Coordinación Antiterrorista CNCA, La Pagina de ASR, <https://intelpage.info/centro-nacional-de-coordinacion-antiterrorista.html> [dostęp: 12 XII 2015].

Dziedzina J., *Imam kazał zabijać*, gość.pl, 7 IX 2017 r., <https://www.gosc.pl/doc/4166327.Imam-kazal-zabijac> [dostęp: 7 IX 2017].

El final del principio en la investigación del 11-M, elmundo.es, 1 XI 2007 r., <https://www.elmundo.es/elmundo/2007/11/01/espana/1193885319.html> [dostęp: 1 XI 2007].

„El Mundo”: *zamachowcy z Madrytu radykalizowali młodych muzułmanów w więzieniach*, TVN24, 11 X 2018 r., <https://tvn24.pl/swiat/zamachowcy-z-madrytu-radykalizowali-mlodych-musulmanow-w-wiezieniach-ra875396-2384538> [dostęp: 11 X 2018].

ETA pretendía volar la estación de Chamartín con un „tren bomba” y provocar una masacre, ABC España, 26 XII 2003 r., https://www.abc.es/espana/abci-pretendia-volar-estacion-chamartin-tren-bomba-y-provocar-masacre-200312260300-228547_noticia.html [dostęp: 26 XII 2003].

Fernández H.A., *Does al-Qaeda have a global strategy?*, Elcano Royal Institute, 4 V 2004 r., <https://www.realinstitutoelcano.org/en/analyses/does-al-qaeda-have-a-global-strategy/> [dostęp: 6 V 2004].

Fernández R., *Número total de musulmanes por comunidad autónoma de España en 2022*, Statista, 11 IV 2023 r., <https://es.statista.com/estadisticas/552893/musulmanes-en-espana-por-comunidad-autonoma/> [dostęp: 11 IV 2023].

Fernando Reinares, *experto en terrorismo internacional*, advierte: “Al Qaeda está hoy más extendida de lo que ha estado nunca”, Universidad Internacional Menéndez Pelayo, <https://www.uimp.es/actualidad-uimp/fernando-reinare-experto-terrorismo-internacional.html> [dostęp: 21 VI 2021].

Gunaratna R., *Spain: An Al Qaeda Hub?*, „UNISCI Discussion Papers” 2004, nr 5, <https://www.redalyc.org/pdf/767/76712467002.pdf> [dostęp: 22 II 2014].

Haahr K., *The Growth of Militant Islamist Micro-Diaspora Communities*, „CTC Sentinel” 2008, t. 1, nr 4, <https://ctc.westpoint.edu/the-growth-of-militant-islamist-micro-diaspora-communities-observations-from-spain/> [dostęp: 18 IV 2008].

Hernández A., *11M: quién fue el autor intelectual y otras claves que plantea el documental de Netflix sobre el mayor atentado yihadista en Europa*, BBC, 11 III 2022 r., <https://www.bbc.com/mundo/noticias-60693476> [dostęp: 11 III 2022].

Hiszpania: Rozpoczął się proces dżihadysty zatrzymanego w Warszawie, Dziennik Gazeta Prawna, 11 VI 2018 r., <https://www.gazetaprawna.pl/wiadomosci/artykuly/1132741,proces-dzhadysty-zatrzymanego-w-warszawie.html> [dostęp: 11 VI 2018].

Hiszpański parlament zgodził się na wysłanie żołnierzy do Iraku, Wirtualna Polska, 22 X 2014 r., <https://wiadomosci.wp.pl/hiszpanski-parlament-zgodzil-sie-na-wyslanie-zolnierzy-do-iraku-6027730872366209a> [dostęp: 22 X 2014].

Interior cesa al jefe del CITCO y nombra a un comisario al frente del Gabinete de Estudios y Coordinación, elDiario.es, 7 VII 2018 r., https://www.eldiario.es/politica/interior-citco-gabinete-estudios-coordinacion_1_2035094.html [dostęp: 7 VII 2018].

La policía eleva a siete los terroristas muertos en Leganés, Cadenaser, 7 IV 2004 r., https://cadenaser.com/ser/2004/04/07/espana/1081295423_850215.html [dostęp: 7 IV 2004].

La Policía Nacional advierte: «estamos en nivel 4 de alerta terrorista». Estas son las claves, Hipertextual, 30 V 2023 r., <https://hipertextual.com/2023/05/la-policia-nacional-advierte-estamos-en-nivel-4-de-alerta-terrorista-estas-son-las-claves> [dostęp: 30 V 2023].

Lindenberg G., *Czy Maroko gra z Hiszpanią imigrantami?*, euroislam.pl, 14 II 2021 r., <https://euroislam.pl/czy-maroko-gra-z-hiszpania-imigrantami/> [dostęp: 14 II 2021].

Llega a España “El Egipcio” para ser juzgado por el 11-M, 20 minutos, 17 XI 2006 r., <https://www.20minutos.es/noticia/173755/0/egipcion/11-m/italia/> [dostęp: 17 XI 2006].

Los terroristas del 11-M se inmolan y matan a un geo al volar su «piso franco» en Leganés, ABC España, 4 IV 2004 r., https://www.abc.es/espana/abci-terroristas-inmolan-y-matan-volar-piso-franco-leganes-200404040300-962802830594_noticia.html [dostęp: 4 IV 2004].

Maclean W., *New evidence of Qaeda tie to Madrid blast: expert*, Reuters, 13 I 2010 r., <https://www.reuters.com/article/cnews-us-security-spain-qaeda-id-CATRE60B52020100112> [dostęp: 13 I 2010].

Madrid bombings 'probably al Qaeda', Stuff, 21 I 2010 r., <https://www.stuff.co.nz/vl-push/world/3226277/Madrid-bombings-probably-al-Qaeda> [dostęp: 21 I 2010].

Madryt: posiedzenie Komitetu Antyterrorystycznego ONZ, Dziennik Gazeta Prawna, 27 VII 2015 r., <https://www.gazetaprawna.pl/wiadomosci/artykuly/885271,madryt-posiedzenie-komitetu-antyterrorystycznego-onz.html> [dostęp: 27 VII 2015].

Martin-Arroyo J., *El Cordobés, the Spanish face of Islamic State*, El Pais, 25 VIII 2017 r., https://english.elpais.com/elpais/2017/08/25/inenglish/1503659430_853709.html [dostęp: 25 VIII 2017].

Martin Plaza A., *Los atentados del 11M que sacudieron España*, RTVE, 11 III 2014 r., <https://www.rtve.es/noticias/20140311/atentados-del-11m-sacudieron-espana/893543.shtml> [dostęp: 11 III 2014].

Mroczek A., *Zamach w Madrycie 11 III 2004 – minuta po minucie*, terroryzm.com, 25 IX 2005 r., <http://www.terroryzm.com/zamach-w-madrycie-11-iii-2004-minuta-po-minucie/> [dostęp: 25 IX 2005].

Po pięciu latach koniec polskiej misji w Iraku, money.pl, 29 X 2008 r., https://www.money.pl/archiwum/wiadomosci_agencyjne/pap/artykul/po;pieniu;latach;koniec;polskiej;misji;w;iraku,188,0,381372.html [dostęp: 29 X 2008].

Reinares F., *The Evidence of Al-Qa`ida's Role in the 2004 Madrid Attack*, „CTC Sentinel” 2012, t. 5, nr 3, <https://ctc.westpoint.edu/the-evidence-of-al-qaidas-role-in-the-2004-madrid-attack/> [dostęp: 18 IV 2012].

Siedmiu hiszpańskich agentów zginęło w Iraku, Wirtualna Polska, 29 XI 2003 r., <https://wiadomosci.wp.pl/siedmiu-hiszpanskich-agentow-zginelo-w-iraku-6036492925121665a> [dostęp: 30 XI 2003].

The Terror Attacks in Madrid, Spain, 2004, Kamedo-report 90, Socialstyrelsen 2007, https://www.socialstyrelsen.se/globalassets/sharepoint-dokument/artikelkatalog/ovrigt/2007-123-36_200712336.pdf [dostęp: 11 III 2008].

What's Osama Talking About?, Slate, 8 X 2001 r., <https://slate.com/news-and-politics/2001/10/what-s-osama-talking-about.html> [dostęp: 8 X 2001].

Wójcik J., *Czy polityczny islam wraca na Bliski Wschód?*, euroislam.pl, 22 VIII 2023 r., <https://euroislam.pl/czy-polityczny-islam-wraca-na-bliski-wschod/> [dostęp: 22 VIII 2023].

Wójcik J., *„Raper ISIS” wrócił do Europy po azyl*, euroislam.pl, 20 V 2020 r., <https://euroislam.pl/rapper-isis-do-europy-powrocil-jako-szukajacy-azylu/> [dostęp: 20 V 2020].

Zamachy terrorystyczne w Hiszpanii. Można było im zapobiec, Magazyn TVN24, <https://archiwum.tvn24.pl/magazyn-tvn24/114/tvn24.pl/magazyn-tvn24/willa-na-uboczumatka-szatana-i-plan-a-zamach-na-niespotykana-skale%2C114%2C2082.html> [dostęp: 22 VIII 2017].

Zamachy w Madrycie – odwet za Irak, Polskie Radio, 11 III 2014 r., <https://www.polskieradio.pl/106/246/Artykul/1071933%2CZamachy-w-Madrycie---odwet-za-Irak> [dostęp: 11 III 2014].

Zmarła czwórka Polaków rannych w Madrycie, Gazeta Wyborcza, 12 III 2004 r., <https://web.archive.org/web/20091214225052/http://wyborcza.pl/1,75248,1961962.html> [dostęp: 12 III 2004].

Krzysztof Izak

Emerytowany funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Kontakt: lizior3@wp.pl


Grupa Wagnera w Afryce. Pozorowana walka rosyjskich najemników z terroryzmem

The Wagner Group in Africa.

The sham battle of Russian mercenaries against terrorism

ALEKSANDER OLECH

Defence24

 <https://orcid.org/0000-0002-3793-5913>

Abstrakt

W ostatnich latach Grupa Wagnera znacznie zwiększyła swoją obecność w kilku krajach Afryki. Rosyjscy najemnicy zaangażowali się w wiele konfliktów, starając się poszerzyć wpływy. Jednym z ich głównych zadań miała być walka z terroryzmem. Przeprowadzone analizy, w ramach których autor wykorzystał metody jakościowe i źródła odnoszące się do teoretycznego i praktycznego wymiaru omawianej problematyki, wskazują, że wagnerowcy pozorują działania, aby utrzymać swoją obecność wojskową na kontynencie afrykańskim. Intensyfikacja obecności Grupy Wagnera to długoterminowa strategia Kremla, który realizuje interesy dwutorowo – korzysta ze współpracy na poziomie państw i angażuje najemników. Do rozwoju współpracy z partnerami z Afryki dążą również kraje szeroko rozumianego Zachodu (członkowie Sojuszu Północnoatlantyckiego i Unii Europejskiej). O wpływy na kontynencie zamierzają walczyć także organizacje terrorystyczne. W związku z tym konieczne jest stałe monitorowanie proaktywnej polityki zagranicznej Rosji ukierunkowanej na rywalizację, gdyż ma ona wpływ na obecność w Afryce Polski i jej sojuszników.

Słowa kluczowe

Grupa Wagnera, Afryka, Rosja, terroryzm, antyterroryzm, najemnicy

Abstract

In recent years, the Wagner Group has significantly increased its presence in several African countries. Russian mercenaries have become involved in many conflicts in an effort to expand their influence. One of their main tasks was to be the fight against terrorism. The analyses carried out, in which the author used qualitative methods and sources relating to the theoretical and practical dimensions of the issue at hand, indicate that the Wagnerists have been posing as operations in order to maintain their military presence on the African continent. Intensifying the Wagner Group's presence is a long-term strategy of the Kremlin, which pursues interests along two tracks - benefiting from cooperation at the state level and engaging mercenaries. Countries of the wider West (members of the North Atlantic Alliance and the European Union) are also seeking to develop cooperation with African partners. Terrorist organisations also intend to fight for influence on the continent. In this regard, it is necessary to constantly monitor Russia's proactive foreign policy aimed at the rivalry as it affects the presence of Poland and its allies in Africa.

Keywords

Wagner Group, Africa, Russia, terrorism, anti-terrorism, mercenaries

Wprowadzenie

Grupa Wagnera została założona¹, za zgodą Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej, ok. 2010 r. przez Dmitrija Utkina i sfinansowana przez Jewgienija Prigożyna. Pierwszych najemników wysłano na misje zagraniczne w 2014 r. – na Krym i do Donbasu, a kolejnych w 2015 r. do Syrii². Strategia zaangażowania najemników za granicą miała poparcie Władimira Putina, a w następnych latach stała się ważną częścią polityki zagranicznej Federacji Rosyjskiej (FR). Grupę Wagnera (w znaczeniu prywatnej firmy wojskowej, ang. *Private Military Company*, PMC) należy postrzegać jako organizację, która jest narzędziem wykorzystywanym przez Rosję do realizowania w skali globalnej operacji o charakterze politycznym, militarnym i ekonomicznym.

¹ W opracowaniach są podawane różne informacje na temat powstania i organizacji Grupy Wagnera.

² Więcej o powstaniu Grupy Wagnera zob. Ch. Faulkner, *Undermining Democracy and Exploiting Clients: The Wagner Group's Nefarious Activities in Africa*, „CTC Sentinel” 2022, t. 15, nr 6, <https://ctc.westpoint.edu/wp-content/uploads/2022/06/CTC-SENTINEL-062022.pdf>, s. 29–31 [dostęp: 4 XII 2023].

W odróżnieniu od państw Europy Zachodniej Rosja nie ma negatywnego doświadczenia w zajmowaniu, zarówno politycznie, jak i gospodarczo, krajów afrykańskich (próbowała natomiast podporządkować sobie m.in. kraje Europy Środkowo-Wschodniej i narzucić im zależność oraz skolonizować Somaliland). Co więcej, w historii części państw Afryki zapisała się jako wspierająca ruchy narodowowyzwoleńcze. Obecnie działania podejmowane przez Rosję w Afryce mają charakter wielotorowy. Kreml dostarcza uzbrojenie, najemników i finansuje wydobywanie surowców naturalnych. Stosuje też lobbing polityczny, co przekłada się zarówno na osiągnięcie celów politycznych, jak i na konkretne korzyści finansowe, w tym przez stworzenie rynku zbytu dla rosyjskiego sprzętu.

Blisko 40 afrykańskich partnerów jest zainteresowanych zacieśnieniem współpracy z Moskwą w tak ważnym obszarze, jakim jest wojskowość³. Federacja Rosyjska jest liderem dostaw broni do Afryki, z udziałem w rynku wynoszącym 26% w przypadku zakupów dokonywanych przez państwa Afryki Subsaharyjskiej. Po uwzględnieniu krajów Maghrebu ten odsetek wzrasta do aż 40%⁴. Rosja dostarcza głównie broń raketową i artyleryjską, broń strzelecką oraz pojazdy opancerzone. Najważniejszymi odbiorcami z regionu Afryki Subsaharyjskiej są: Angola, Mali, Nigeria i Sudan.

W latach 2019–2023 Grupa Wagnera stała się ważnym instrumentem w rosyjskiej polityce zagranicznej, zwłaszcza w Afryce, gdzie Moskwa stara się poszerzać swoje wpływy i rywalizować z Zachodem. Aby ten cel osiągnąć, wagnerowcy nawiązali relacje z rządami wielu państw afrykańskich, oferując usługi wojskowe i zapewnienie bezpieczeństwa w zamian za koncesje wydobywcze i poszerzenie wpływów politycznych. Grupa nie jest jednak zainteresowana prawdziwym budowaniem potencjału obronnego czy walką z terroryzmem. Stara się przede wszystkim kapitalizować zyski i czerpać korzyści z przedłużającego się chaosu, aby utrzymać swoją obecność na kontynencie.

Najemnicy mogą zostać wykorzystani do utrzymania stanu bezpieczeństwa, ponieważ Grupa Wagnera ma doświadczenie wojskowe w Afryce,

³ A. Olech i in., *Militarne zaangażowanie Federacji Rosyjskiej w Afryce. Zawarte porozumienia i umowy*, Instytut Nowej Europy, 23 V 2023 r., <https://ine.org.pl/militarne-zaangazowanie-federacji-rosyjskiej-w-afryce-zawarte-porozumienia-i-umowy/> [dostęp: 23 V 2023].

⁴ M. Douet, *Russia overtakes China as leading arms seller in sub-Saharan Africa*, Le Monde, 28 III 2023 r., https://www.lemonde.fr/en/le-monde-africa/article/2023/03/28/russia-overtakes-china-as-leading-arms-seller-in-sub-saharan-africa_6021018_124.html [dostęp: 10 XII 2023].

zwłaszcza w zakresie ochrony osób i obiektów, a także jest w stanie sprawnie się przemieszczać oraz realizować operacje ad hoc. Co ważne, w przypadku współpracy z rosyjskim podmiotem nie ma obostrzeń w postaci spełnienia określonych warunków (np. istnienia rządu demokratycznego, przestrzegania praw człowieka), co jest wymagane przez organizacje międzynarodowe i kraje Zachodu. Ponadto wagnerowcy wspierają rządy lub przywódców junt po zamachach stanu. Perspektywa zmiany władzy i uzyskania wsparcia od rosyjskich najemników może kusić niektórych ludzi w niestabilnych krajach Afryki.

Problem badawczy

Grupę Wagnera można sklasyfikować jako podmiot paraprywatny z uwagi na jej bliskie powiązania z elitą polityczną Rosji i sposoby, na jakie Kreml wykorzystuje tę organizację w bezpośredniej polityce zagranicznej. Grupa nie jest zarejestrowaną organizacją ani nie funkcjonuje jako podmiot państwowy, przez co trudno określić, z jakiego rodzaju zagrożeniem należy walczyć. Została ona celowo wpleciona w złożoną sieć podmiotów gospodarczych i firm fasadowych (część ówczesnego komercyjnego imperium Prigożyna i osób związanych z rosyjskimi władzami), a także w równie złożoną sieć podmiotów rządowych. Wagnerowcy prowadzą nie tylko działania stricte wojskowe, lecz także m.in.: operacje informacyjne, szkolenia, transfery broni i środków finansowych, działania w cyberprzestrzeni, zapewniają też wsparcie logistyczne, ochronę firm i nadzór nad nimi.

W trakcie kwerendy naukowej autor artykułu stwierdził, że istnieje bardzo mało publikacji, zarówno w języku polskim, jak i angielskim, które szczegółowo traktowałyby o obecności i działaniach Grupy Wagnera w każdym z państw afrykańskich, a także przedstawiały, w jaki sposób przenika się problematyka terroryzmu i antyterroryzmu, gdyż Kreml wykorzystuje różne definicje tych zjawisk na rzecz własnych interesów, także w FR⁵. Autor zebrał dane na podstawie kilkuset polskich i zagranicznych artykułów, raportów, książek, doniesień medialnych, a także licznych materiałów uzyskanych w ramach kwerendy własnej.

⁵ A. Olech, *Ataki terrorystyczne w Federacji Rosyjskiej w XXI wieku*, „Nowa Polityka Wschodnia” 2019, nr 4 (23), s. 109–127.

W artykule nie ujęto zagadnienia obecności Grupy Wagnera w Syrii i w Ukrainie, ale autor ma świadomość, że są to ważne korpusy wagnerowców operujące na świecie. Nie przedstawiono również szczegółowego opisu organizacji terrorystycznych (grup, komórek, batalionów), tj. historii ich powstania, obecnie prezentowanych poglądów, reprezentowanej religii, planów ekspansji oraz zależności pomiędzy poszczególnymi organizacjami a państwami, w których operują⁶.

W wymiarze globalnym Grupa Wagnera mogła działać, w mniejszym lub większym zakresie, w ok. 30 państwach, m.in. w Europie Wschodniej (np. w Ukrainie), na Bliskim Wschodzie (np. w Syrii) i Ameryce Południowej (np. w Wenezueli), ale najbardziej widoczna jest jej obecność na kontynencie afrykańskim. To zaangażowanie, mające wpływ na sytuację wewnętrzną państw oraz na ich politykę zagraniczną, dotyczy przede wszystkim Mali, Burkina Faso, Libii, Republiki Środkowoafrykańskiej (RŚA) i Sudanu (rysunek 1). Wpływy wagnerowców na tym kontynencie sięgają jednak znacznie szerzej, o czym traktuje niniejsza analiza⁷.



Rysunek 1. Państwa w Afryce, w których działa bądź działała Grupa Wagnera.

Źródło: opracowanie własne.

⁶ Na ten temat zob. K. Izak, *Leksykon organizacji i ruchów islamistycznych*, Warszawa 2014.

⁷ Badania przeprowadzone na potrzeby niniejszego artykułu zostały zakończone 31 XII 2023 r.

Mali

Bamako zwróciło się do rosyjskich prywatnych firm wojskowych (głównie do Grupy Wagnera), aby zwiększyć poziom bezpieczeństwa, z uwagi na powtarzające się ataki grup terrorystycznych⁸, a także po to, aby ograniczyć w Mali wpływy Republiki Francuskiej. Przedstawiciele Grupy Wagnera lobbingsowali u malijskich władz tymczasowych już po podpisaniu przez nie w 2019 r. porozumienia obronnego z Moskwą. Do zacieśnienia współpracy doszło po puczu wojskowym w maju 2021 r., gdy do pełni władzy doszedł płk Assimi Goita.

Sytuacja w Mali jest trudna z uwagi na zaangażowanie kilku aktorów walczących o wpływy. Obecnie można wyróżnić trzy strony:

- 1) siły zbrojne Mali (Forces Armées Maliennes, FAMA) wspierane przez Niger i Burkina Faso w ramach Sojuszu Państw Sahelu⁹, Grupę Wagnera oraz niektóre tuareskie ugrupowania;
- 2) milicje i grupy zbrojne Tuaregów i Arabów działające w ramach koalicji zrzeszających organizacje tuareskie walczące o niepodległość Azawad¹⁰ [m.in. członkowie Stałych Ram Strategicznych (Cadre stratégique permanent) oraz Narodowego Ruchu Wyzwolenia Azawadu (Coordination des mouvements de l'Azawad, CMA)];
- 3) organizacje terrorystyczne aktywne m.in. w Mali, Burkina Faso i Nigrze¹¹, tj.: Grupa Wsparcia Islamu i Muzułmanów (Jama'at Nasr al-Islam wa al-Muslimin, JNIM) oraz tzw. Państwo Islamskie (Islamic State, Ad-Dawla al-Islamijja; Islamic State of Iraq and Syria,

⁸ J. Wójcik, *Ekspansja dżihadu w Afryce: z Sahelu ku południu*, „Układ Sił” 2020, nr 20.

⁹ Regionalna organizacja bezpieczeństwa zbiorowego (Alliance des États du Sahel), ale mająca aspiracje, aby współpracować także w wymiarze gospodarczym, stanowiąc przeciwwagę dla Wspólnoty Gospodarczej Państw Afryki Zachodniej (Economic Community of West African States).

¹⁰ Sytuacja na północy Mali miała się uspokoić po zawarciu porozumienia pokojowego w Algierze w 2015 r. między władzami centralnymi i separatystycznymi ugrupowaniami Tuaregów i Arabów. Jednak po latach te ugrupowania ponownie włączyły się do walk o ziemię i wpływy. W tym samym czasie działania podejmowane w ramach operacji MINUSMA i Barkhane nie były w stanie zatrzymać odrodzenia i ekspansji grup terrorystycznych powiązanych z Al-Kaidą i ISIS. Zob. J. Czerep, *Przyszłość misji ONZ w Afryce po wycofaniu MINUSMA z Mali*, PISM, 6 X 2023 r., <https://www.pism.pl/publikacje/przyszlosc-misji-onz-w-afryce-po-wycofaniu-minusma-z-mali> [dostęp: 2 XI 2023].

¹¹ K. Chesnutt, K. Zimmerman, *The State of al Qaeda and ISIS Around the World*, Critical Threats, 8 IX 2022 r., <https://www.criticalthreats.org/analysis/the-state-of-al-qaeda-and-isis-around-the-world> [dostęp: 5 XI 2023].

ISIS)¹² i jego komórki, m.in. Państwo Islamskie w Sahelu (Islamic State Sahel Province, ISSP; Sahil Wilajet ad-Dawla al-Islamijja) oraz Państwo Islamskie w Afryce Zachodniej (Islamic State West Africa Province, ISWAP)¹³.

Początek oficjalnego i w pełni militarnego zaangażowania Grupy Wagnera należy datować na grudzień 2021 r., gdy organizacja rozpoczęła budowę obozu tuż obok międzynarodowego lotniska Modibo Keita w Bamako, w nieznaczonej odległości od Airbase 101 – obiektu wojskowego używanego przez siły powietrzne Mali. W pierwszych miesiącach 2022 r. wagnerowcy podjęli operacje w środkowym Mali, a rosyjski personel rozlokował się także w Timbuktu, gdzie zajął dawne bazy francuskiej operacji Barkhane. Przybycie rosyjskich najemników przyspieszyło wycofanie się sił francuskich i sił innych krajów europejskich.

Za 10,8 mln dolarów miesięcznej opłaty oraz koncesje na wydobycie w kopalniach złota wagnerowcy zapewniają malijskiej juncie bezpieczeństwo oraz szkolenia, a także angażują się militarnie, aby walczyć z dżihadystami. Na początku 2024 r. w Mali działa ok. 2000 rosyjskich najemników. Dokładne oszacowanie ich liczby jest trudne, gdyż Rosjanie docierają do tego kraju z pominięciem Bamako. Większość rosyjskich samolotów ląduje w Gao i Timbuktu, a wagnerowcy są też wysyłani na wschód kraju, do Menaiki. Ich główna aktywność polega na wspieraniu malijskiej armii w próbach przejęcia kontroli nad północnymi terytoriami państwa, od lat zdominowanymi głównie przez tuareskich separatystów¹⁴. Zbrojne potyczki, w jakie są zaangażowani najemnicy wspierający malijską armię, dotyczą prób przejęcia strategicznych miast (m.in. Kidalu) oraz baz wojskowych (w których stacjonowały wcześniej siły Organizacji Narodów Zjednoczonych) na północy kraju¹⁵, a w mniejszym stopniu walk z ugrupowaniami terrorystycznymi¹⁶.

¹² J. Czerep, *Afryka Subsaharyjska w strategii tzw. Państwa Islamskiego*, PISM, 1 VIII 2022 r., <https://www.pism.pl/publikacje/afryka-subsaharyjska-w-strategii-tzw-panstwa-islamskiego> [dostęp: 2 XI 2023].

¹³ Al-Kaida i ISIS są ze sobą skonfliktowane. Niejednokrotnie operują na tym samym terytorium i starają się rekrutować członków spośród tych samych społeczności.

¹⁴ Tuarescy separatyści również mają sprzeczne interesy wewnątrz społeczności, plemion i klanów. Zob. M. Shurkin (@MichaelShurkin), X, 22 XI 2023 r., <https://twitter.com/MichaelShurkin/status/1727337675806650866> [dostęp: 22 XI 2023].

¹⁵ K. Gadera, *Mali: chaotyczny koniec MINUSMA, Azawad znów walczy o niepodległość*, Konflikty.pl, 9 XI 2023 r., <https://www.konflikty.pl/aktualnosci/wiadomosci/mali-azawad-niepodleglosc/> [dostęp: 13 XI 2023].

¹⁶ Pod koniec października 2023 r. członkom misji ONZ opuszczającym kraj nie wydano pozwolenia na transport swoich żołnierzy drogą powietrzną z bazy w Kidalu. Z tego powodu

W ramach budowania potencjału finansowego Grupa Wagnera wykorzystuje obecność w Mali do kontrolowania sektorów: transportowego, rolniczego i wydobywczego. Pobiera opłaty i cła, aby finansować swoich najemników. Podobnie jak w innych państwach Afryki malijskie władze oraz krajowe wojsko akceptują zbrodnie popełniane przez wagnerowców na ludności cywilnej lub też celowo ich nie dostrzegają¹⁷.

Należy podkreślić, że po ponad dwóch latach od przybycia rosyjskich najemników do Mali pogorszyła się sytuacja bezpieczeństwa w tym kraju. Pomimo walk między Al-Kaidą¹⁸ a oddziałami Państwa Islamskiego w Sahelu obie te grupy terrorystyczne łączą swoje możliwości i angażują w działania mniejsze grupy terrorystyczne i rebelianckie, co pozwala im na znaczne powiększenie terytorium działań. Konflikt rozprzestrzenia się na cały region Sahelu i stanowi zagrożenie dla państw położonych w Zatoce Gwinejskiej. Jednocześnie w regionie silną pozycję utrzymuje JNIM, której komórki są aktywne w Burkina Faso, Beninie i Togo.

Grupa Wagnera nigdy nie działała w Mali samodzielnie i logistycznie jest całkowicie zależna od gospodarzy, czyli malijskiej armii. W przeciwieństwie do wagnerowców Francja miała wieloletnie doświadczenie w aktywności w tym regionie oraz dysponowała bardzo dobrym wyposażeniem wojskowym. Współpracowała przy tym z koalicją państw w ramach Barkhane i Takuba Task Force. Zdolności rosyjskich najemników w porównaniu z działaniami kierowanymi przez Paryż są niewielkie. Francuskie wojska były wyspecjalizowane w prowadzonych z powietrza operacjach polegających na neutralizowaniu statków i obiektów powietrznych należących do organizacji terrorystycznych.

Wszelkie działania malijskiej junty, wspierane przez Grupę Wagnera, przeciwko ruchom na rzecz niepodległego Azawadu są z uwagą obserwowane przez Algierię. Istnieją obawy ze strony administracji prezydenta Abdelmadjida Tebboune'a, że ponowny konflikt spowoduje napływ tysięcy uchodźców przez 1300-kilometrową granicę. Ponadto zaangażowanie Mali

żołnierze (m.in. z Czadu, Gwinei, Egiptu, Nepalu, Kambodży i Bangladeszu) wyruszyli w 350-kilometrową podróż drogową do Gao. Konwój składający się z prawie 850 pojazdów został wielokrotnie zaatakowany. Baza sił MINUSMA w Kidalu początkowo przypadła CMA, a następnie w krótkim czasie została przejęta przez wojska malijskie oraz wagnerowców.

¹⁷ Ch. Faulkner, *Undermining Democracy...*, s. 21; P. Wójcik (@SaladinAlDronni), X, 7 XI 2023 r., <https://twitter.com/SaladinAlDronni/status/1721821654660092201> [dostęp: 28 XI 2023].

¹⁸ Już w marcu 2017 r. Al-Kaida zjednoczyła inne grupy w ramach JNIM i nadal rozwija swój potencjał.

w walkę z milicjami i grupami zbrojnymi Tuaregów i Arabów powoduje, że malijska junta traci z oczu rosnące zagrożenie terrorystyczne. Wkrótce może być za późno, aby je skutecznie neutralizować¹⁹. Już pod koniec 2023 r. pojawiły się informacje, że część uzbrojenia dla Tuaregów i Arabów trafia do Mali z terytorium Algierii, co dodatkowo zaognia sytuację. Kolejnym etapem ochładzania relacji jest odwołanie przez obie strony ambasadorów i zacieśnienie stosunków Maroka z Mali, Burkina Faso i Nigrem²⁰.

Grupa Wagnera nie będzie w stanie wesprzeć sił zbrojnych Mali, aby w pełni przeciwstawić się organizacjom terrorystycznym oraz grupom Tuaregów i Arabów z regionu. Malijska junta musi działać jednocześnie na co najmniej dwóch frontach. Realne byłoby utrzymanie części terytoriów, ale większe sukcesy wymagałyby dużych dostaw uzbrojenia bezpośrednio z Rosji, a także oddelegowania do Mali co najmniej kilkuset żołnierzy. Federacja Rosyjska z uwagi na konflikt w Ukrainie oraz zaangażowanie w innych regionach Afryki i Bliskiego Wschodu nie może sobie na to pozwolić. Moskwa będzie zatem częścią tłącego się konfliktu, a w tym samym czasie będzie maksymalnie drenować Mali finansowo, aby uzyskać środki na budowanie swojej obecności wojskowej w Sahelu.

Burkina Faso i Niger

Grupa Wagnera została zidentyfikowana na terytorium Burkina Faso w listopadzie 2023 r. Pierwszy transport (20 żołnierzy) przybył do stolicy kraju samolotem Il-76 należącym do rosyjskich sił powietrznych. Od próby zamachu we wrześniu 2023 r. prezydent Ibrahim Traoré obawiał się utraty swojego reżimu, dlatego zwrócił się o wsparcie do Rosji²¹. To potwierdza, że jednym z głównych zadań wagnerowców jest ochrona wyższych rangą przedstawicieli władzy, zwłaszcza prezydenta (podobnie jak w RŚA).

¹⁹ *Much ado about Kidal*, Africa Confidential, 30 XI 2023 r., https://www.africa-confidential.com/article/id/14715/Much_ado_about_Kidal [dostęp: 30 XI 2023].

²⁰ F. Bobin, *Coup de froid dans les relations entre l'Algérie et le Mali*, Le Monde, 27 XII 2023 r., https://www.lemonde.fr/afrique/article/2023/12/27/coup-de-froid-dans-les-relations-entre-l-algerie-et-le-mali_6207961_3212.html?fbclid=IwAR0ZDmZbfg7Wz-a4vIf4pVoLJzi1MmsUqe5LpaYFGYx85_966-Y9yrQ4Y [dostęp: 27 XII 2023].

²¹ B. Roger, *Au Burkina Faso, des militaires russes pour protéger Ibrahim Traoré?*, jeuneafrique, 17 XI 2023 r., <https://www.jeuneafrique.com/1503219/politique/au-burkina-faso-des-militaires-russes-pour-protoger-ibrahim-traore/> [dostęp: 10 XII 2023].

W Burkina Faso źródłem zagrożenia terrorystycznego jest ugrupowanie dżihadystyczne Ansar al-Islam związane z JNIM. W jego szeregach są głównie zradykalizowani Fulanie (mieszkający na północy i wschodzie kraju) sprzeciwiający się dominacji ludu Mossi (najliczniejszej grupy etnicznej Burkina Faso).

Scenariusz, który zaistniał w Mali, nie został zrealizowany (do początku 2024 r.) w Burkina Faso, chociaż Rosja miała taki zamysł. Władze w Wagadugu interesuje przede wszystkim zwiększanie własnych zdolności do walki z terroryzmem oraz rozwijanie służb antyterrorystycznych. To oznacza, że realne są wspólne ćwiczenia rosyjsko-burkińskie, zakup zagranicznego uzbrojenia oraz międzynarodowe działania w walce z terrorystami (grupami rebeliantów). Burkina Faso nie chce jednak zapraszać dużej grupy wagnerowców. Rosyjscy najemnicy mają wesprzeć konsolidację władzy przez burkińską juntę.

Analizowana jest również obecność wagnerowców w Nigrze, ponieważ 26 lipca 2023 r. gen. Abdourahamane Tchiani dokonał zamachu stanu, odsuwając od władzy prozachodniego (ściśle współpracującego z Francją i Stanami Zjednoczonymi) prezydenta Mohameda Bazouma. Przez ostatnie lata Niger stanowił źródło stabilizacji w regionie Sahelu, dlatego nagły zwrot w kierunku Rosji był zaskoczeniem.

Zmiana władzy w Nigrze spowodowała, że wstrzymano wszelkie działania na rzecz budowania odporności na ataki grup rebeliantów, jak również operacje przeciw grupom terrorystycznym. Utrzymywane przez USA (ok. 1100 żołnierzy) i Francję (ok. 1500 żołnierzy)²² wsparcie antyterrorystyczne (np. przy wykorzystaniu bazy lotniczej w Agadez – kluczowej dla operacji dronów czy centrum wywiadowczego w stolicy kraju Niamey), a także szkolenie lokalnych wojsk stanowiły fundament w walce z terroryzmem w Sahelu. Głównymi przeciwnikami byli – podobnie jak w Mali i Burkina Faso – terroryści z JNIM, ISSP, ISWAP oraz częściowo z Boko Haram. Ostatecznie Niger opuścili wszyscy francuscy żołnierze, a francuska ambasada przestała funkcjonować.

Pod koniec lipca 2023 r., kilka dni po zamachu stanu, przedstawiciele Grupy Wagnera pojawili się w Niamey. Junta w Nigrze zdecydowała jednak, że zamiast zacieśniać relacje z wagnerowcami, od razu zbliży się do FR. Dnia 4 grudnia 2023 r. oba państwa podpisały porozumienie dotyczące umocnienia współpracy wojskowej. Niger ostatecznie wybrał Rosję, ale nadal

²² W Nigrze angażowały się także Belgia, Kanada, Niemcy, Włochy i Australia.

pozostają w nim amerykańskie wojska, co pozwala mieć nikłą nadzieję na współpracę Zachodu z tym krajem.

W kontekście sytuacji w Sahelu – po zamachach stanu w Mali, Burkina Faso, Nigrze i Sudanie pojawiają się informacje, że Grupa Wagnera współpracuje z rebeliantami z Czadu, aby obalić obecnego prezydenta tego kraju²³. To również zagraża bezpieczeństwu, ponieważ część francuskich żołnierzy z Nigru udała się do Czadu, a kraje UE planują udzielić wsparcia władzom w Ndżamenie, m.in. Węgry wysyłają kontyngent liczący do 400 żołnierzy.

Chociaż aktywność wagnerowców w Burkina Faso na początku była niewielka, to ich pojawienie się okazało się preludium do rozwoju współpracy. W 2024 r. zwiększono ich liczebność przez wysłanie kolejnych 100 najemników. Jeśli FR uzna, że chce budować swój potencjał w tym regionie, to obecność w Burkina Faso może zmienić się w przyczółek dla rosyjskich najemników.

Libia

Współcześnie Libia to kraj podzielony, pozbawiony jednego aparatu politycznego, umożliwiającego spójne administrowanie państwem i prowadzenie polityki zagranicznej. Z uwagi na rywalizujące ośrodki władzy, zaangażowanie innych państw, a także aktywność grup terrorystycznych i najemników, w tym Grupy Wagnera, niemożliwe jest wyłonienie wspólnego rządu (o co usilnie zabiegają ONZ i USA), który pozwoliłby wyjść z kryzysu oraz zatrzymać katastrofę humanitarną, jaka dotyka Libijczyków oraz osoby migrujące przez ten kraj.

Po zakwestionowanych wyborach parlamentarnych w 2014 r. kraj podzielił się na dwa obszary z konkurującymi ze sobą ośrodkami władzy – Wysoką Radę Państwa (High Council of State, HCS) z siedzibą w Trypolisie w zachodniej Libii oraz Izbę Reprezentantów (House of Representatives, HoR) z siedzibą w Tobruku we wschodniej części kraju. Dzięki zabiegom politycznym pod egidą ONZ w 2020 r. zawarto zawieszenie broni, które częściowo jest przestrzegane do dziś²⁴.

²³ W. Rampe, *What Is Russia's Wagner Group Doing in Africa?*, Council on Foreign Relations, 23 V 2023 r., <https://www.cfr.org/in-brief/what-russias-wagner-group-doing-africa> [dostęp: 21 XII 2023].

²⁴ Zawieszenie broni w październiku 2020 r. znacznie zmniejszyło zaangażowanie Grupy Wagnera w Libii, dlatego część personelu przerzucono do Mali i Ukrainy.

Izba Reprezentantów ze wschodniej części Libii wykreowała i popiera Rząd Stabilności Narodowej (Government of National Stability, GNS) oraz otrzymuje wsparcie od Libijskiej Armii Narodowej (Libyan National Army, LNA) dowodzonej przez gen. Khalifę Haftara (na jego zaproszenie do Libii przybyli wagnerowcy). Rywalami politycznymi GNS i HoR są Rząd Jedności Narodowej (Government of National Unity, GNU) i HCS, jednak relacje między dwoma ostatnimi nie są harmonijne. Ta tzw. wielka piątka jest odpowiedzialna za sytuację w Libii, gdzie nadal daleko jest do zawarcia porozumienia, które pozwoliłoby zakończyć konflikt. W tym chaotycznym środowisku swoją pozycję próbuje zaznaczyć Grupa Wagnera.

Wagnerowcy pojawili się w Libii w 2015 r. wraz z rosyjskimi siłami specjalnymi, wspieranymi także przez inną rosyjską grupę najemników – Rossiskie System Bezopasnosti. Grupa Wagnera, zachęcona przez gen. Haftara, wzmogła aktywność pod koniec 2018 r., a do połowy 2019 r. stała się w pełni zaangażowanym uczestnikiem walk. Wspierała m.in. atak LNA na Trypolis przeciwko Rządowi Porozumienia Narodowego (Government of National Accord) uznanemu przez ONZ²⁵.

Obecnie w Libii przebywa maksymalnie 2000 najemników pracujących dla Grupy Wagnera²⁶. Są wyposażeni m.in. w pojazdy opancerzone, systemy obrony powietrznej, sprzęt do walki elektronicznej, przeciwpancerne pociski kierowane, samoloty bojowe oraz drony. W Libii, będącej czołowym producentem ropy naftowej na kontynencie, działania rosyjskich najemników koncentrują się na dostępie zarówno do tego surowca, jak i do złóż gazu²⁷.

W połowie 2023 r. gen. Haftar groził podjęciem działań wojennych, jeśli dochody z ropy naftowej nie zostaną sprawiedliwie podzielone. W jego ocenie profity z tego surowca są w większej części przekazywane Rządowi Porozumienia Narodowego, mimo że ropę wydobywa się głównie na polach położonych na wschodzie kraju²⁸. Rosja robi wiele, aby przy wsparciu

²⁵ Ch. Faulkner, *Undermining Democracy...*, s. 30.

²⁶ W szczytowym momencie obecności zadania na terytorium Libii realizowało co najmniej 2500 najemników powiązanych z Grupą Wagnera.

²⁷ Gospodarka Libii jest bardzo mocno uzależniona, aż w ok. 85%, od produkcji węglowodorów.

²⁸ P. Wintour, *Fears for Libyan oil production amid military threats*, The Guardian, 4 VII 2023 r., <https://www.theguardian.com/world/2023/jul/04/fears-for-libyan-oil-production-amid-military-action-threats> [dostęp: 13 XII 2023].

Grupy Wagnera zyskać wpływy, i w tym celu wykorzystuje własne porozumienia energetyczne i zaangażowanie rosyjskich spółek²⁹.

Walka z terroryzmem w żadnym momencie nie była celem obecności Grupy Wagnera w Libii, w przeciwieństwie do jej aktywności w Syrii, Mali czy Mozambiku. Wynika to z tego, że najsilniejszą pozycję Państwo Islamskie (m.in. Islamic State – Libya Province) miało w Libii w latach 2014–2016, a w 2018 r. utraciło duże terytoria³⁰ (jeszcze przed przybyciem do kraju wagnerowców³¹).

Należy wskazać, że metody wykorzystywane podczas operacji wojskowych realizowanych przez Grupę Wagnera również w Libii wpisują się w definicję terroryzmu. Jest to podmiot zewnętrzny, który próbuje zdestabilizować porządek w kraju, angażuje się w działania o charakterze zbrojnym i dokonuje ataków terrorystycznych. Żołnierze Grupy Wagnera, którzy walczyli u boku LNA podczas ataków na Trypolis w 2019 r., zostali oskarżeni o dokonywanie nieuzasadnionych zabójstw i podkładania min lądowych na obszarach zamieszkałych przez cywili³².

Obecnie FR podejmuje działania na rzecz wzmocnienia swojej obecności militarnej w Libii. Po wizycie rosyjskiego wiceministra obrony Junus-Bieka Jewkurowa w Bengazi w sierpniu 2023 r., do której doszło z inicjatywy gen. Haftara, ogłoszono plan utworzenia Rosyjskiego Korpusu Wojskowego w Afryce. Zgodnie z nim żołnierze realizowaliby operacje wojskowe na całym kontynencie afrykańskim na rzecz współpracy między Rosją a wybranymi państwami (reżimami/rządami)³³. Jednocześnie Moskwa utrzymuje kontakt z rządem w Trypolisie, aby podtrzymać szansę na kooperację, jeśli doszłoby do znacznego osłabienia sił Grupy Wagnera i gen. Haftara.

²⁹ G. Kuczyński, *Russia's Tatneft Discovers New Oil Field in Libya*, Warsaw Institute, 25 V 2023 r., <https://warsawinstitute.org/russias-tatneft-discovers-new-oil-field-in-libya/> [dostęp: 21 XII 2023].

³⁰ Center for Preventive Action, *Civil Conflict in Libya?*, Council on Foreign Relations, 19 IX 2023 r., <https://www.cfr.org/global-conflict-tracker/conflict/civil-war-libya> [dostęp: 23 XI 2023].

³¹ Prawdą jest, że część najemników Grupy Wagnera działała wcześniej w Syrii, gdzie walczyli przeciwko Państwu Islamskiemu, ale w Libii mieli oni inne zadania.

³² W. Rampe, *What Is Russia's Wagner Group Doing in Africa?*...

³³ *Russia works with Libya on the creation of a military corps in Africa*, Agenzia Nova, 17 XI 2023 r., <https://www.agenzianova.com/en/news/la-russia-lavora-con-la-libia-alla-creazione-di-un-corpo-militare-in-africa/> [dostęp: 23 XI 2023].

Mozambik

Grupa Wagnera pojawiła się w Mozambiku w związku z rosnącą od 2017 r. aktywnością grup terrorystycznych powiązanych z Państwem Islamskim, operujących w regionie Cabo Delgado graniczącym z Tanzanią. Główną przyczyną pogarszającej się sytuacji bezpieczeństwa w kraju była radykalizacja ludności marginalizowanej ekonomicznie (ponad 60% mieszkańców Cabo Delgado to muzułmanie, a w Mozambiku większość stanowią chrześcijanie) oraz zaangażowanie ekstremistów m.in. z ugrupowania ISIS-Mozambik³⁴, znanego też jako Ansar al-Sunna³⁵ (jak również Ahl-al-Sunna) i lokalnie jako Al-Shabaab w Mozambiku³⁶. Ekstremiści chcieli odseparowania regionu od kraju, kontroli szlaków narkotykowych oraz zysków z odkrytych złóż surowców. Rosnące napięcia w regionie doprowadziły do wybuchu powstania³⁷. Armia i służby mozambijskie nie mogły sobie poradzić z ugrupowaniami ekstremistycznymi i potrzebowały wsparcia zagranicznych sił³⁸.

We wrześniu 2019 r. do Mozambiku przybyło 200 rosyjskich najemników, którzy mieli na wyposażeniu śmigłowce szturmowe, drony oraz sprzęt do walki w terenie. Grupie Wagnera powierzono zadanie szkolenia i dowodzenia lokalnymi siłami zbrojnymi. Jej członkowie nie potrafili jednak odnaleźć się w gęsto zalesionym terenie, nie układała się współpraca z mozambijskimi żołnierzami, posiadany sprzęt okazał się mało przydatny w walce z terrorystami koncentrującymi się na zasadzkach i nieregularnych atakach, a ponadto zawiodło rozpoznanie wroga. W ciągu pierwszych tygodni zginęło kilkunastu wagnerowców.

³⁴ *ISIS-Mozambique*, Counter Terrorism Guide, listopad 2022 r., https://www.dni.gov/nctc/ftos/isis_mozambique_fto.html [dostęp: 12 XII 2023].

³⁵ Działające również z Madinat at-Tawhid wa al-Muwahidin z Demokratycznej Republiki Konga (DR Konga).

³⁶ *State Department Terrorist Designations of ISIS Affiliates and Leaders in the Democratic Republic of the Congo and Mozambique*, U.S. Department of State, 10 III 2023 r., <https://www.state.gov/state-department-terrorist-designations-of-isis-affiliates-and-leaders-in-the-democratic-republic-of-the-congo-and-mozambique/> [dostęp: 12 XII 2023].

³⁷ J. Penney, *Rwanda Helped Oust Jihadists in Mozambique. Can This Model Work in West Africa?*, PassBlue, 16 VIII 2023 r., <https://www.passblue.com/2023/08/16/rwanda-helped-oust-jihadists-in-mozambique-can-it-work-as-a-counterinsurgency-model-in-west-africa> [dostęp: 14 XII 2023].

³⁸ J. Czerep, *Nowy front dżihadu w Mozambiku*, PISM, 22 IX 2020 r., https://pism.pl/publikacje/Nowy_front_dzihadu_w_Mozambiku [dostęp: 21 XI 2023].

Na początku 2020 r. sytuacja w Cabo Delgado była zła – grupy terrorystyczne zyskały znaczną przewagę. Utrata dużej części terytorium i kolejne nieudane operacje doprowadziły do tego, że zrezygnowano ze współpracy z wagnerowcami. W marcu 2020 r. opuścili oni Mozambik, zaledwie pół roku od przybycia. W ich miejsce pojawili się inni najemnicy z prywatnej firmy wojskowej Dyck Advisory Group. Tym samym działalność Grupy Wagnera w Mozambiku była krótkotrwała i można ją uznać za porażkę. To kolejny przykład potwierdzający, że rosyjscy najemnicy opuszczają każdy kraj, w którym postrzegają przeciwnika jako zbyt wymagającego, a ich obecność nie jest opłacalna ani politycznie, ani finansowo. Federacja Rosyjska zignorowała ucieczkę wagnerowców i nie podjęła żadnych działań na rzecz poprawienia i wzmocnienia relacji dwustronnych z Mozambikiem.

Sudan

Grupa Wagnera jest obecna w Sudanie od 2017 r., a w obliczu nasilającej się walki o władzę w kraju działa bezpośrednio na rzecz interesów Rosji³⁹. Współpraca między tymi dwoma państwami zacieśniała się od 2015 r. Kluczowym momentem było spotkanie w 2017 r. ówczesnego prezydenta Omara Al-Bashira z Władimirem Putinem, podczas którego rządzący Sudanem poprosił o wsparcie. Federacja Rosyjska była zainteresowana współpracą energetyczną i transportową przy wykorzystaniu cieśniny Bab al-Mandab⁴⁰. Podpisano wówczas porozumienia, a także podjęto rozmowy, m.in. w sprawie utworzenia rosyjskiej bazy morskiej w Port Sudan na Morzu Czerwonym. Oprócz wspomnianych w 2017 r. sygnowano umowy koncesyjne na wydobycie złota.

W kwietniu 2023 r. doszło w Sudanie do kolejnego zamachu stanu. Zarówno Prigożyn, jak i Grupa Wagnera nie miałyby oporów, aby wesprzeć gen. Abdela Fattaha al-Burhana i Sudańskie Siły Zbrojne (Sudanese Armed Forces, SAF), ale podtrzymali działania na rzecz gen. Mohameda Hamdana

³⁹ I. Sheludkova, *Why is Russia's Wagner Group in Sudan, and what does it have to do with the war in Ukraine?*, EuroNews, 27 IV 2023 r., <https://www.euronews.com/2023/04/27/why-is-russias-wagner-group-in-sudan-and-what-does-it-have-to-do-with-the-war-in-ukraine> [dostęp: 16 XI 2023].

⁴⁰ *Sudan's President Bashir asks Putin for 'protection' from 'aggressive' US*, France24, 23 XI 2017 r., <https://www.france24.com/en/20171123-sudan-president-bashir-asks-putin-protection-aggressive-us> [dostęp: 16 XI 2023].

Dagalo (ps. „Hemeti”, „Hemedti”) i Sił Szybkiego Wsparcia (Rapid Support Forces, RSF)⁴¹, z którymi już wcześniej utrzymywali współpracę szkoleniową, a także przekazywali sprzęt (m.in. amunicję, drony i rakiety)⁴².

Obecnie FR (jako państwo i przy wsparciu czołowych polityków Kremla) chce utrzymać powiązania z Al-Burhanem i SAF na wypadek, gdyby przypadło im zwycięstwo w wojnie domowej. Jednocześnie Rosjanie mogą za kulisami faworyzować RSF, wykorzystując w tym celu Grupę Wagnera, ze względu na sytuację w Libii i dobre relacje Haftara i Hemettiego⁴³, jak również wsparcie⁴⁴ udzielane im obu przez Zjednoczone Emiraty Arabskie⁴⁵.

Celem Grupy Wagnera w Sudanie (gdzie obecnie przebywa 500–700 najemników) jest zapewnienie dostępu do surowców, które następnie Rosja wykorzysta do finansowania wojny w Ukrainie oraz udziału w innych teatrach działań. Pozyskiwanie złota z Sudanu, który jest czołowym (w pierwszej trójce⁴⁶) producentem tego minerału w Afryce, nie jest trudne z uwagi na niestabilną sytuację w tym kraju i łatwość kontroli wybranych kopalni.

Utrzymując się załamanie władzy w Sudanie i przedłużające się walki oznaczają dla Moskwy żmudne odbudowywanie współpracy. Istnieje ryzyko, że stanięcie po stronie RSF nie przyniesie efektów i Kreml nie zrealizuje swoich planów ekspansji w Afryce Wschodniej. Opowiedzenie się po jednej stronie oznacza straty nie tylko polityczne i militarne, lecz także gospodarcze. Wyjście z Sudanu nie będzie dla FR korzystne, a utrzymanie obecności jest niezbędne, jeśli Rosja nadal chce walczyć o swoją pozycję w regionie.

⁴¹ Na początku konfliktu Prigożyn wyraził chęć zaangażowania się w mediacje pokojowe z uwagi na dobre kontakty z obiema stronami konfliktu.

⁴² Jeszcze przed wybuchem konfliktu dostarczano broń dla RSF z wykorzystaniem lotniska Entebbe w Ugandzie, na które za pośrednictwem Grupy Wagnera trafiały dostawy z RŚA.

⁴³ G. Aftandilian, *The Fate of the Wagner Group in Syria, Libya, and Sudan*, Arab Center Washington DC, 18 VII 2023 r., <https://arabcenterdc.org/resource/the-fate-of-the-wagner-group-in-syria-libya-and-sudan/> [dostęp: 23 XI 2023].

⁴⁴ J. Czerep, *Perspektywy zakończenia wojny w Sudanie*, PISM, 25 V 2023 r., <https://pism.pl/publikacje/perspektywy-zakonczenia-wojny-w-sudanie> [dostęp: 23 XI 2023].

⁴⁵ Dla tego kraju dobre byłoby również odcięcie się od wagnerowców oraz zaprzestanie dostarczania broni dla RSF. Zjednoczone Emiraty Arabskie chcą podkreślić swoją pozycję na arenie międzynarodowej, organizując choćby COP28, a takimi działaniami jak w Sudanie podważają swój autorytet. Zob. E. Sirleaf, *UAE must cut ties with Sudan's war*, The Times, 27 XI 2023 r., <https://www.thetimes.co.uk/article/uae-must-cut-ties-with-sudans-war-czpw-pms2n> [dostęp: 27 XI 2023].

⁴⁶ M. Goosen, *Biggest Gold Producing Countries in Africa*, Energy Capital Power, 5 IX 2022 r., <https://energycapitalpower.com/biggest-gold-producing-countries-in-africa/> [dostęp: 25 XI 2023].

Można wskazać analogię do sytuacji w Libii, gdzie Moskwa wspomaga militarnie gen. Haftara, ale dba również o poprawne relacje z rządem w Trypolisie, gdyż jest on uznawany na arenie międzynarodowej. Tak samo wygląda sytuacja z Sudanem, w którym jest uznawany Al-Burhan. W przypadku jego zwycięstwa Grupa Wagnera zostałaby wypchnięta ze względu na współpracę z RSF.

Wątek ukraiński

Warto nadmienić, że rośnie liczba ujawnianych ataków ukraińskich sił specjalnych na pozycje najemników Grupy Wagnera w Sudanie. Priorytetem dla Ukrainy pozostaje nie tylko otwieranie w najbliższym czasie nowych placówek dyplomatycznych w Afryce⁴⁷, lecz także zwalczanie wagnerowców na całym kontynencie afrykańskim⁴⁸.

Warto zaznaczyć, że w 2024 r. (gdy Kijów ma prowadzić kontrofensywę militarną w kraju) rozpowszechnianie w mediach światowych ukraińskiego zaangażowania w Sudanie ma cele polityczne. Spotkanie prezydenta Wołodymyra Zełenskigo z Al-Burhanem 23 września 2023 r. na lotnisku Shannon w Irlandii było sygnałem wskazującym na wsparcie dla sudańskiego dowódcy⁴⁹.

Pojawiają się ponadto informacje, że ukraińscy żołnierze szkolą i doradzają tuareskim rebeliantom w Mali, którzy prowadzą działania zbrojne przeciwko prorosyjskiemu rządowi i stacjonującej tam Grupie Wagnera⁵⁰. Ukraina – przynajmniej w teorii – chciałaby rzucić wyzwanie FR, której obecność polityczna w Afryce jest znacząca. Nawet jeśli część państw wołałaby współpracę z Kijowem, to obawia się przeniesienia rywalizacji rosyjsko-ukraińskiej na kontynent afrykański.

⁴⁷ *Ukraine Expands Diplomatic Presence in Africa: New Embassy Launches in Ghana*, Kyiv Independent, 27 XII 2023 r., <https://www.kyivpost.com/post/26022/> [dostęp: 29 XII 2023].

⁴⁸ T. Eydoux, L. Savoye, *Quand les forces spéciales ukrainiennes combattent des mercenaires russes de Wagner au Soudan*, Le Monde, 19 XI 2023 r., https://www.lemonde.fr/videos/video/2023/11/19/quand-les-forces-speciales-ukrainiennes-combattent-des-mercenaires-russes-de-wagner-au-soudan_6201120_1669088.html [dostęp: 21 XI 2023].

⁴⁹ R. Black, *Zelensky meets Sudanese official during 'technical stopover' in Ireland*, Independent, 23 IX 2023 r., <https://www.independent.co.uk/news/uk/volodymyr-zelensky-north-america-ireland-joe-biden-department-of-foreign-affairs-b2417251.html> [dostęp: 10 XII 2023].

⁵⁰ S. Sadkiewicz (@StanSadkiewicz), X, 7 XI 2023 r., <https://twitter.com/StanSadkiewicz/status/1721882283916079351> [dostęp: 7 XI 2023].

Republika Środkowoafrykańska

Grupa Wagnera jest szczególnie aktywna w RŚA. Na terenie kraju przebywa ok. 1000 najemników⁵¹. Warto wskazać, że duża część członków grupy opuściła Afrykę, głównie RŚA, z powodu inwazji Rosji na Ukrainę, a kolejni – po buncie Prigożyna. Ich liczebność znacznie się zmniejszyła w porównaniu ze szczytowym momentem, kiedy w RŚA działało ponad 2500 wagnerowców⁵². Priorytetem, zwłaszcza na początku działalności, były szkolenia dla środkowoafrykańskich sił zbrojnych, przede wszystkim dla wojsk specjalnych. Wspólne ćwiczenia miały poprawić interoperacyjność krajowych wojsk i pozwolić na przeprowadzanie szybkich uderzeń na pozycje wroga, ponieważ RŚA zmaga się z obecnością grup rebeliantów.

Rosyjscy najemnicy prowadzą na terenie RŚA działania pozwalające im na uzyskanie znacznych korzyści majątkowych. Ochraniają kopalnie oraz mają prawa do wydobywania lub dystrybucji konkretnych surowców w zamian za świadczone usługi. Przez lata Grupa Wagnera zyskała w kraju mocną pozycję. Przede wszystkim dzięki wsparciu prezydenta Faustina-Archange Touadéry, który zaprosił najemników w 2018 r. (rozmowy trwały już w 2017 r., a pierwsze kontrakty podpisano z inną rosyjską grupą – Sewa Security Group⁵³).

Podobnie jak w innych krajach Afryki, w których wagnerowcy budują swoją pozycję, w RŚA wcześniej były obecne (od 2012 r.) wojska Republiki Francuskiej. W 2013 r. rozpoczęły one operację Sangaris, mającą na celu walkę z rebeliantami i terrorystami⁵⁴. W szczytowym okresie Francja rozmieściła w RŚA ok. 2500 żołnierzy, wspierając ok. 10 000 żołnierzy sił pokojowych ONZ w ramach misji MINUSCA⁵⁵. W 2016 r. siły francuskie

⁵¹ R. Chason, B. Debout, *In Wagner's largest African outpost, Russia looks to tighten its grip*, Washington Post, 18 IX 2023 r., <https://www.washingtonpost.com/world/2023/09/18/wagner-central-african-republic-touadera/> [dostęp: 5 XI 2023].

⁵² L. Serwat, *Moving out of the shadows: Shifts in Wagner Group Operations Around the World*, ACLED, 2 VIII 2023 r., https://acleddata.com/acleddatanew/wp-content/uploads/2023/08/ACLED_Report_Shifts-in-Wagner-Group-Operations-Around-the-World_2023.pdf [dostęp: 5 XI 2023].

⁵³ Sewa Security Group obsługiwała swoją spółkę Lobaye Invest SARLU realizującą kontrakty na wydobycie surowców.

⁵⁴ Rozpoczęta pod koniec 2013 r. operacja Sangaris była siódmą francuską interwencją wojskową w RŚA od czasu uzyskania przez ten kraj niepodległości w 1960 r. Jej oficjalne zakończenie Francja ogłosiła 30 października 2016 r.

⁵⁵ *France to end Central African Republic military mission in 2016*, France24, 30 III 2016 r., <https://www.france24.com/en/20160330-france-end-military-operations-central-african-republic/> [dostęp: 5 XI 2023].

ostatecznie wycofały się z tego kraju. W przeciwieństwie do Mali w RŚA misja ONZ jest realizowana, pomimo stałej obecności Grupy Wagnera, której najemnicy dokonują zbrodni na ludności cywilnej i pozostają bezkarni⁵⁶. Warto nadmienić, że w 2021 r. wagnerowcom postawiono pomnik w Bangi⁵⁷.

W obecnej sytuacji wojska francuskie nie wrócą do RŚA, głównie z powodu obecności wagnerowców. Dla Paryża relacja z Bangi nie jest jednak zupełnie stracona⁵⁸. Podobnie sprawę postrzega Waszyngton pozostający w kontakcie z administracją Touadéry, któremu oferuje współpracę w zakresie bezpieczeństwa⁵⁹. Rozmowy są prowadzone również z Bancroft Global Development – amerykańską prywatną firmą wojskową.

Rola Rwandy

W kontekście RŚA warto nadmienić o wojskowym zaangażowaniu Rwandyjczyków, którzy stanowią w tym kraju przeciwwagę dla Grupy Wagnera. To właśnie Kigali potrafiło poprawić poziom bezpieczeństwa w kilku regionach RŚA, wesprzeć reformę struktur bezpieczeństwa i przeprowadzić szkolenia dla grup antyterrorystycznych. Chociaż początkowo rosyjscy najemnicy współpracowali z rwandyjskimi żołnierzami, z którymi wspólnie walczyli z grupami rebeliantów, zwłaszcza w 2021 r., to od połowy 2022 r. (gdy Rosjanie zaczęli się mocniej angażować w RŚA, Sudanie i wspierać DR Konga, która pozostaje w konflikcie z Rwandą) coraz częściej dochodzi do napięć między nimi. Rywalizacja dotyczy przede wszystkim kontroli złóż surowców i działań na terenach objętych konfliktem. Kigali ma dobre relacje z Moskwą, ale nie chce być kojarzone z działaniami Grupy Wagnera. Obie grupy – teoretycznie – walczą z rebeliantami (terroryzmem), ale

⁵⁶ *Wagner Group Uses Mafia-Style Tactics to Dominate CAR's Diamond Sector*, ADF, 1 VIII 2023 r., <https://adf-magazine.com/2023/08/wagner-group-uses-mafia-style-tactics-to-dominate-cars-diamond-sector/> [dostęp: 25 XI 2023].

⁵⁷ W latach 2020–2023 Grupa Wagnera była zaangażowana w blisko 40% ataków, do których doszło podczas konfliktów rozgrywających się w RŚA.

⁵⁸ *Touadéra stirs the geopolitical cauldron*, Africa Confidential, 2 XI 2023 r., https://www.africa-confidential.com/article/id/14682/Touad%C3%A9ra_stirs_the_geopolitical_cauldron [dostęp: 5 XI 2023].

⁵⁹ E. Peltier, *Battle for Influence Rages in Heart of Wagner's Operations in Africa*, The New York Times, 26 XI 2023 r., <https://www.nytimes.com/2023/11/26/world/africa/wagner-russia-central-african-republic.html> [dostęp: 15 XII 2023].

jednocześnie rywalizują. Warto dodać, że obecnie to właśnie Rwanda ma najliczniejszy i najważniejszy kontyngent zagraniczny w ramach misji MINUSCA.

Partnerstwo RŚA–Rwanda przyniosło pozytywne skutki w kontekście walki z terroryzmem, ale spowodowało też, że w kraju pojawił się kolejny aktor zewnętrzny. Rwandyjczycy zaangażowali się w te same obszary, w jakich działa ekonomicznie Grupa Wagnera (m.in. sektor wydobywczy). Współpraca rosyjskich najemników z administracją RŚA jest bardzo dobra i Kreml nie zamierza dokonywać zmian politycznych w tym kraju (jak np. zrobił to w Syrii)⁶⁰. Dostrzega jednak rosnącą rolę Rwandy. Na tę chwilę Grupa Wagnera i wojska rwandyjskie akceptują swoją obecność w RŚA, ponieważ widzą płynące z tego korzyści. Relacje są jednak bardzo napięte i może dojść do konfliktu.

Demokratyczna Republika Konga i możliwa obecność rosyjskich najemników

Pojawiają się kolejne informacje o zaangażowaniu Grupy Wagnera w DR Konga⁶¹. Ma ona prowadzić skoordynowane działania wraz z siłami zbrojnymi Konga w pobliżu granicy z Ugandą. Wagnerowcy mają być też obecni w Kiwu Północnym w ramach przeciwdziałania Ruchowi 23 Marca (wspieranemu przez Kigali) oraz grupom terrorystycznym [m.in. Madina at Tauheed Wau Mujahedeen (znana również jako ISIS-DRC)⁶² wywodząca się z Allied Democratic Forces (ADF) powiązanej z Państwem Islamskim⁶³].

Grupa Wagnera jest kolejną organizacją, która mogłaby w dużym stopniu wesprzeć działania armii kongijskiej. Trzeba dodać, że rosyjscy najemnicy przebywający w DR Konga mogą korzystać ze wsparcia swoich stałych baz w RŚA. Obecnie Kongo potrzebuje dostaw uzbrojenia, a Rosja obiecała

⁶⁰ J. Czerep, A. Legucka, *Przyszłość „imperium” Prigożyna*, PISM, 17 VII 2023 r., <https://www.pism.pl/publikacje/przyszlosc-imperium-prigozyna> [dostęp: 16 XI 2023].

⁶¹ S. Schlindwein, *Are white mercenaries fighting in the DRC conflict?*, Deutsche Welle, 17 I 2023 r., <https://www.dw.com/en/are-white-mercenaries-fighting-in-the-drc-conflict/a-64407711> [dostęp: 16 XII 2023].

⁶² *Country Reports on Terrorism 2020: Democratic Republic of the Congo*, U.S. Department of State, <https://www.state.gov/reports/country-reports-on-terrorism-2020/democratic-republic-of-the-congo/> [dostęp: 16 XII 2023].

⁶³ *State Department Terrorist...*

pomoc w wyposażeniu w nowy sprzęt wojskowy, zwłaszcza w wozy opancerzone, czołgi, śmigłowce i samoloty bojowe.

Madagaskar

Budowanie przez Grupę Wagnera wpływów na Madagaskarze to dość unikalny przykład, gdyż była ona tam zaangażowana nie militarnie, lecz politycznie i ekonomicznie. W połowie 2018 r. do kraju przybyła grupa ekspertów politycznych z Rosji. Zapewnili oni wsparcie finansowe, ochronę oraz doradztwo osobom, które według Kremla powinny zwyciężyć w wyborach prezydenckich⁶⁴. Oprócz tego organizowali kampanie dezinformacyjne w mediach społecznościowych, wspierali protesty i angażowali niektóre media, co miało stworzyć wrażenie, że na Madagaskarze trwają spontaniczne kampanie wyborcze polityków. Malgaskie władze namierzyły zagrożenie i wydalili z kraju osoby ingerujące w wybory⁶⁵. Niemniej w marcu 2022 r. została podpisana umowa o współpracy wojskowej pomiędzy Madagaskarem a FR i na wyspie są dostrzegalne wpływy Kremla. To powoduje, że ryzyko zaangażowania rosyjskich najemników nadal jest tam wysokie.

Rosyjski terroryzm i antyterroryzm

Skuteczność Grupy Wagnera w walce z terroryzmem w Afryce jest bardzo dyskusyjna. Interwencje rosyjskich najemników w Mali nie przynoszą efektów i prowadzą do coraz większej liczby ataków terrorystycznych. Wskazuje się, że wagnerowcy nie mają motywacji, aby zakończyć konflikty, w których uczestniczą, ponieważ kierują się motywacją finansową. Nawet w przypadku zakończenia operacji lub osiągnięcia pokoju najemnicy wojskowi nie są jak rezerwiści, których angażuje się tylko wtedy, gdy się ich potrzebuje. Po zakończeniu operacji najemnicy nie integrują się i nie odbudowują

⁶⁴ *Master and Chef. How Evgeny Prigozhin led the Russian offensive in Africa*, The Proekt team, 14 III 2023 r., <https://www.proekt.media/en/article-en/evgeny-prigozhin-africa/> [dostęp: 5 XI 2023].

⁶⁵ A. Legucka, J. Czerep, *Wzrost zaangażowania Rosji w Afryce*, PISM, 20 XI 2019 r., https://pism.pl/publikacje/Wzrost_zaangazowania_Rosji_w_Afryce [dostęp: 16 XII 2023].

państwa, lecz szukają nowych pracodawców i możliwości zysku. Przedłużając się zwalczanie zagrożeń terrorystycznych to ich sposób na zarabianie⁶⁶.

Innym ważnym aspektem jest to, że FR może realizować działania określane jako terrorystyczne m.in. w Ukrainie i Syrii. W tym samym czasie jest utrzymywana aktywność Grupy Wagnera w Afryce, będąca przedłużeniem polityki zagranicznej Rosji. Kreml z jednej strony nadzoruje prywatne grupy najemników angażowane do walki z terroryzmem, a z drugiej obliguje rosyjskich żołnierzy do podejmowania działań o charakterze terrorystycznym.

Należy odnieść się do faktycznego poziomu zagrożenia terroryzmem w krajach, w których są obecni rosyjscy najemnicy. Grupy terrorystyczne w Sahelu i Rogu Afryki mają ogromne zdolności adaptacyjne⁶⁷. Przetrvanie Al-Kaidy przez ponad 30 lat, a także regularne rozwijanie nowych organizacji i grup (m.in. Państwo Islamskie i jego komórki) stanowią dowody na bardzo wysoki stopień odporności, właściwe planowanie i długofalową strategię tych grup. Terrorysty w Afryce, przenikając się z rebeliantami, są niezwykle trudnym przeciwnikiem, którego żadna koalicja (także ta krajów Zachodu) nie zdołała pokonać. Większość państw, w których działają wagnerowcy, jest w bardzo wysokim stopniu zagrożona terroryzmem i jego wpływem na bezpieczeństwo państwa⁶⁸.

Kierunek współpracy na rzecz walki z terroryzmem powinny wyznaczać kraje Afryki, a ich partnerzy (szeroko rozumiany Zachód) powinni im w tym pomagać. Nie ma „jednej Afryki”, także w wymiarze zwalczania terroryzmu, ponieważ jest tak wiele cech szczególnych, jak wiele jest państw na tym kontynencie. Nie można porównywać walki z terroryzmem w Sahelu z tą prowadzoną w Mozambiku. W przeciwdziałaniu terrorystom i rebeliantom Rosja nie jest w stanie zapewnić krajom afrykańskim skutecznego wsparcia finansowego, zbrojeniowego, technologicznego czy też – jak opisano w artykule – przez delegowanie Grupy Wagnera.

⁶⁶ T. Mehra, M. Demuynck, *Raising the stakes against the Wagner Group: From mercenaries to a designated terrorist group?*, ICCT, 17 I 2023 r., <https://www.icct.nl/publication/raising-stakes-against-wagner-group-mercenaries-designated-terrorist-group> [dostęp: 16 XII 2023].

⁶⁷ J. Warner, *A View from the CT Foxhole: Idriss Mounir Lallali, Deputy Director, African Centre for the Study and Research on Terrorism (ACSRT)*, „CTC Sentinel” 2021, t. 14, nr 5, <https://ctc.westpoint.edu/a-view-from-the-ct-foxhole-idriss-mounir-lallali-deputy-director-african-centre-for-the-study-and-research-on-terrorism-acsr/>, s. 12–13 [dostęp: 16 XII 2023].

⁶⁸ *Global Terrorism Index 2023: Measuring the Impact of Terrorism*, Institute for Economics & Peace, Sydney, marzec 2023 r.

Terroryzm pozostaje w Afryce ogromnym problemem. Obecność na kontynencie Grupy Wagnera, która dobrze wykorzystuje swoją imitowaną specjalizację, tj. walkę z terroryzmem, aby zaangażować się w wybranym państwie, i która dąży do przeciwstawienia się krajom Zachodu, powoduje, że w nadchodzących latach to zagrożenie nie zniknie. Jeśli jednak wagnerowcy lub inni rosyjscy najemnicy będą postrzegani jako niekompetentni lub niewiarygodni z powodu braku realnego wpływu na poprawę sytuacji bezpieczeństwa, to kraje Afryki będą rezygnować z ich usług⁶⁹.

Zakończenie i wnioski

Kreml nie zrezygnuje z budowania wpływów w Afryce, ponieważ zaszkodziłoby to jego rosnącej pozycji zaufanego partnera rządów potrzebujących wsparcia.

Obecnie Grupa Wagnera jest wchłaniana przez rosyjską armię i służby⁷⁰. Po śmierci Prigożyna część wagnerowców rozproszyła się, aby znaleźć zatrudnienie w innych grupach najemników, lub zakłada własne przedsiębiorstwa⁷¹. Ważne jest to, że grupa nie zostanie rozwiązana – z uwagi na swoją pozycję, na którą pracowała od kilku lat. Część kontraktów, umów i zadań będzie przekazana do innych organizacji zrzeszających najemników, a będących pod wpływem FR. Wydobycie kruszców w Afryce pozwala m.in. na finansowanie wojny w Ukrainie, a zyski Grupy Wagnera sięgają nawet miliarda dolarów rocznie⁷².

Nadanie siłom Wagnera oficjalnego charakteru, stricte rosyjskiego, może nie mieć znaczenia w krajach takich jak Mali czy RŚA, do których zaprosili je rządzący. Zupełnie inaczej może być jednak w Libii i Sudanie,

⁶⁹ A. Kadlec, *In Africa, Wagner Is Not the Only Game in Town*, New Lines Magazine, 17 VII 2023 r., <https://newlinesmag.com/spotlight/in-africa-wagner-is-not-the-only-game-in-town/> [dostęp: 16 XII 2023].

⁷⁰ S. Rynn, K. Cockayne, *Where Next for Wagner Group in Africa?*, RUSI, 2 VIII 2023 r., <https://rusi.org/explore-our-research/publications/commentary/where-next-wagner-group-africa> [dostęp: 16 XII 2023].

⁷¹ *Wagner Leadership Fractures After Prigozhin Death*, ADF, 17 X 2023 r., <https://adf-magazine.com/2023/10/wagner-leadership-fractures-after-prigozhin-death> [dostęp: 26 XI 2023].

⁷² *Politico: Wagner Group capable of gaining \$1 billion from mining projects in Africa to finance war in Ukraine*, Kyiv Independent, 20 I 2023 r., <https://kyivindependent.com/politico-wagner-group-capable-of-gaining-1-billion-from-mining-projects-in-africa-to-finance-war-in-ukraine> [dostęp: 16 XII 2023].

gdzie takie siły można scharakteryzować jako terrorystów i potencjalnie winnych agresji na rząd wspierany przez społeczność międzynarodową. To nie jest przekaz, którym Moskwa chce się posługiwać⁷³. Dlatego w zależności od afrykańskiego kraju Kreml manewruje, opierając się na tym, czy ma związki z wagnerowcami czy nie. Podważa to zasadność jakiegokolwiek współpracy z FR i należy to akcentować w kontaktach z partnerami z Afryki. Ponadto trzeba podkreślać, że wagnerowcy nie mają oporów, aby zabijając dziennikarzy, którzy interesują się ich obecnością w krajach Afryki, a zwłaszcza kwestiami wydobycia surowców z kopalni diamentów, złota i uranu⁷⁴.

Pojawiające się sugestie na temat zaangażowania Grupy Wagnera we współczesnej Afryce można podzielić na dwie kategorie: 1) faktyczne niewielkie zaangażowanie (potwierdzone w kilku materiałach źródłowych) oraz 2) domniemane zaangażowanie (znikoma obecność w przeszłości i prawdopodobieństwo jej wystąpienia w przyszłości). Przesłankami przemawiającymi za wysuwaniem takich sugestii są działania, takie jak: sprzedaż broni z Rosji, współpraca polityczna jeszcze na przełomie XX i XXI w., wymiana gospodarcza, pojawiające się oferty szkolenia ze strony rosyjskich wojsk lub najemników. W kontekście faktycznego zaangażowania wagnerowców można wskazać Sudan Południowy, Gwineę, Burundi i Ugandę, z zaznaczeniem, że podłożem wzmianek o kooperacji wskazanych państw z rosyjskimi najemnikami jest współpraca tych krajów z Rosją, co pośrednio oznacza wejście rosyjskich najemników. W przypadku domniemanej obecności⁷⁵ można wskazać takie państwa, jak: Czad, Eswatini, Gwinea Bissau, DR Kongo, Kamerun, Komory, Botswana i Zimbabwe (rysunek 2)⁷⁶.

⁷³ *All quiet on the Wagner front*, Africa Confidential, 6 VI 2023 r., https://www.africa-confidential.com/article-preview/id/14516/All_quiet_on_the_Wagner_front [dostęp: 16 XII 2023].

⁷⁴ S. Ingber, *3 Russian Journalists Killed While Probing Reports Of Mercenaries In Africa*, NPR, 2 VIII 2018 r., <https://www.npr.org/2018/08/02/635046238/3-russian-journalists-killed-while-probing-reports-of-mercenaries-in-africa> [dostęp: 15 XI 2023].

⁷⁵ W postaci m.in. wizyt przedstawicieli Ministerstwa Obrony FR, służb specjalnych lub instruktorów Grupy Wagnera w krajach, w których rozwinęła się lub mogłaby się rozwinąć współpraca.

⁷⁶ A. Askar, *The Increasing Presence and Role of Private Security Firms in Africa: The Russian Company "Wagner" as a Model*, EPC, 6 VI 2020 r., <https://epc.ae/en/details/featured/the-increasing-presence-and-role-of-private-security-firms-in-africa-the-russian-company-wagner-as-a-model> [dostęp: 29 XII 2023]; *Private military contractors bolster Russian influence in Africa*, France24, 4 II 2022 r., <https://www.france24.com/en/live-news/20220204-private-military-contractors-bolster-russian-influence-in-africa> [dostęp: 29 XII 2023]; *Por qué el golpe*

Analizując obecność rosyjskich najemników w Afryce, warto dodać, że jednym z narzędzi dezinformacyjnych Kremla jest sztuczne kreowanie potęgi FR na tym kontynencie, jak również trzeba mieć na uwadze rosyjskie działania inspiracyjne.



Rysunek 2. Państwa w Afryce, w przypadku których można mówić o faktycznym niewielkim zaangażowaniu bądź domniemanej obecności Grupy Wagnera.

Źródło: opracowanie własne.

Grupa Wagnera pozostaje siłą Rosji w Afryce. To nic innego jak zastępczy charakter rosyjskiej obecności militarnej, realizowany bez bezpośredniego, oficjalnego udziału rosyjskich sił zbrojnych (poza instruktorami) przez niepaństwową grupę paramilitarną, blisko związaną z rosyjskim establishmentem. Rosja (jako państwo) ma umowy dwu- i wielostronne oraz kontrakty z wybranymi państwami i podmiotami z Afryki. Są to wielomilionowe projekty technologiczne, energetyczne, wojskowe, gospodarcze. Natomiast wagnerowcy bezpośrednio współpracują w wybranych krajach

de Estado en Níger puede ayudar a expandir la influencia del Grupo Wagner y Rusia en África, BBC News Mundo, 29 VII 2023 r., <https://www.bbc.com/mundo/articles/c3gz9v41xw9o> [dostęp: 29 XII 2023].

lub regionach Afryki i ich działania mają zupełnie inny charakter. Jest to np. czerpanie zysków z ochrony, realizacji konkretnych misji, szkoleń i przejmowania inwestycji (w tym głównie kopalni). Rosja i Grupa Wagnera uzupełniają się w zakresie oddziaływania na dany kraj afrykański.

Federacja Rosyjska nie miała i nie ma potencjału gospodarczego, aby konkurować w Afryce z UE i np. Chinami. W ostatnich latach jej zaangażowanie pokazało jednak, że w dłuższej perspektywie staje się silnym rywalem w niektórych obszarach i wypycha z nich kraje Zachodu⁷⁷. W dużej mierze dzieje się to z udziałem Grupy Wagnera⁷⁸. Obecnie poziom obaw o wejście rosyjskich najemników do któregośkolwiek kraju afrykańskiego jest tak wysoki, że gdy dochodzi do zamachu lub jego próby (jak m.in. w 2023 r. w Sudanie, Nigrze, Gabonie czy Sierra Leone), od razu pojawiają się pytania o wątek rosyjski.

W przypadku krajów Sahelu, w których wcześniej była obecna Republika Francuska, a teraz działa Grupa Wagnera, trzeba uwzględnić również inną perspektywę. Część elit politycznych i wojskowych tych krajów była niechętna współpracy z Francją (i szerzej z Zachodem), a przez to zbliżyła się do Rosji. Popelniono wiele błędów w relacjach z partnerami z Afryki i część zarzutów o nadmierne wykorzystywanie przez kraje Zachodu swojej pozycji jest słuszna. Tym samym wejście Grupy Wagnera powinno być ważną lekcją w procesie dalszego angażowania się w Afryce, podejmowania wspólnych przedsięwzięć i uwydatniania korzyści ze współpracy państw tego kontynentu z krajami UE i NATO.

Państwa członkowskie UE powinny przede wszystkim skoncentrować się na kilku obszarach, które są ważne dla przeciwdziałania Grupie Wagnera i podobnym formacjom. Najważniejszą rolę w ograniczeniu pozyskiwania przez nie środków finansowych odgrywa nakładanie – w skali globalnej – sankcji na podmioty (i osoby) związane zarówno z FR, jak i z Grupą Wagnera. Powinno się to odbywać we współpracy z partnerami z Afryki. Należy również pozostawać w stałym kontakcie nie tylko z tymi krajami afrykańskimi, które chcą współpracować z Zachodem, lecz także z tymi, które obecnie mają bardziej zacieśnioną relację z Moskwą (lub rosyjskimi najemnikami). Wskazywanie szkodliwych wpływów wagnerowców i nieprawdziwych obietnic Kremla powinno być częścią stałej narracji UE.

⁷⁷ A. Legucka, J. Czerep, *Wzrost zaangażowania Rosji w Afryce...*

⁷⁸ M. Bartosiewicz, *Kontrolowany chaos: rosyjska polityka wobec Afryki*, OSW, 23 VIII 2023 r., <https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2023-08-23/kontrolowany-chaos-rosyjska-polityka-wobec-afryki> [dostęp: 8 XII 2023].

Jednocześnie trzeba proponować krajom afrykańskim alternatywną współpracę z partnerami unijnymi.

Innym elementem, również ważnym dla bezpieczeństwa, jest prowadzenie szkoleń wojskowych (głównie antyterrorystycznych), pozwalających na walkę z terroryzmem w Afryce. W ocenie autora ograniczanie tego zjawiska na tym kontynencie pozwoli na zmniejszenie zagrożeń terrorystycznych, które zostały już zidentyfikowane w UE⁷⁹. Ostatni aspekt to niska efektywność i efektowność Grupy Wagnera w kwestii faktycznej walki z terroryzmem oraz utrzymaniem bezpieczeństwa w krajach Afryki. Eksponowanie błędów rosyjskiej doktryny w Afryce – o czym traktuje również niniejszy artykuł – powinno być częścią polityki informacyjnej krajów Zachodu. Trzeba dążyć do rozwijania współpracy z kontynentem afrykańskim oraz do minimalizowania (na tyle, na ile to możliwe) rozprzestrzeniania się konfliktów, skutków zamachów stanu i ataków terrorystycznych na kilka państw Afryki. Pośrednio będzie to oddziaływać na bezpieczeństwo Europy, Bliskiego Wschodu i Azji. Rywalizacja z FR jest obecnie prowadzona w skali globalnej i warto mieć to na uwadze.

Międzynarodowa działalność Grupy Wagnera ma znaczenie również dla Polski. Wynika to nie tylko z rosnącego zaangażowania RP w Afryce, lecz także z rosyjskiej agresji na Ukrainę oraz szkodliwych działań na granicach UE i NATO. W związku z tym planowany rozwój polskiej obecności dyplomatycznej, politycznej, ekonomicznej, humanitarnej, misyjnej, a także wojskowej będzie zależał od operacji realizowanych na kontynencie afrykańskim przez rosyjskich najemników. Polskie władze weryfikują, gdzie trzeba zwiększyć aktywność, mając na uwadze zagrożenia interesów RP. W Sudanie wybuchła wojna domowa i wycofano polski personel dyplomatyczny, jednak w tym samym czasie otwarto placówkę w Rwandzie oraz zrealizowano kilkanaście dużych projektów gospodarczych na kontynencie afrykańskim. Mimo że wyzwania w Europie Wschodniej są obecnie priorytetem dla polskiej dyplomacji, to symultanicznie są realizowane działania na rzecz utrzymywania regularnych kontaktów z państwami Afryki. W obu przypadkach wagnerowcy stanowią zagrożenie, które należy brać pod uwagę. Rosyjscy najemnicy (szerzej PMC) mogą być wykorzystywani do kontroli wybranych terytoriów, będąc swego rodzaju częścią armii FR.

Trzeba podkreślić, że Grupa Wagnera będzie się rozwijała. Federacja Rosyjska i najemnicy wojskowi to podmioty połączone i kooperujące.

⁷⁹ D. Szlachter, *Walka z terroryzmem w Unii Europejskiej – nowy impuls*, Toruń 2006.

W Rosji funkcjonuje ponad 20 nieco podobnych, mniej znanych, półpaństwowych, zagranicznych, prywatnych firm wojskowych. Czeczeński watażka Ramzan Kadyrow stworzył grupę Achmat, istnieje też organizacja Redut (bardzo aktywna w RŚA), a swoje inwestycje w PMC mają Gazprom i Roskosmos. Rosja będzie kontynuowała ekspansję, wykorzystując w tym celu wagnerowców. Na pewno podejmie próby ingerencji w kolejnych krajach – tych, w których rządzący będą chcieli „podtrzymać” swoją władzę.

Bibliografia

Global Terrorism Index 2023: Measuring the Impact of Terrorism, Institute for Economics & Peace, Sydney, marzec 2023 r.

Izak K., *Leksykon organizacji i ruchów islamistycznych*, Warszawa 2014.

Olech A., *Ataki terrorystyczne w Federacji Rosyjskiej w XXI wieku*, „Nowa Polityka Wschodnia” 2019, nr 4 (23), s. 109–127.

Olech A., *Terrorist Threats to the Energy Sector in Africa and the Middle East*, w: *Countering Terrorism on Tomorrow's Battlefield: Critical Infrastructure Security and Resiliency Handbook 2*, S.J. Lohman (red.), grudzień 2022 r.

Olech A., Rogozińska A., *Zagraniczne obiekty wojskowe jako system wzmacniania międzynarodowego potencjału militarnego Federacji Rosyjskiej*, Warszawa 2022.

Olech A., Wójtowicz B., *Rywalizacja o surowce w Sahelu – region konfliktu mocarstw*, Warszawa 2022.

Szlachter D., *Walka z terroryzmem w Unii Europejskiej – nowy impuls*, Toruń 2006.

Wójcik J., *Ekspansja dżihadu w Afryce: z Sahelu ku południu*, „Układ Sił” 2020, nr 20.

Źródła internetowe

Aftandilian D., *The Fate of the Wagner Group in Syria, Libya, and Sudan*, Arab Center Washington DC, 18 VII 2023 r., <https://arabcenterdc.org/resource/the-fate-of-the-wagner-group-in-syria-libya-and-sudan/> [dostęp: 23 XI 2023].

All quiet on the Wagner front, Africa Confidential, 6 VI 2023 r., https://www.africa-confidential.com/article-preview/id/14516/All_quiet_on_the_Wagner_front [dostęp: 16 XII 2023].

Askar A., *The Increasing Presence and Role of Private Security Firms in Africa: The Russian Company "Wagner" as a Model*, EPC, 6 VI 2020 r., <https://epc.ae/en/details/featured/the-increasing-presence-and-role-of-private-security-firms-in-africa-the-russian-company-wagner-as-a-model> [dostęp: 29 XII 2023].

Bartosiewicz M., *Kontrolowany chaos: rosyjska polityka wobec Afryki*, OSW, 23 VIII 2023 r., <https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2023-08-23/kontrolowany-chaos-rosyjska-polityka-wobec-afryki> [dostęp: 8 XII 2023].

Benjamin I., *Troops Kill 10 Terrorists, Recover Arms, Motorcycles, Leadership*, 5 XI 2023 r., <https://leadership.ng/troops-kill-10-terrorists-recover-arms-motorcycles> [dostęp: 4 XII 2023].

Bensimon C. i in., *Au Sahel, l'insurmontable échec de la stratégie française*, Le Monde, 3 XI 2023 r., https://www.lemonde.fr/afrique/article/2023/11/03/au-sahel-l-insurmontable-echec-de-la-strategie-francaise_6197973_3212.html [dostęp: 28 XI 2023].

Bermudez J., Katz B., *Moscow's Next Front: Russia's Expanding Military Footprint in Libya*, Center for Strategic and International Studies, 17 VI 2020 r., <https://www.csis.org/analysis/moscows-next-front-russias-expanding-military-footprint-libya> [dostęp: 9 XII 2023].

Black R., *Zelensky meets Sudanese official during 'technical stopover' in Ireland*, Independent, 23 IX 2023 r., <https://www.independent.co.uk/news/uk/volodymyr-zelensky-north-america-ireland-joe-biden-department-of-foreign-affairs-b2417251.html> [dostęp: 10 XII 2023].

Bobin F., *Coup de froid dans les relations entre l'Algérie et le Mali*, Le Monde, 27 XII 2023 r., https://www.lemonde.fr/afrique/article/2023/12/27/coup-de-froid-dans-les-relations-entre-l-algerie-et-le-mali_6207961_3212.html?fbclid=IwAR0ZDmZbfge7Wz-a4vIft4pVoLJzi1MmsUqe5LpaYFGYx85_966-Y9yrQ4Y [dostęp: 27 XII 2023].

Bobin F., *La grande désillusion algérienne au Sahel*, Le Monde, 23 XI 2023 r., https://www.lemonde.fr/international/article/2023/11/23/la-grande-desillusion-algerienne-au-sahel_6201889_3210.html [dostęp: 24 XI 2023].

Center for Preventive Action, *Civil Conflict in Libya?*, Council on Foreign Relations, 19 IX 2023 r., <https://www.cfr.org/global-conflict-tracker/conflict/civil-war-libya> [dostęp: 23 XI 2023].

Central African Republic: President Touadéra meets Macron in France, Africa News, 13 IX 2023 r., <https://www.africanews.com/2023/09/13/central-african-republic-president-touadera-meets-macron-in-france> [dostęp: 14 XI 2023].

Chan M., *Wagner mercenaries rescued Chinese gold miners in Central African Republic in July, paramilitary group says*, South China Morning Post, 13 VII 2023 r., <https://www.scmp.com/news/china/military/article/3227490/wagner-mercenaries-rescued-chinese-gold-miners-central-african-republic-july-paramilitary-group-says> [dostęp: 10 XI 2023].

Chason R., Debout B., *In Wagner's largest African outpost, Russia looks to tighten its grip*, Washington Post, 18 IX 2023 r., <https://www.washingtonpost.com/world/2023/09/18/wagner-central-african-republic-touadera> [dostęp: 5 XI 2023].

Chesnutt K., Zimmerman K., *The State of al Qaeda and ISIS Around the World*, Critical Threats, 8 IX 2022 r., <https://www.criticalthreats.org/analysis/the-state-of-al-qaeda-and-isis-around-the-world> [dostęp: 5 XI 2023].

Country Reports on Terrorism 2020: Democratic Republic of the Congo, U.S. Department of State, <https://www.state.gov/reports/country-reports-on-terrorism-2020/democratic-republic-of-the-congo/> [dostęp: 16 XII 2023].

Czerep J., *Afryka Subsaharyjska w strategii tzw. Państwa Islamskiego*, PISM, 1 VIII 2022 r., <https://www.pism.pl/publikacje/afryka-subsaharyjska-w-strategii-tzw-panstwa-islamskiego> [dostęp: 2 XI 2023].

Czerep J., *Erytrea nieformalnym reprezentantem prorosyjskich sił w Afryce*, PISM, 22 III 2023 r., <https://www.pism.pl/publikacje/erytrea-nieformalnym-reprezentantem-prorosyjskich-sil-w-afryce> [dostęp: 28 XI 2023].

Czerep J., *Nowy front dżihadu w Mozambiku*, PISM, 22 IX 2020 r., https://pism.pl/publikacje/Nowy_front_dzihadu_w_Mozambiku [dostęp: 21 XI 2023].

Czerep J., *Perspektywy zakończenia wojny w Sudanie*, PISM, 25 V 2023 r., <https://pism.pl/publikacje/perspektywy-zakonczenia-wojny-w-sudanie> [dostęp: 23 XI 2023].

Czerep J., *Przyszłość misji ONZ w Afryce po wycofaniu MINUSMA z Mali*, PISM, 6 X 2023 r., <https://www.pism.pl/publikacje/przyszlosc-misji-onz-w-afryce-po-wycofaniu-minusma-z-mali> [dostęp: 2 XI 2023].

Czerep J., Legucka A., *Przyszłość „imperium” Prigożyna*, PISM, 17 VII 2023 r., <https://www.pism.pl/publikacje/przyszlosc-imperium-prigozyna> [dostęp: 16 XI 2023].

Diallo T., *Mali signs agreement with Russia to build gold refinery*, Reuters, 22 XI 2023 r., <https://www.reuters.com/markets/commodities/mali-signs-agreement-with-russia-build-gold-refinery-2023-11-22/?rpc=401&> [dostęp: 23 XI 2023].

Douet M., *Russia overtakes China as leading arms seller in sub-Saharan Africa*, Le Monde, 28 III 2023 r., https://www.lemonde.fr/en/le-monde-africa/article/2023/03/28/russia-overtakes-china-as-leading-arms-seller-in-sub-saharan-africa_6021018_124.html [dostęp: 10 XII 2023].

Eydoux T., Savoye L., *Quand les forces spéciales ukrainiennes combattent des mercenaires russes de Wagner au Soudan*, Le Monde, 19 XI 2023 r., https://www.lemonde.fr/videos/video/2023/11/19/quand-les-forces-speciales-ukrainiennes-combattent-des-mercenaires-russes-de-wagner-au-soudan_6201120_1669088.html [dostęp: 21 XI 2023].

Faulkner Ch., *Undermining Democracy and Exploiting Clients: The Wagner Group's Nefarious Activities in Africa*, „CTC Sentinel” 2022, t. 15, nr 6, <https://ctc.westpoint.edu/wp-content/uploads/2022/06/CTC-SENTINEL-062022.pdf> [dostęp: 4 XII 2023].

France to end Central African Republic military mission in 2016, France24, 30 III 2016 r., <https://www.france24.com/en/20160330-france-end-military-operations-central-african-republic> [dostęp: 5 XI 2023].

Gadera K., *Mali: chaotyczny koniec MINUSMA, Azawad znów walczy o niepodległość*, Konflikty.pl, 9 XI 2023 r., <https://www.konflikty.pl/aktualnosci/wiadomosci/mali-azawad-niepodleglosc> [dostęp: 13 XI 2023].

Gadera K., *Wagnerowcy wycofują się z Mozambiku*, Konflikty.pl, 2 XII 2019 r., <https://www.konflikty.pl/aktualnosci/wiadomosci/wagnerowcy-wycofuja-sie-z-mozambiku/> [dostęp: 22 XII 2023].

Goosen M., *Biggest Gold Producing Countries in Africa*, Energy Capital Power, 5 IX 2022 r., <https://energycapitalpower.com/biggest-gold-producing-countries-in-africa/> [dostęp: 25 XI 2023].

Grynszpan E., *L'Ukraine tente de défier la Russie en Afrique*, Le Monde, 20 XI 2023 r., https://www.lemonde.fr/afrique/article/2023/11/20/l-ukraine-tente-de-defier-la-russie-en-afrique_6201324_3212.html [dostęp: 22 XI 2023].

Gustafson K. i in., *Sudan: questions about Wagner Group involvement as another African country falls prey to Russian mercenaries*, Brunel University London, 2 V 2023 r., <https://www.brunel.ac.uk/news-and-events/news/articles/Sudan-questions-about-Wagner-Group-involvement-as-another-African-country-falls-prey-to-Russian-mercenaries> [dostęp: 22 XI 2023].

Ingber S., *3 Russian Journalists Killed While Probing Reports of Mercenaries in Africa*, NPR, 2 VIII 2018 r., <https://www.npr.org/2018/08/02/635046238/3-russian-journalists-killed-while-probing-reports-of-mercenaries-in-africa> [dostęp: 15 XI 2023].

IS group-linked militants kill 17 in Nigeria for failing to pay 'cattle tax', France24, 1 XI 2023 r., <https://www.france24.com/en/africa/20231101-jihadists-kill-17-people-in-raid-on-remote-village-in-northeast-nigeria> [dostęp: 4 XII 2023].

ISIS-Mozambique, Counter Terrorism Guide, listopad 2022 r., https://www.dni.gov/nctc/ftos/isis_mozambique_fto.html [dostęp: 12 XII 2023].

Kacewicz M., *Do czego Putin potrzebuje Afryki i co może jej dać?*, Belsat, 28 VII 2023 r., <https://belsat.eu/pl/news/28-07-2023-do-czego-putin-potrzebuje-afryki-i-co-moze-jej-dac> [dostęp: 18 XI 2023].

Kadlec A., *In Africa, Wagner Is Not the Only Game in Town*, New Lines Magazine, 17 VII 2023 r., <https://newlinesmag.com/spotlight/in-africa-wagner-is-not-the-only-game-in-town/> [dostęp: 16 XII 2023].

Kuczyński G., *Russia's Tatneft Discovers New Oil Field in Libya*, Warsaw Institute, 25 V 2023 r., <https://warsawinstitute.org/russias-tatneft-discovers-new-oil-field-in-libya/> [dostęp: 21 XII 2023].

Kuwali D., *Oversight and Accountability to Improve Security Sector Governance in Africa*, Africa Center for Strategic Studies, 11 IX 2023 r., <https://africacenter.org/publication/asb42en-oversight-accountability-security-sector-governance> [dostęp: 4 XII 2023].

Legucka A., Czerep J., *Wzrost zaangażowania Rosji w Afryce*, PISM, 20 XI 2019 r., https://www.pism.pl/publikacje/Wzrost_zaangazowania_Rosji_w_Afryce_ [dostęp: 16 XII 2023].

Master and Chef. How Evgeny Prigozhin led the Russian offensive in Africa, The Proekt team, 14 III 2023 r., <https://www.proekt.media/en/article-en/evgeny-prigozhin-africa/> [dostęp: 5 XI 2023].

Mehra T., Demuyneck M., *Raising the stakes against the Wagner Group: From mercenaries to a designated terrorist group?*, ICCT, 17 I 2023 r., <https://www.icct.nl/publication/raising-stakes-against-wagner-group-mercenaries-designated-terrorist-group> [dostęp: 16 XII 2023].

Mozambique, Global Centre for the Responsibility to Protect, 30 XI 2023 r., <https://www.globalr2p.org/countries/mozambique/> [dostęp: 11 XII 2023].

Much ado about Kidal, Africa Confidential, 30 XI 2023 r., https://www.africa-confidential.com/article/id/14715/Much_ado_about_Kidal [dostęp: 30 XI 2023].

Nasr W., *How the Wagner Group Is Aggravating the Jihadi Threat in the Sahel*, „CTC Sentinel” 2022, t. 15, nr 11, <https://ctc.westpoint.edu/wp-content/uploads/2022/12/CTC-SENTINEL-112022.pdf> [dostęp: 4 XII 2022].

Noulens M., *Général Frédéric Blachon au JDD: «Au Sahel, le risque d'une victoire des djihadistes est réel»*, Le Journal du Dimanche, 5 XI 2023 r., <https://www.lejdd.fr/international/general-frederic-blachon-au-jdd-au-sahel-le-risque-dune-victoire-des-djihadistes-est-reel-139434> [dostęp: 6 XI 2023].

Olech A., *Afryka i Bliski Wschód w wymiarze bezpieczeństwa – podsumowanie 2022 roku*, Defence24, 31 XII 2022 r., <https://defence24.pl/geopolityka/afryka-i-bliiski-wschod-w-wymiarze-bezpieczenstwa-podsumowanie-2022-roku> [dostęp: 18 XI 2023].

Olech A., *Francja wycofuje się z Mali i idzie na zachód Afryki [analiza]*, Defence24, 14 VIII 2022 r., <https://defence24.pl/geopolityka/francja-wycofuje-sie-z-mali-i-idzie-na-zachod-afryki-analiza> [dostęp: 18 XI 2023].

Olech A. i in., *Militarne zaangażowanie Federacji Rosyjskiej w Afryce. Zawarte porozumienia i umowy*, Instytut Nowej Europy, 23 V 2023 r., <https://ine.org.pl/militarne-zaangazowanie-federacji-rosyjskiej-w-afryce-zawarte-porozumienia-i-umowy/> [dostęp: 10 XII 2023].

Olech A., Pawłowski M., *Wyzwania i szanse dla Europy w krajach Maghrebu [raport]*, Instytut Nowej Europy, 1 VII 2022 r., <https://ine.org.pl/wyzwania-i-szanse-dla-euro-py-w-krajach-maghrebu/> [dostęp: 4 XII 2022].

Otłowski T., *Wagner Group Activities in Libya and the Sahel Region After the Failed “Putsch” in Russia – Business as Usual*, Casmir Pulaski Foundation, 27 X 2023 r., <https://pulaski.pl/en/wagner-group-activities-in-libya-and-the-sahel-region-after-the-failed-putsch-in-russia-business-as-usual> [dostęp: 25 XI 2023].

Peltier E., *Battle for Influence Rages in Heart of Wagner’s Operations in Africa*, The New York Times, 26 XI 2023 r., <https://www.nytimes.com/2023/11/26/world/africa/wagner-russia-central-african-republic.html> [dostęp: 15 XII 2023].

Penney J., *Rwanda Helped Oust Jihadists in Mozambique. Can This Model Work in West Africa?*, PassBlue, 16 VIII 2023 r., <https://www.passblue.com/2023/08/16/rwanda-helped-oust-jihadists-in-mozambique-can-it-work-as-a-counterinsurgency-model-in-west-africa> [dostęp: 14 XII 2023].

Politico: Wagner Group capable of gaining \$1 billion from mining projects in Africa to finance war in Ukraine, Kyiv Independent, 20 I 2023 r., <https://kyivindependent.com/politico-wagner-group-capable-of-gaining-1-billion-from-mining-projects-in-africa-to-finance-war-in-ukraine> [dostęp: 16 XII 2023].

Por qué el golpe de Estado en Níger puede ayudar a expandir la influencia del Grupo Wagner y Rusia en África, BBC News Mundo, 29 VII 2023 r., <https://www.bbc.com/mundo/articles/c3gz9v41xw9o> [dostęp: 29 XII 2023].

Private military contractors bolster Russian influence in Africa, France24, 4 II 2022 r., <https://www.france24.com/en/live-news/20220204-private-military-contractors-bolster-russian-influence-in-africa> [dostęp: 29 XII 2023].

Putin Gains Influence in Oil-Rich Libya as US Struggles to Oust Wagner Group, Bloomberg, 4 VI 2023 r., <https://www.bloomberg.com/news/articles/2023-06-04/putin-gains-in-oil-exporter-libya-as-us-struggles-to-oust-wagner-group#xj4y7vzkg> [dostęp: 14 XII 2023].

Rampe W., *What Is Russia's Wagner Group Doing in Africa?*, Council on Foreign Relations, 23 V 2023 r., <https://www.cfr.org/in-brief/what-russias-wagner-group-doing-africahttps://www.cfr.org/in-brief/what-russias-wagner-group-doing-africa> [dostęp: 21 XII 2023].

Rapport d'information par la Commission des Affaires Étrangères en conclusion des travaux d'une mission d'information constituée le 14 décembre 2022 sur les relations entre la France et l'Afrique, enregistré à la Présidence de l'Assemblée nationale le 8 novembre 2023, https://www.assemblee-nationale.fr/dyn/16/rapports/cion_afetr/l16b1841_rapport-information# [dostęp: 23 XI 2023].

Roger B., *Au Burkina Faso, des militaires russes pour protéger Ibrahim Traoré?*, jeuneafrique, 17 XI 2023 r., <https://www.jeuneafrique.com/1503219/politique/au-burkina-faso-des-militaires-russes-pour-protoger-ibrahim-traore/> [dostęp: 10 XII 2023].

Rolley S., *Islamic State affiliate expanding reach in DR Congo, UN Experts Say*, Reuters, 20 VI 2023 r., <https://www.reuters.com/world/africa/islamic-state-affiliate-expanding-reach-dr-congo-un-experts-say-2023-06-20/> [dostęp: 17 XI 2023].

Russia Emerges as Top Weapons Supplier to Sub-Saharan Africa, ADF, 21 IV 2023 r., <https://adf-magazine.com/2023/04/russia-emerges-as-top-weapons-supplier-to-sub-saharan-africa> [dostęp: 4 XII 2023].

Russia works with Libya on the creation of a military corps in Africa, Agenzia Nova, 17 XI 2023 r., <https://www.agenzianova.com/en/news/la-russia-lavora-con-la-libia-alla-creazione-di-un-corpo-militare-in-africa/> [dostęp: 23 XI 2023].

Rynn S., Cockayne K., *Where Next for Wagner Group in Africa?*, RUSI, 2 VIII 2023 r., <https://rusi.org/explore-our-research/publications/commentary/where-next-wagner-group-africa> [dostęp: 16 XII 2023].

Sadkiewicz S. (@StanSadkiewicz), X, 7 XI 2023 r., <https://twitter.com/StanSadkiewicz/status/1721882283916079351> [dostęp: 7 XI 2023].

Sch lindwein S., *Are white mercenaries fighting in the DRC Conflict?*, Deutsche Welle, 17 I 2023 r., <https://www.dw.com/en/are-white-mercenaries-fighting-in-the-drc-conflict/a-64407711> [dostęp: 16 XII 2023].

Serwat L., *Moving out of the shadows: Shifts in Wagner Group Operations Around the World*, ACLED, 2 VIII 2023 r., https://acleddata.com/acleddatanew/wp-content/uploads/2023/08/ACLED_Report_Shifts-in-Wagner-Group-Operations-Around-the-World_2023.pdf [dostęp: 5 XI 2023].

Sharife K. i in., *Documents Reveal Wagner's Golden Ties to Sudanese Military Companies*, Organized Crime and Corruption Reporting Project, 2 XI 2022 r., <https://www.occrp.org/en/investigations/documents-reveal-wagners-golden-ties-to-sudanese-military-companies> [dostęp: 4 XI 2023].

Sheludkova I., *Why is Russia's Wagner Group in Sudan, and what does it have to do with the war in Ukraine?*, EuroNews, 27 IV 2023 r., <https://www.euronews.com/2023/04/27/why-is-russias-wagner-group-in-sudan-and-what-does-it-have-to-do-with-the-war-in-ukraine> [dostęp: 16 XI 2023].

Shurkin M. (@MichaelShurkin), X, 22 XI 2023 r., <https://twitter.com/MichaelShurkin/status/1727337675806650866> [dostęp: 22 XI 2023].

Sirleaf E., *UAE must cut ties with Sudan's war*, The Times, 27 XI 2023 r., <https://www.thetimes.co.uk/article/uae-must-cut-ties-with-sudans-war-czpwpms2n> [dostęp: 27 XI 2023].

Sixto D., *Russian Mercenaries: A String of Failures in Africa*, Geopolitical Monitor, 24 VIII 2020 r., <https://www.geopoliticalmonitor.com/russian-mercenaries-a-string-of-failures-in-africa/> [dostęp: 28 XI 2023].

South-west bias claims weaken Tinubu's standing, Africa Confidential, 30 XI 2023 r., https://www.africa-confidential.com/article/id/14716/South-west_bias_claims_weaken_Tinubu%27s_standing [dostęp: 14 XII 2023].

State Department Terrorist Designations of ISIS Affiliates and Leaders in the Democratic Republic of the Congo and Mozambique, U.S. Department of State, 10 III 2023 r., <https://www.state.gov/state-department-terrorist-designations-of-isis-affiliates-and-leaders-in-the-democratic-republic-of-the-congo-and-mozambique/> [dostęp: 12 XII 2023].

Sudan's President Bashir asks Putin for 'protection' from 'aggressive' US, France24, 23 XI 2017 r., <https://www.france24.com/en/20171123-sudan-president-bashir-asks-putin-protection-aggressive-us> [dostęp: 16 XI 2023].

Touadéra stirs the geopolitical cauldron, Africa Confidential, 2 XI 2023 r., https://www.africa-confidential.com/article/id/14682/Touad%c3%a9ra_stirs_the_geopolitical_cauldron [dostęp: 5 XI 2023].

Ukraine Expands Diplomatic Presence in Africa: New Embassy Launches in Ghana, Kyiv Independent, 27 XII 2023 r., <https://www.kyivpost.com/post/26022/> [dostęp: 29 XII 2023].

Wagner Group Terrorizing Sudanese Gold Miners, ADF, 19 VII 2022 r. <https://adf-magazine.com/2022/07/wagner-group-terrorizing-sudanese-gold-miners> [dostęp: 4 XI 2023].

Wagner Group Uses Mafia-Style Tactics to Dominate CAR's Diamond Sector, ADF, 1 VIII 2023 r., <https://adf-magazine.com/2023/08/wagner-group-uses-mafia-style-tactics-to-dominate-cars-diamond-sector/> [dostęp: 25 XI 2023].

Wagner Leadership Fractures After Prigozhin Death, ADF, 17 X 2023 r., <https://adf-magazine.com/2023/10/wagner-leadership-fractures-after-prigozhin-death> [dostęp: 26 XI 2023].

Warner J., *A View from the CT Foxhole: Idriss Mounir Lallali, Deputy Director, African Centre for the Study and Research on Terrorism (ACSRT)*, „CTC Sentinel” 2021, t. 14, nr 5, <https://ctc.westpoint.edu/a-view-from-the-ct-foxhole-idriss-mounir-lallali-deputy-director-african-centre-for-the-study-and-research-on-terrorism-acsr/> [dostęp: 16 XII 2023].

Wintour P., *Fears for Libyan oil production amid military threats*, The Guardian, 4 VII 2023 r., <https://www.theguardian.com/world/2023/jul/04/fears-for-libyan-oil-production-amidmilitary-action-threats> [dostęp: 13 XII 2023].

Dr Aleksander Olech

Szef Działu Współpracy Międzynarodowej Defence24. Wykładowca na uczelniach polskich i zagranicznych, współpracownik NATO, analityk i publicysta. Były zastępca dyrektora Departamentu Afryki i Bliskiego Wschodu Ministerstwa Spraw Zagranicznych. Absolwent Europejskiej Akademii Dyplomacji oraz Akademii Sztuki Wojennej. Główne zainteresowania badawcze: relacje francusko-rosyjskie, wyzwania w Afryce i polityka bezpieczeństwa NATO.

Kontakt: a.olech@defence24.pl

Między konfliktem zbrojnym a terroryzmem państwowym – szczególnie indywidualne środki ograniczające przyjęte w Polsce w kontekście wojny w Ukrainie i sytuacji w Białorusi. Perspektywa prawna

Between armed conflict and state terrorism - specific individual restrictive measures adopted in Poland in the context of the war in Ukraine and the situation in Belarus. Legal perspective

MARIUSZ CICHOMSKI

Ministerstwo Spraw Wewnętrznych
i Administracji



<https://orcid.org/0000-0003-3707-7856>

Abstrakt

Agresja Federacji Rosyjskiej na Ukrainę w 2022 r. oraz działania Białorusi, zarówno wewnętrzne, jak i te wspierające Rosję, spowodowały liczne zmiany w wymiarze geopolitycznym wykraczające poza kontynent europejski. Skutkowały one również podjęciem szczególnych środków prawnych, zarówno na poziomie Unii Europejskiej, jak i w Polsce w kwestii przeciwdziałania wspieraniu tej agresji. Celem artykułu jest omówienie rozwiązań prawnych przyjętych w Polsce, które dotyczą środków ograniczających wobec osób i podmiotów. Środki te zostały wprowadzone *Ustawą z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego*. W artykule określono relacje do mechanizmów zawartych w rozporządzeniach Unii Europejskiej, a także wskazano potrzebę zmian prawnych mających na celu przyjęcie stałych systemowych rozwiązań w zakresie stosowania krajowych środków ograniczających.

Słowa kluczowe

sankcje, środki ograniczające, lista sankcyjna, zamrożenie środków finansowych, wojna w Ukrainie

Abstract

The aggression of the Russian Federation against Ukraine in 2022 and the actions of Belarus, both at the internal level and in support of Russia, have caused numerous changes in the geopolitical dimension, with consequences reaching beyond the European continent. They also resulted in the adoption of specific legal measures, both at the European Union and national levels, to counteract support for this aggression. The aim of this study is to present national legal solutions regarding restrictive measures against persons and entities that were introduced by the Act on special solutions for counteracting support for aggression against Ukraine and for the protection of national security. The article sets out their relationship to the mechanisms contained in European Union regulations and identifies the need for legal changes to adopt permanent systemic solutions for the application of national restrictive measures.

Keywords

sanctions, restrictive measures, sanctions list, freezing of financial resources, war in Ukraine

Konflikt zbrojny a terroryzm państwowy

Zbrojny atak Federacji Rosyjskiej (FR) na Ukrainę 24 lutego 2022 r., będący rozwinięciem działań z 2014 r., w efekcie których została dokonana aneksja Półwyspu Krymskiego do Rosji, od początku był konfliktem militarnym prowadzonym przez regularną armię rosyjską, przy wsparciu różnego rodzaju jednostek i sił, w tym Grupy Wagnera. Jednak sposób prowadzenia przez Rosję działań zbrojnych oraz jej zaangażowanie w inne konflikty na świecie szybko spowodowały, że postrzega się ją nie tylko jako państwo agresora konfliktu zbrojnego, lecz także państwo sponsorujące bądź wspierające terroryzm, a władze FR nazywa się nawet reżimem terrorystycznym. W tym kontekście istotny akt prawny na gruncie europejskim to *Rezolucja Parlamentu Europejskiego z dnia 23 listopada 2022 r. w sprawie uznania Federacji Rosyjskiej za państwo sponsorujące terroryzm* (dalej: rezolucja z 23 listopada 2022 r.). Parlament Europejski uwzględnił w niej podstawy prawne wskazujące na militarny charakter konfliktu, w tym *Rezolucję z dnia 6 października 2022 r. w sprawie eskalowania przez Rosję wojny napastniczej przeciwko Ukrainie*, *Rezolucję z dnia 19 maja 2022 r. w sprawie zwalczania bezkarności za zbrodnie wojenne w Ukrainie* oraz *Rezolucję z dnia 25 listopada 2021 r.*

w sprawie przypadków łamania praw człowieka przez prywatne firmy wojskowe i ochroniarskie, zwłaszcza Grupę Wagnera. Parlament wziął pod uwagę także Kartę Narodów Zjednoczonych, konwencję w sprawie zapobiegania i karnia zbrodni ludobójstwa z 9 grudnia 1948 r.¹, czwartą konwencję genewską o ochronie osób cywilnych podczas wojny z 12 sierpnia 1949 r. czy Rzymski Statut Międzynarodowego Trybunału Karnego. Parlament Europejski odwołał się również do międzynarodowych i unijnych regulacji dotyczących zapobiegania terroryzmowi bądź zwalczania go, w tym rezolucji Rady Bezpieczeństwa ONZ nr 2341 o ochronie infrastruktury krytycznej przed aktami terrorystycznymi (z 13 lutego 2017 r.), konwencji o zwalczaniu terroryzmu z 27 stycznia 1977 r.² oraz przyjętych po niej konwencji międzynarodowych, a także przepisów UE dotyczących zwalczania terroryzmu, w tym *Wspólnego stanowiska Rady 2001/931/WPZiB z 27 grudnia 2001 r. w sprawie zastosowania szczególnych środków w celu zwalczania terroryzmu oraz Rozporządzenia Rady (WE) nr 2580/2001 z 27 grudnia 2001 r. w sprawie szczególnych środków restrykcyjnych skierowanych przeciwko niektórym osobom i podmiotom mających na celu zwalczanie terroryzmu.*

Parlament Europejski, wskazując powody uznania Rosji za państwo sponsorujące terroryzm, poza wymienionymi podstawami prawnymi przytoczył przesłanki faktyczne stanowiące uzasadnienie do przyjętej rezolucji z 23 listopada 2022 r. Wskazano m.in., że:

(...) od 2014 r., a zwłaszcza od 24 lutego 2022 r., kiedy Rosja wznowiła bezprawną, niesprowokowaną i nieuzasadnioną wojnę napastniczą przeciwko Ukrainie, jej siły prowadzą masowe ataki na obszary zamieszkałe i infrastrukturę cywilną, w których zginęły tysiące ukraińskich cywilów, i dopuszcza się w całym kraju aktów terrorku wymierzonych w różne elementy infrastruktury cywilnej, na przykład dzielnice mieszkaniowe, szkoły, szpitale, dworce kolejowe, teatry oraz sieci wodociągowe i elektroenergetyczne³.

Zwrócono uwagę, że Rosja od lat wspiera i finansuje reżimy i organizacje terrorystyczne, zwłaszcza syryjski reżim Baszszara al-Asada, któremu

¹ *Konwencja w sprawie zapobiegania i karnia zbrodni ludobójstwa, uchwalona przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 9 grudnia 1948 r. (ratyfikowana zgodnie z ustawą z dnia 18 lipca 1950 r.)* – (przyp. red.).

² *Europejska konwencja o zwalczaniu terroryzmu, sporządzona w Strasburgu dnia 27 stycznia 1977 r.*

³ Rezolucja z 23 listopada 2022 r., lit. A.

dostarcza broń i w którego obronie prowadziła umyślne ataki na syryjskich cywilów, miasta i infrastrukturę cywilną. Odwołano się do ataków, m.in. morderstw lub ich usiłowań, na przeciwników politycznych, w tym dziennikarzy, polityków, działaczy i przywódców zagranicznych. Przypomniano, że 15 listopada 2022 r. holenderski sąd skazał zaocznie dwóch Rosjan i prokremlowskiego ukraińskiego separatystę za zamordowanie 298 osób przez zestrzelenie samolotu malezyjskich linii lotniczych⁴.

Okoliczności przytoczone w rezolucji z 23 listopada 2022 r. nie wyczerpują przesłanek przywołanych dla jej uzasadnienia, ale jednoznacznie rozszerzają sposób postrzegania działań Rosji, które są analizowane nie tylko z perspektywy strictly militarnej, lecz także w kontekście terroryzmu w wymiarze państwowym. Warto zwrócić uwagę, że w rezolucji odwołano się do oświadczenia urzędującego wówczas polskiego Ministra Spraw Zagranicznych Zbigniewa Raua, pełniącego wtedy funkcję Przewodniczącego Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE), z 14 marca 2022 r., który (...) *ataki rządu Federacji Rosyjskiej na niewinnych cywilów i infrastrukturę cywilną w Ukrainie określił mianem „terroryzmu państwowego”*⁵.

W rezolucji tej stwierdzono, że wprawdzie Unia Europejska (UE) prowadzi wykaz objętych sankcjami osób, grup i podmiotów zamieszanych w akty terrorystyczne, lecz jej obowiązujące przepisy, w przeciwieństwie do przepisów np. Stanów Zjednoczonych czy Kanady, nie przewidują uznania całego państwa za sponsora terroryzmu. W tym kontekście Parlament Europejski

(...) wzywa Unię Europejską i jej państwa członkowskie do opracowania ram prawnych UE pozwalających uznać dane państwo za sponsorujące terroryzm i stosujące środki terroru, co pociągałoby za sobą szereg istotnych środków ograniczających wobec tych krajów i miało daleko idące restrykcyjne skutki dla stosunków UE z tymi krajami; wzywa Radę, aby następnie rozważyła wpisanie Federacji Rosyjskiej na taką unijną listę państw sponsorujących terroryzm; wzywa partnerów UE do przyjęcia podobnych środków⁶.

⁴ Tamże, lit. B, L, N.

⁵ Tamże, lit. T.

⁶ Tamże, pkt 4.

Parlament Europejski zaapelował także o umieszczenie Rosji i Białorusi w unijnym wykazie państw trzecich wysokiego ryzyka w kontekście przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu⁷.

Parlament Europejski wezwał ponadto UE i jej państwa członkowskie, co oczywiste w tego rodzaju okolicznościach, do podjęcia względem Rosji działań o charakterze izolacyjnym na arenie międzynarodowej, do (...) *umieszczenia grupy Wagnera i 141. Specjalnego Pułku Zmotoryzowanego, znanego także jako kadyrowcy, oraz innych finansowanych przez Rosję grup zbrojnych, milicji i popleczników, takich jak działające na okupowanych terytoriach Ukrainy, na unijnej liście osób, grup i podmiotów zaangażowanych w akty terrorystyczne (unijnej liście terrorystów)*⁸. Apelował też o zakończenie prac nad kolejnym pakietem sankcji związanych z mrożeniem środków finansowych, funduszy i zasobów gospodarczych osób i podmiotów wspierających działania Rosji i Białorusi. W odniesieniu do sankcji wezwał zarówno Komisję Europejską (KE), jak i państwa członkowskie UE, aby dopilnowały szybkiego wdrożenia i pełnego egzekwowania wszystkich sankcji indywidualnych i sektorowych i zapobiegały ich obchodzeniu, a także prowadziły dochodzenia w takich sprawach i ściagały sprawców. Zaapelowano również, aby (...) *kary krajowe za nieprzestrzeganie sankcji UE były skuteczne, proporcjonalne i odstraszające*⁹.

Podstawą dla wprowadzenia mechanizmu sankcyjnego na poziomie UE jest art. 29 *Traktatu o Unii Europejskiej* (TUE)¹⁰, który pozwala Radzie UE na nakładanie środków ograniczających (sankcji) wymierzonych w rządy państw niebędących państwami członkowskimi UE, podmioty niepaństwowe (np. spółki) oraz osoby fizyczne w celu wywołania zmian w ich polityce lub działaniach. Zgodnie z art. 215 ust. 2 *Traktatu o funkcjonowaniu Unii Europejskiej*¹¹ Rada może przyjąć natomiast niezbędne środki w celu

⁷ Tamże, pkt 9.

⁸ Tamże, pkt 6.

⁹ Tamże, pkt 7.

¹⁰ *Traktat o Unii Europejskiej* (wersja skonsolidowana) – Tytuł V – Postanowienia ogólne o działaniach zewnętrznych Unii i postanowienia szczególne dotyczące wspólnej polityki zagranicznej i bezpieczeństwa – Rozdział 2 – Postanowienia szczególne dotyczące wspólnej polityki zagranicznej i bezpieczeństwa – Sekcja 1 – Postanowienia wspólne – Artykuł 29 (dawny artykuł 15 TUE).

¹¹ *Traktat o funkcjonowaniu Unii Europejskiej* (wersja skonsolidowana) – Część 5 – Działania zewnętrzne Unii – Tytuł IV – Środki ograniczające – Artykuł 215 (dawny artykuł 301 Traktatu ustanawiającego Wspólnotę Europejską).

wykonania decyzji przyjętych zgodnie z art. 29 *Traktatu o Unii Europejskiej*, aby zagwarantować ich jednolite stosowanie we wszystkich państwach członkowskich¹².

Unia Europejska nakłada środki ograniczające jako środki własne (tzn. sankcje autonomiczne) lub w celu realizacji rezolucji Rady Bezpieczeństwa Organizacji Narodów Zjednoczonych (ONZ) w przypadku gdy państwa trzecie, osoby fizyczne lub prawne, grupy lub podmioty niepaństwowe nie przestrzegają prawa międzynarodowego lub praw człowieka bądź prowadzą politykę lub działania sprzeczne z praworządnością lub zasadami demokracji. Po raz pierwszy takie autonomiczne sankcje Europejska Wspólnota Gospodarcza zastosowała w 1982 r. w odniesieniu do Związku Socjalistycznych Republik Radzieckich. Następnie były one nakładane na Chiny, Birmę (Mjanmę), Białoruś, Indonezję, Zimbabwe, Uzbekistan czy separatystyczne terytorium Naddniestrza. Jak podkreśla Piotr Kobza: *We wszystkich tych przypadkach Unia Europejska występowała jako „eksporter wartości europejskich”, zwłaszcza w dziedzinie demokracji, rządów prawa i praw człowieka*¹³.

Zgodnie z założeniami środki ograniczające powinny być nie tylko adekwatne do okoliczności nakazujących ich zastosowanie, lecz także stopniowalne, a ich nakładanie wiąże się z koniecznością osiągnięcia konsensusu politycznego na poziomie państw członkowskich. Bywa to jednak utrudnione ze względu na partykularne interesy państw¹⁴. Wśród podstawowych rodzajów sankcji pozostających w dyspozycji UE należy wskazać sankcje dyplomatyczne (takie jak wydalenie dyplomatów, zawieszenie oficjalnych wizyt, dwustronnej lub wielostronnej współpracy z UE, bojkot wydarzeń sportowych lub kulturalnych) oraz sankcje gospodarcze i finansowe (embarga na broń, ograniczenia przywozu i wywozu określonych produktów). Takie środki ograniczające mogą obejmować:

- zamrożenie środków finansowych i zasobów gospodarczych będących w posiadaniu lub pod kontrolą osób lub organizacji objętych sankcjami (np. gotówki, depozytów bankowych, udziałów, akcji),

¹² *Ogólne ramy dla sankcji unijnych*, <https://eur-lex.europa.eu/PL/legal-content/summary/general-framework-for-eu-sanctions.html> [dostęp: 26 X 2023].

¹³ P. Kobza, *Środki restrykcyjne jako instrument Wspólnej Polityki Zagranicznej i Bezpieczeństwa Unii Europejskiej*, „*Studia Europejskie*” 2006, nr 3, s. 22.

¹⁴ Zob. szerzej: P. Pospieszna, *Sankcje Unii Europejskiej wobec Rosji: proces decyzyjny, trwałość i rola państw członkowskich*, „*Rocznik Integracji Europejskiej*” 2018, nr 12, s. 311–321. <https://doi.org/10.14746/rie.2018.12.21>.

które nie mogą zostać przesunięte, sprzedane lub do których nie można uzyskać dostępu, oraz nieruchomości, których nie można sprzedać ani wynająć,

- zakaz wydawania wiz lub zakaz podróży uniemożliwiający osobom wjazd na teren UE,
- zakazy sektorowe, np. zakaz przywozu lub wywozu określonych towarów lub technologii¹⁵.

W kontekście problematyki omawianej w artykule podstawowe akty prawne na poziomie UE, w których środki ograniczające są scharakteryzowane, to:

- *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* (dalej: rozporządzenie 765/2006),
- *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* (dalej: rozporządzenie 269/2014),
- *Rozporządzenie Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie*.

Warto podkreślić, że rozporządzenie 765/2006 i rozporządzenie 269/2014 zawierają stosowane we wszystkich krajach członkowskich unijne listy osób i podmiotów, wobec których zostały wprowadzone środki ograniczające (zwane sankcjami) polegające na zamrażaniu aktywów tych podmiotów i osób w związku z działaniami Rosji wymierzonymi w Ukrainę oraz sytuacją w Białorusi. Ponadto te rozporządzenia stały się w Polsce podstawą do przyjęcia autonomicznych krajowych rozwiązań, które dotyczą szczególnych środków ograniczających względem osób i podmiotów wspierających działania władz rosyjskich i białoruskich, o czym szerzej w dalszej części artykułu.

Należy zauważyć, że w czasie przyjmowania przez Parlament Europejski rezolucji w sprawie uznania FR za państwo sponsorujące terroryzm, parlamenty lub poszczególne izby parlamentarne niektórych państw UE, tj. Litwy, Łotwy, Estonii, Polski i Czech, przyjęły już wcześniej krajowe odpowiedniki rezolucji, czyli dokumenty o charakterze deklaratywnym,

¹⁵ Tamże.

a nie normatywnym, uznające Rosję za państwo terrorystyczne lub sponsorujące terroryzm bądź obecny reżim rosyjski za terrorystyczny. W Polsce była to *Uchwała Senatu Rzeczypospolitej Polskiej z dnia 26 października 2022 r. o uznaniu władz Federacji Rosyjskiej za reżim terrorystyczny*. Wskazano w niej m.in., że:

Rosyjscy najeźdźcy terroryzują mieszkańców ukraińskich miast, bombardując cywilne cele: przedszkola, szkoły, teatry i osiedla mieszkaniowe. Bandyci w rosyjskich mundurach torturują i mordują jeńców wojennych oraz cywilów na okupowanych terytoriach. Uprawdają ukraińskie dzieci, by wychować je na reżimowych janczarów. Wywożą, przesiedlają i zsyłają ukraińskich obywateli na dalekie peryferia Rosji (...). Wszystkie te akty państwowego terroryzmu znamy dobrze z kart historii.

W związku z tym Senat (...) *z całą mocą potępia agresję rosyjską i wzywa wszystkie kraje opowiadające się za pokojem, demokracją i prawami człowieka do uznania władz Federacji Rosyjskiej za reżim terrorystyczny*¹⁶.

Niespełna dwa miesiące później Sejm podjął analogiczną uchwałę w sprawie uznania Federacji Rosyjskiej za państwo wspierające terroryzm¹⁷. Odwołał się w niej, podobnie jak wcześniej Parlament Europejski w rezolucji, m.in. do bezpośredniej odpowiedzialności Rosji za zestrzelenie samolotu malezyjskich linii lotniczych w lipcu 2014 r. czy dopuszczania się przez FR aktów terroru wymierzonych w infrastrukturę cywilną, zbiorowych egzekucji, uprowadzeń, przemocy seksualnej i tortur, odseparowywania dzieci od rodzin w celu poddania ich rusyfikacji, masowych deportacji ludności, przymusowego poboru obywateli Ukrainy do rosyjskich sił zbrojnych oraz rabunku mienia. Sejm wezwał Radę Ministrów do kontynuowania i intensyfikacji działań mających na celu nakładanie kolejnych pakietów sankcji na FR i osoby wspierające reżim Władimira Putina, a także dalsze materialne i polityczne wsparcie Ukrainy w walce z agresorem.

W Polsce odpowiedzią na działania Rosji oraz wspierającej ją Białorusi na poziomie już nie deklaratywnym, lecz normatywnym było przyjęcie *Ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie*

¹⁶ *Uchwała Senatu Rzeczypospolitej Polskiej z dnia 26 października 2022 r. o uznaniu władz Federacji Rosyjskiej za reżim terrorystyczny.*

¹⁷ *Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 14 grudnia 2022 r. w sprawie uznania Federacji Rosyjskiej za państwo wspierające terroryzm.*

bezpieczeństwa narodowego (dalej: ustawa sankcyjna). Na jej mocy został stworzony m.in. krajowy mechanizm umożliwiający zamrażanie środków finansowych, funduszy i zasobów gospodarczych osób i podmiotów związanych bezpośrednio lub pośrednio z reżimami w Rosji i w Białorusi, a spełniających określone kryteria tego powiązania. Te rozwiązania przyjęto wcześniej niż wspomnianą rezolucję Parlamentu Europejskiego oraz uchwały polskiego Sejmu i Senatu, były one natomiast ściśle skorelowane z obowiązującymi ówczasie, a następnie zmienianymi w ramach kolejnych unijnych pakietów sankcyjnych, rozporządzeniami 765/2006 i 269/2014. Późniejsze stosowanie ustawy wpisywało się we wskazane w przywołanych rezolucjach i uchwałach postrzeganie FR jako państwa wspierającego lub finansującego terroryzm, przez wykorzystanie jako jednego ze środków ograniczających mechanizmu zamrażania aktywów osób i podmiotów, a zatem typowego instrumentu stosowanego do przeciwdziałania finansowaniu terroryzmu i praniu pieniędzy, chociaż wykorzystywanego przez UE już wcześniej jako środek ograniczający w odniesieniu do innych państw. Sankcje wymierzone w terroryzm stanowią (...) *administracyjne, i równoległe (np. wobec konfiskaty mienia w procedurze karnej) działania instytucji obowiązanych, mające skutkować niemożnością skorzystania przez sprawców z aktywów na rzecz przestępczej działalności terrorystycznej*¹⁸.

Należy podkreślić, że samo pojęcie sankcji jest w tym wymiarze dużym uproszczeniem, które należy pochylić za skrót myślowy, mimo że zarówno wspomnianą ustawę, jak i prowadzoną na jej podstawie listę osób i podmiotów, wydawane na jej mocy decyzje czy stosowane środki ograniczające określa się zazwyczaj odpowiednio „ustawą sankcyjną”, „listą sankcyjną” „decyzjami sankcyjnymi” czy „środkami sankcyjnymi”. Jest to wykorzystywane również na potrzeby tego artykułu, a określeń tych powszechnie używa się także na poziomie UE, choćby w ramach wcześniej przywołanej rezolucji¹⁹. Cel, w jakim – na podstawie przyjętych w Polsce czy unijnych aktów prawnych – są stosowane instrumenty w postaci zamrażania środków finansowych, zasobów czy środków gospodarczych, ma

¹⁸ M.A. Kędziński, *Szczególne środki ograniczające i sankcje jako forma przeciwdziałania wobec podmiotów terrorystycznych na tle polskiego ustawodawstwa (część 1)*, „Prokuratura i Prawo” 2021, nr 10, s. 22–23.

¹⁹ Na temat relacji pojęć: sankcje, środki ograniczające, środki odwetowe na poziomie UE zob. szerzej: P. Kobza, *Środki restrykcyjne jako instrument...*, s. 10–14. Temat genezy pojęcia sankcji w wymiarze prawa międzynarodowego został podjęty w: M. Sułek, *Zachodnie sankcje wobec Rosji – sens i skuteczność*, „Rocznik Strategiczny” 2014/2015, t. 20, s. 398–400.

wymiar nie karzący, lecz zapobiegawczy, zatem bardziej adekwatne jest tu użycie, stosowanego zazwyczaj zamiennie, określenia „środek ograniczający”. Jego zastosowanie uniemożliwia transfer aktywów, które mogłyby zostać wykorzystane do finansowania agresji na Ukrainę czy łamania praw człowieka i zwalczania opozycji demokratycznej w Rosji i Białorusi, ale nie należy postrzegać go jako instrumentu karania takich podmiotów. Wprawdzie jego skutkiem może być np. uniemożliwienie prowadzenia działalności gospodarczej, jednak ma on w założeniu efekt tymczasowy. Podmiot objęty zamrożeniem środków nie naraża się na odpowiedzialność finansową w wymiarze karnym czy karno-administracyjnym, dopóki nie złamie nałożonego zakazu. W wymiarze polskim środki ograniczające stanowią unilateralny instrument polityki zagranicznej państwa (...) *polegający na podjęciu działań ograniczających lub zawieszających normalne stosunki z innym państwem, w odpowiedzi na jego nieakceptowalne działania, zarówno zewnętrzne, jak i wewnętrzne*²⁰.

Podobne spostrzeżenia zawarła KE w opinii z 19 czerwca 2020 r. w sprawie art. 2 rozporządzenia 269/2014 (odpowiedź na pytanie nr 2.5), zgodnie z którą:

Środki ograniczające nie mają charakteru represyjnego ani konfiskacyjnego, lecz stanowią instrumenty zapobiegawcze. Zgodnie z art. 4 ust. 1 lit. c rozporządzenia (269/2014 – dop. aut.), który ustanawia odstępstwo od ograniczeń finansowych określonych w art. 2, właściwe organy krajowe mogą wyrazić zgodę na zwolnienie określonych zamrożonych środków finansowych lub zasobów gospodarczych lub udostępnienie określonych środków finansowych lub zasobów gospodarczych po ustaleniu, że te środki finansowe i zasoby gospodarcze są przeznaczone wyłącznie na pokrycie opłat i należności za usługi polegające na zwykłym przechowywaniu lub utrzymywaniu zamrożonych środków finansowych lub zasobów gospodarczych²¹.

²⁰ Tamże.

²¹ *Opinia Komisji z dnia 19 czerwca 2020 r. w sprawie art. 2 rozporządzenia Rady (UE) nr 269/2014*, Bruksela, 19 VI 2020 r., C (2020) 4117 final, s. 6. Analogiczna opinia w tym zakresie została przedstawiona w pkt 28 dokumentu *Aktualizacja dobrych praktyk UE w zakresie skutecznego wprowadzania w życie środków ograniczających*, Bruksela, 4 V 2018 r., dokument nr 8519/18, <http://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/pl/pdf> [dostęp: 30 X 2023].

Założenia badawcze

Celem artykułu jest omówienie indywidualnych środków ograniczających wprowadzonych w Polsce ustawą sankcyjną oraz ukazanie ich relacji do mechanizmów zawartych w rozporządzeniach UE, a także przedstawienie skali i sposobu wykorzystania tych instrumentów w praktyce. Warty uwagi jest szczególnie charakter ustawy sankcyjnej, który został podkreślony już w samym tytule tego aktu prawnego. W tym kontekście nasuwają się pytania badawcze – na czym polega szczególnie charakter ustawy, czy należy postrzegać go z perspektywy okoliczności powstania tej regulacji czy też zakresu podmiotowego lub przedmiotowego jej normowania, a może zarówno materialnego, jak i proceduralnego charakteru zawartych w nim przepisów.

Wspomniane wcześniej postrzeżenie konfliktu w Ukrainie również w kontekście terroryzmu państwowego, a nie tylko z perspektywy militarnej, współgra ze stosowaniem podobnych mechanizmów zapobiegawczych, jakimi są środki związane z zamrażaniem aktywów typowe dla przeciwdziałania finansowaniu terroryzmu i praniu pieniędzy. Na gruncie polskim ten mechanizm został wprowadzony już wcześniej, tj. w *Ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, jednak w praktyce nie był on wykorzystywany. Pierwsze decyzje Generalnego Inspektora Informacji Finansowej (GIIF) w sprawie wpisu na listę osób i podmiotów, wobec których stosuje się szczególne środki ograniczające na podstawie tej ustawy²², wydano dopiero 26 września 2023 r., podczas gdy pierwsze decyzje na podstawie ustawy sankcyjnej – już 25 kwietnia 2022 r.

Ze względu na obszerność omawianego zagadnienia pominięto w artykule wartość oddzielnego i szczegółowego omówienia kwestię sieci zależności pomiędzy podmiotami i osobami, względem których zastosowano środki ograniczające. Nie odwołano się także do problematyki struktury bezpośrednich bądź pośrednich ich powiązań z aparatami państwowymi Rosji i Białorusi lub związanych z nimi osób i podmiotów gospodarczych. Warto zaznaczyć, że zakres ustawy wykracza poza kwestię indywidualnych środków ograniczających stosowanych względem konkretnych osób i podmiotów gospodarczych, których dotyczą rozwiązania przyjęte w tej ustawie. Obejmuje bowiem również sankcje sektorowe (związane z zakazem obrotu węglem pochodzenia rosyjskiego lub białoruskiego), przepisy

²² Na podstawie art. 104 § 1 *Ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego* w zw. z art. 120 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

zapewniające stosowanie wspomnianych rozporządzeń UE (tj. przepisy określające właściwość organów, przepisy proceduralne i przepisy sankcjonujące naruszenie unijnych środków ograniczających) oraz przepisy karne penalizujące stosowanie, używanie lub propagowanie symboli bądź nazw wspierających agresję FR na Ukrainę.

Problematyka wprowadzonych w Polsce indywidualnych środków ograniczających w kontekście agresji Rosji na Ukrainę i sytuacji w Białorusi, w przeciwieństwie do problematyki stosowania sankcji na poziomie UE czy ONZ, nie była w czasie przygotowania tego artykułu przedmiotem publikacji naukowych²³, dlatego źródłami są w tym przypadku ogólnie dostępne akty normatywne, wytyczne UE, decyzje ministra właściwego do spraw wewnętrznych, a także wyroki Wojewódzkiego Sądu Administracyjnego (WSA) w Warszawie oraz postanowienia Naczelnego Sądu Administracyjnego (NSA) wydawane w konkretnych sprawach (na dzień przygotowania publikacji NSA nie wydał jeszcze wyroków w omawianym zakresie).

Relacja między przyjętymi w Polsce a unijnymi indywidualnymi środkami ograniczającymi

Rozwiązania krajowe w zakresie określania indywidualnych środków ograniczających przyjęte w ustawie sankcyjnej opierają się na prowadzonej przez ministra właściwego do spraw wewnętrznych liście osób i podmiotów, wobec których są stosowane m.in. środki określone w art. 2 ust. 1–3 rozporządzenia 765/2006 oraz w art. 2 i art. 9 rozporządzenia 269/2014 (dalej: lista sankcyjna lub lista). Wpis na powszechnie dostępną i publikowaną w Biuletynie Informacji Publicznej (BIP)²⁴ listę jest poprzedzony wydaniem zindywidualizowanej i zaskarżalnej do sądu administracyjnego decyzji ministra właściwego do spraw wewnętrznych.

²³ W czasopiśmie „Prokuratura i Prawo” (2023, nr 6) ukazał się tekst Andrzeja Lewny pt. *Kiedy wojenny zapal może zaszkodzić. Kilka uwag o przestępstwie z art. 16 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego*, jednak nie dotyczy on omawianego w tym artykule zagadnienia indywidualnych środków ograniczających.

²⁴ *Lista osób i podmiotów objętych sankcjami*, Ministerstwo Spraw Wewnętrznych i Administracji, <https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami> [dostęp: 30 X 2023].

Zgodnie z przywołanym art. 2 ust. 1–3 rozporządzenia 765/2006 zamrożenie środków finansowych polega na zamrażaniu wszystkich funduszy (czyli zapobieganiu jakimkolwiek ich ruchom, przenoszeniu, zmianom, wykorzystaniu, udostępnianiu lub dokonywaniu nimi transakcji w sposób powodujący jakąkolwiek zmianę ich wielkości, wartości, lokalizacji, własności, posiadania, charakteru, przeznaczenia lub inną zmianę, która umożliwiłaby korzystanie z tych funduszy, w tym również zarządzanie portfelem²⁵), i zasobów gospodarczych będących własnością, pozostających w posiadaniu, faktycznym władaniu lub pod kontrolą osób fizycznych lub prawnych, podmiotów i organów wskazanych na liście sankcyjnej. Z tym że zasoby gospodarcze oznaczają aktywa każdego rodzaju, materialne i niematerialne, ruchome i nieruchome, które nie są funduszami, lecz mogą służyć do uzyskiwania funduszy, towarów lub usług. Zamrożenie zasobów gospodarczych to zapobieganie ich wykorzystaniu do uzyskiwania funduszy, towarów lub usług w jakikolwiek sposób, w tym – choć nie tylko – przez sprzedaż, wynajem lub ich obciążenie²⁶.

Zgodnie z rozporządzeniem 765/2006 nie mogą być udostępniane, bezpośrednio ani pośrednio, żadne fundusze ani zasoby gospodarcze wskazanym na liście osobom fizycznym lub prawnym, podmiotom i organom. Zakazuje się również świadomego i umyślnego udziału w działaniach, których celem lub skutkiem jest bezpośrednio lub pośrednio obejście środków ograniczających²⁷.

Nieco inny aparat pojęciowy, nieróżnicujący skutków regulacji, został użyty w art. 2 rozporządzenia 269/2014. Zgodnie z nim zamrożeniu podlegają wszystkie środki finansowe²⁸ (w rozporządzeniu 765/2006 mowa jest,

²⁵ Artykuł 1 pkt 2 rozporządzenia 765/2006.

²⁶ Artykuł 1 pkt 4 rozporządzenia 765/2006.

²⁷ Na podstawie uzasadnienia do *Rządowego projektu ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego*, Druk nr 2131, s. 6–8, <https://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=2131> [dostęp: 18 X 2023].

²⁸ Zgodnie z art. 1 pkt 1 rozporządzenia 765/2006 fundusze to aktywa finansowe i każdego rodzaju korzyści, w tym m.in. gotówka, czeki, roszczenia pieniężne, polecenia zapłaty, przekazy pieniężne i inne instrumenty płatnicze; depozyty złożone w instytucjach finansowych lub innych podmiotach, salda na rachunkach, długi i zobowiązania dłużne; papiery wartościowe i papiery dłużne w obrocie publicznym lub niepublicznym, w tym akcje i udziały, świadectwa papierów wartościowych, obligacje, weksle, warranty, skrypty dłużne, kontrakty pochodne; odsetki, dywidendy lub inne przychody z aktywów oraz wartości narosłe z aktywów lub wygenerowane przez te aktywa; kredyty, prawa do potrącenia, gwarancje,

jak wspomniano, o funduszach²⁹) i zasoby gospodarcze będące własnością, pozostające w posiadaniu, w faktycznym władaniu lub pod kontrolą wskazanych na liście osób fizycznych lub prawnych, podmiotów, organów lub powiązanych z nimi osób fizycznych lub prawnych, podmiotów lub organów wskazanych na liście sankcyjnej. Analogicznie żadne środki finansowe ani zasoby gospodarcze nie podlegają udostępnieniu – bezpośrednio lub pośrednio – wskazanym na liście osobom fizycznym lub prawnym, podmiotom lub organom ani powiązanim z nimi osobom fizycznym lub prawnym, podmiotom lub organom, ani też na ich rzecz.

W związku z tym, że ustawa sankcyjna odwołuje się wprost do rozporządzeń UE, komentarza wymaga relacja między oboma porządkami prawnymi. Jak stwierdzono w uzasadnieniu: *Projektowana ustawa, w oparciu o wybrane instrumenty prawne zawarte w rozporządzeniu 765/2006 oraz w rozporządzeniu 269/2014, pozwalała będzie na tworzenie na gruncie prawa krajowego odrębnej od wykazów zawartych w tych rozporządzeniach listy osób i podmiotów, wobec których stosuje się wybrane środki określone w tych rozporządzeniach*³⁰. Ustawa sankcyjna jest zatem samodzielny aktem prawa krajowego bazującym na unijnych mechanizmach stosowania indywidualnych środków ograniczających. Została w niej zawarta również norma zapobiegająca powielaniu nakładanych środków ograniczających, którą określono w art. 2 ust. 2. Zgodnie z tym przepisem zakres środków stosowanych wobec osób i podmiotów wpisanych na listę nie może powielać zakresu środków określonych w rozporządzeniu 765/2006 lub w rozporządzeniu 269/2014.

gwarancje właściwego wykonania umowy lub inne zobowiązania finansowe; akredytywy, listy przewozowe (konosamenty), kwity zastawne; dokumenty poświadczające posiadanie udziałów w funduszach lub środkach finansowych.

²⁹ Środki finansowe w rozumieniu art. 1 lit. g rozporządzenia 269/2014 oznaczają aktywa finansowe i dowolnego rodzaju korzyści, m.in. gotówkę, czeki, roszczenia pieniężne, weksle, przekazy pieniężne i inne instrumenty płatnicze; depozyty złożone w instytucjach finansowych lub innych podmiotach, salda na rachunkach, wierzytelności i zobowiązania dłużne; papiery wartościowe i papiery dłużne w obrocie publicznym lub niepublicznym, w tym akcje i udziały, certyfikaty papierów wartościowych, obligacje, weksle, warranty, skrypty dłużne, kontrakty na instrumenty pochodne; odsetki, dywidendy lub inne przychody z aktywów oraz wartości narosłe z aktywów lub wygenerowane przez te aktywa; kredyty, tytuły do przeprowadzania kompensat, gwarancje, gwarancje należytego wykonania umów lub inne zobowiązania finansowe; akredytywy, konosamenty, dokumenty poświadczające nabycie oraz dokumenty poświadczające udział w środkach finansowych lub zasobach finansowych.

³⁰ Uzasadnienie do *Rządowego projektu ustawy o szczególnych rozwiązaniach...*, s. 4.

Wprowadzenie obok prawa unijnego rozwiązań krajowych, w efekcie czego powstała oddzielna od list unijnych polska lista sankcyjna, wpisuje się w art. 4 ust. 2 *Traktatu o Unii Europejskiej* z dnia 7 lutego 1992 r., zgodnie z którym:

Unia szanuje równość Państw Członkowskich wobec Traktatów, jak również ich tożsamość narodową, nierozzerwalnie związaną z ich podstawowymi strukturami politycznymi i konstytucyjnymi, w tym w odniesieniu do samorządu regionalnego i lokalnego. Szanuje podstawowe funkcje państwa, zwłaszcza funkcje mające na celu zapewnienie jego integralności terytorialnej, utrzymanie porządku publicznego oraz ochronę bezpieczeństwa narodowego. W szczególności bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego Państwa Członkowskiego.

Na zasadność rozpatrywania ustawy z perspektywy bezpieczeństwa narodowego wskazuje już sam jej tytuł – (...) *służących ochronie bezpieczeństwa narodowego*, choć odwołania do tego pojęcia znajdują się również w poszczególnych przepisach wprost powołujących się na przesłankę bezpieczeństwa narodowego (art. 3 ust. 4 i art. 8 ustawy sankcyjnej).

Warto tu przywołać przyjętą także przez Radę UE *Aktualizację dobrych praktyk UE w zakresie skutecznego wprowadzania w życie środków ograniczających*, w której w pkt 25 jednoznacznie wskazano, że:

Oprócz prawodawstwa przyjętego przez Unię państwa członkowskie w razie potrzeby powinny dysponować dodatkowymi ramami prawnymi, przepisami ustawowymi lub wykonawczymi umożliwiającymi zamrażanie środków finansowych i aktywów finansowych oraz zasobów gospodarczych osób i podmiotów podlegających środkom ograniczającym na szczeblu krajowym, w tym osób lub podmiotów zaangażowanych w działalność terrorystyczną, i umożliwiających zakaz udostępniania środków finansowych i zasobów gospodarczych tym podmiotom i osobom lub na ich korzyść, w szczególności przez administracyjne środki zamrażające lub przez zastosowanie sądowych postanowień o zabezpieczeniu, mających te same skutki³¹.

Ten dokument wprowadzie nie ma charakteru normatywnego, ale stanowi podstawę wykładni stosowania środków ograniczających, w tym

³¹ *Aktualizacja dobrych praktyk UE...*

w odniesieniu do rozporządzeń 765/2006 i 269/2014. Co istotne w kontekście tych rozwiązań i poszukiwania analogii do rozwiązań przyjętych w zakresie przeciwdziałania finansowaniu terroryzmu, w dalszej części tego dokumentu podkreśla się, że rozwiązania dotyczące środków ograniczających powinny być zgodne ze standardami Grupy Specjalnej do spraw Przeciwdziałania Praniu Pieniędzy (The Financial Action Task Force, FATF), zwłaszcza z 6. zaleceniem w sprawie ukierunkowanych sankcji finansowych związanych z terroryzmem i finansowaniem terroryzmu. Realizację tych założeń na gruncie polskim stanowią właśnie ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu³² i ustawa sankcyjna.

Kwestię autonomiczności ustawy sankcyjnej względem rozporządzeń UE, mimo skorzystania w ustawodawstwie krajowym z mechanizmów zawartych w tych rozporządzeniach, podnosi również Minister Spraw Wewnętrznych i Administracji w wydawanych przez siebie decyzjach sankcyjnych:

Polska od początku stanowczo potępiła agresję Rosji na Ukrainę oraz łamanie praw człowieka na Białorusi, wskazując jednocześnie na konieczność zastosowania daleko idących i skutecznych sankcji, o szerokich konsekwencjach zarówno dla Federacji Rosyjskiej, jak i współpracującej z nią Białorusi. Z tych właśnie powodów podjęta została inicjatywa ustawodawcza, której efektem jest ustawa z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, która – jak należy ponownie podkreślić – bazując jedynie na mechanizmach sankcyjnych określonych w wymienionych rozporządzeniach unijnych – tworzy odrębne, krajowe rozwiązania sankcyjne³³.

Minister Spraw Wewnętrznych i Administracji nadmienił również, że:

(...) w szczególności bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego.

³² Zob. szerzej: M.A. Kędzierski, *Szczególne środki ograniczające i sankcje... (część 1)*; tegoż, *Szczególne środki ograniczające i sankcje jako forma przeciwdziałania wobec podmiotów terrorystycznych na tle polskiego ustawodawstwa (część 2)*, „Prokuratura i Prawo” 2021, nr 11, s. 36–55.

³³ Decyzja Ministra Spraw Wewnętrznych i Administracji z dnia 29 sierpnia 2023 r. DPP-T-PZ.0272.2.2023.AK(38), Decyzja odmowna – Timur Raszidow, s. 9, <https://www.gov.pl/web/mswia/decyzje-ministra-swia-w-sprawie-wpisu-na-liste-sankcyjna> [dostęp: 22 X 2023].

Zatem prawo europejskie nie wyłącza możliwości stosowania środków podejmowanych przez państwo członkowskie z uwagi na bezpieczeństwo narodowe, zwłaszcza przez państwo w tak szczególnej i trudnej sytuacji geopolitycznej jak Rzeczpospolita Polska, której nie doświadczają państwa położone z dala od strefy działań wojennych³⁴.

Ustawa sankcyjna jednak nie tylko tworzy odrębny krajowy system nakładania środków ograniczających na osoby i podmioty wspierające działania FR czy Białorusi, lecz także, w ramach przyjętych w niej przepisów, zapewnia stosowanie wspomnianych wcześniej rozporządzeń UE. W uzasadnieniu ustawy wskazano, że: *Wprowadzone po agresji Federacji Rosyjskiej na Ukrainę zmiany do rozporządzeń sankcyjnych wymagają podjęcia działań legislacyjnych związanych z jednoznacznym uregulowaniem kwestii organu podejmującego decyzje o odmrożeniu określonych środków finansowych lub zasobów gospodarczych*³⁵.

Obowiązki państw członkowskich w tym zakresie wynikają z prawa traktatowego. Zgodnie z art. 291 ust. 1 *Traktatu o funkcjonowaniu Unii Europejskiej* państwa członkowskie są zobowiązane do podjęcia wszelkich środków prawa krajowego niezbędnych do wprowadzenia w życie prawnie wiążących aktów Unii. Analogicznie w *Traktacie o Unii Europejskiej*, w art. 4 ust. 3 zdanie drugie, wskazano, że państwa członkowskie podejmują wszelkie środki ogólne lub szczególne właściwe dla zapewnienia wykonania zobowiązań wynikających z traktatów lub aktów instytucji Unii.

Zakres wykonywania przez ustawę sankcyjną rozporządzenia 269/2014 należy odnieść również do realizacji dyspozycji jego art. 15 ust. 1, zgodnie z którą (...) *państwa członkowskie przyjmują przepisy określające sankcje, w tym odpowiednio sankcje karne, mające zastosowanie w przypadkach naruszeń przepisów niniejszego rozporządzenia oraz przyjmują wszelkie środki niezbędne do zapewnienia ich stosowania*. Z kolei w art. 9 ust. 1 zdanie pierwsze rozporządzenia 765/2006 wskazano, że: *Państwa członkowskie określają zasady dotyczące sankcji mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia i podejmują wszelkie środki niezbędne w celu zapewnienia ich stosowania*. Przepisy te dotyczą zatem uregulowania kwestii właściwego organu, który podejmuje decyzje o odmrożeniu określonych środków finansowych lub zasobów gospodarczych i jest odpowiedzialny za nakładanie kar za nieprzestrzeganie nałożonych środków ograniczających.

³⁴ Tamże, s. 10.

³⁵ Uzasadnienie do *Rządowego projektu ustawy o szczególnych rozwiązaniach...*, s. 4.

Zakres wykonywania unijnych rozporządzeń sankcyjnych przez ustawę sankcyjną sprowadza się zatem do zmian wprowadzonych przez art. 19 tej ustawy w *Ustawie z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej*. W dodanym na tej podstawie m.in. *Dziale Va* SzeF Krajowej Administracji Skarbowej (KAS) został wskazany jako organ właściwy do podejmowania decyzji w kwestii stosowania odstępstw od indywidualnych środków ograniczających nałożonych na podstawie unijnych rozporządzeń sankcyjnych (zwalniania zamrożonych środków finansowych lub zasobów gospodarczych lub udostępniania środków finansowych lub zasobów gospodarczych) oraz nakładania kar pieniężnych za niezastosowanie się do tych środków.

Przyznane KAS uprawnienie do wyrażania zgody na zwolnienie określonych zamrożonych środków finansowych lub zasobów gospodarczych lub też na udostępnienie określonych środków finansowych lub zasobów gospodarczych w odniesieniu do osób i podmiotów objętych sankcjami jest stosowane po ustaleniu, że środki finansowe i zasoby gospodarcze, o których mowa, są m.in.:

- niezbędne do zaspokojenia podstawowych potrzeb osób fizycznych lub prawnych, podmiotów lub organów objętych sankcjami oraz członków rodzin pozostających na utrzymaniu takich osób fizycznych, w tym opłat za żywność, z tytułu najmu lub kredytu hipotecznego, za leki i leczenie, podatków, składek ubezpieczeniowych oraz opłat za usługi użyteczności publicznej,
- przeznaczone wyłącznie na pokrycie uzasadnionych honorariów lub zwrot wydatków związanych ze świadczeniem usług prawnych,
- przeznaczone wyłącznie na pokrycie opłat i należności za usługi polegające na zwykłym przechowywaniu lub utrzymywaniu zamrożonych środków finansowych lub zasobów gospodarczych.

Ponadto w art. 6 ustawy sankcyjnej wskazano m.in., że osoba lub podmiot, które w stosunku do osoby lub podmiotu wpisanych na listę nie dopełniają obowiązku zamrożenia środków finansowych, funduszy lub zasobów gospodarczych lub zakazu ich udostępniania, lub też nie stosują się do zakazu świadomego i celowego udziału w działaniach, których celem lub skutkiem jest ominięcie stosowania środków określonych w tych rozporządzeniach, podlegają karze pieniężnej w wysokości do 20 mln zł nakładanej przez naczelnika urzędu celno-skarbowego.

Indywidualne środki ograniczające przyjęte w Polsce

Zgodnie z art. 1 ustawy sankcyjnej wobec osób i podmiotów wpisanych na listę sankcyjną stosuje się:

- odpowiednio środki określone w art. 2 ust. 1–3 rozporządzenia 765/2006 (w związku z sytuacją w Białorusi i jej udziałem w agresji Rosji wobec Ukrainy), tj.:
 - zamraża się wszystkie fundusze i zasoby gospodarcze będące własnością, pozostające w posiadaniu, w faktycznym władaniu lub pod kontrolą osób fizycznych lub prawnych, podmiotów i organów wymienionych na liście sankcyjnej prowadzonej przez ministra właściwego do spraw wewnętrznych,
 - nie udostępnia się, bezpośrednio ani pośrednio, żadnych funduszy ani zasobów gospodarczych wymienionych na liście sankcyjnej osobom fizycznym lub prawnym, podmiotom i organom ani na ich rzecz,
 - zakazuje się świadomego i umyślnego udziału w działaniach, których celem lub skutkiem jest bezpośrednio lub pośrednio obejście ww. środków;
- odpowiednio środki określone w art. 2 i art. 9 rozporządzenia 269/2014 (w związku z działaniami Rosji), tj.:
 - zamraża się wszystkie środki finansowe i zasoby gospodarcze będące własnością, pozostające w posiadaniu, w faktycznym władaniu lub pod kontrolą wymienionych na liście sankcyjnej osób fizycznych lub prawnych, podmiotów lub organów lub powiązanych z nimi osób fizycznych lub prawnych, podmiotów lub organów,
 - nie udostępnia się wymienionym na liście sankcyjnej osobom fizycznym lub prawnym, podmiotom lub organom ani powiązanim z nimi osobom fizycznym lub prawnym, podmiotom lub organom, ani też na ich rzecz, bezpośrednio lub pośrednio, żadnych środków finansowych ani zasobów gospodarczych,
 - zakazuje się świadomego i umyślnego udziału w działaniach, których celem lub skutkiem jest obchodzenie ww. środków;
- wykluczenie z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie *Ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych*;
- wpis do wykazu cudzoziemców, których pobyt na terytorium RP jest niepożądany, o którym mowa w art. 434 *Ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach*.

Dwa pierwsze rodzaje indywidualnych środków ograniczających zaczerpnięto bezpośrednio z rozporządzeń UE i oba dotyczą mrożenia aktywów, różni je natomiast cel zastosowania (powiązanie z Białorusią lub Rosją). Pozostałe dwa mają odrębny charakter oparty na ustawodawstwie krajowym, tj. ustawie – prawo zamówień publicznych oraz ustawie o cudzoziemcach.

Podjętą ocenę charakteru przyjętych przez ustawodawcę indywidualnych środków ograniczających służących mrożeniu aktywów, za uzasadnieniem do projektu ustawy, należy wskazać, że:

(...) projekt dotyczy jedynie tzw. mrożenia majątków, a więc czasowej niemożności nim dysponowania. Nie oznacza to odjęcia własności, które na gruncie Konstytucji RP może być dokonane jedynie w ramach wywłaszczenia (na cel publiczny i za słusznym odszkodowaniem – art. 21 Konstytucji) lub przepadku (orzeczonego prawomocnym orzeczeniem sądu – art. 46 Konstytucji). Jest to działanie, które jest już przewidziane w ramach polskiego porządku prawnego, czy to przez bezpośrednio skuteczne rozporządzenie UE czy to przez ustawę o przeciwdziałaniu praniu brudnych pieniędzy i finansowaniu terroryzmu, i mieści się w zakrojonych przez Konstytucję RP ramach³⁶.

W tym kontekście warto zwrócić uwagę także na treść uzasadnienia wyroku WSA w Warszawie w sprawie wykreślenia z polskiej listy sankcyjnej jednego ze znajdujących się na niej podmiotów:

Ustawa z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, jest szczególnym aktem prawnym, gdyż reguluje wyjątkowo ważną kwestię, a mianowicie ma przeciwdziałać wspieraniu agresji na Ukrainę oraz służyć ochronie bezpieczeństwa narodowego. Te dwa główne cele stały się priorytetem dla ustawodawcy, i przez ich pryzmat należy odczytywać zapisy ustawy. Ewentualne negatywne skutki dla określonego podmiotu wpisanego na listę, nie mogą stanowić podstawy uchylecia decyzji gdyż byłoby to sprzeczne z ratio legis omawianej ustawy i nie służyło głównym jej celom. Oczywistym przy tym jest, że ustawa z dnia 13 kwietnia 2022 r. ma charakter represyjny, sankcyjny i trudno oczekiwać aby

³⁶ Uzasadnienie do *Rządowego projektu ustawy o szczególnych rozwiązaniach...*, s. 7.

zastosowanie jej zapisów do określonego podmiotu nie miało wywoływać negatywnych dla tego podmiotu skutków³⁷.

Ponadto w uzasadnieniu jednego z postanowień oddalającego zażalenie na brak wstrzymania wykonalności decyzji sankcyjnej NSA wskazał, że (...) *ustawa dotyczy tzw. „mrożenia majątku”, a więc czasowej niemożności dysponowania tym majątkiem. Nie oznacza to pozbawienia spółki prawa własności, które w świetle art. 21 ust. 2 Konstytucji RP z 2 kwietnia 1997. (Dz. U. nr 78, poz. 483 ze zm.) jest dopuszczalne jedynie wówczas, gdy jest dokonywane na cel publiczny i za słusznym odszkodowaniem lub przypadku orzeczonego prawomocnym orzeczeniem sądu (art. 46 Konstytucji RP)*³⁸.

Mrożenie środków finansowych, funduszy czy zasobów gospodarczych stanowi zatem podstawowy, ale nie jedyny instrument oddziaływania na osoby i podmioty, które znalazły się na polskiej liście sankcyjnej. W odniesieniu do nieprzewidzianej w rozporządzeniach 765/2006 i 269/2014 sankcji wykluczenia z postępowania lub konkursu prowadzonego na podstawie ustawy – prawo zamówień publicznych, kontrola udzielania zamówień jest wykonywana zgodnie z art. 596 tej ustawy, a podlegające wykluczeniu osoby lub podmioty przystępujące do postępowania o udzielenie zamówienia publicznego oraz konkursów podlegają karze pieniężnej w wysokości do 20 mln zł nakładanej przez Prezesa Urzędu Zamówień Publicznych.

Wykluczenie z postępowania lub konkursu dotyczy:

- wykonawcy oraz uczestnika konkursu wpisanego do wykazów określonych w rozporządzeniach 765/2006 i 269/2014,
- wykonawcy oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu jest osoba lub podmiot wymieniony w wykazach określonych w rozporządzeniach wymienionych w art. 1 ustawy albo wpisany na polską listę sankcyjną,
- wykonawcy oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 *Ustawy z dnia 29 września 1994 r. o rachunkowości* jest podmiot wymieniony w wykazach określonych w rozporządzeniach 765/2006 i 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r.,

³⁷ Wyrok WSA w Warszawie z 18 V 2023 r., sygn. I SA/Wa 2524/22. Analogiczna konstatacja znalazła się w innych wyrokach WSA w Warszawie, np. w wyroku WSA w Warszawie z 4 VII 2023 r., sygn. I SA/Wa 2528/22.

³⁸ Postanowienie NSA z 9 V 2023 r., sygn. III OZ 207/23.

o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na polską listę sankcyjną, rozstrzygającej o zastosowaniu omawianego środka³⁹.

W kontekście indywidualnego środka ograniczającego w postaci wpisu do wykazu cudzoziemców, których pobyt na terytorium RP jest niepożądany, warto zauważyć, że wpisu dokonuje z urzędu Prezes Urzędu do spraw Cudzoziemców w przypadku wskazania tego środka w decyzji wydanej przez Ministra Spraw Wewnętrznych i Administracji. Praktyka wydawania tych decyzji wskazuje, że w zdecydowanej większości ten instrument nie jest stosowany samodzielnie, lecz wspólnie z pozostałymi indywidualnymi środkami ograniczającymi, tj. zamrożeniem aktywów lub zakazem udziału w postępowaniach i konkursach prowadzonych na podstawie ustawy – prawo zamówień publicznych. Prezes Urzędu przekazuje przechowywane w wykazie dane cudzoziemca, na okres ich przechowywania w wykazie, do Systemu Informacyjnego Schengen w celu odmowy wjazdu i pobytu nie tylko w Polsce, lecz także na obszarze całej UE.

Przesłanki wpisu na polską listę sankcyjną

Najważniejszym zagadnieniem związanym z analizą polskich rozwiązań w zakresie indywidualnych środków ograniczających jest określenie przesłanek do wpisu na listę sankcyjną. Zgodnie z rozwiązaniami ustawowymi minister właściwy do spraw wewnętrznych podejmuje decyzję w sprawie wpisu względem osób i podmiotów dysponujących środkami finansowymi, funduszami oraz zasobami gospodarczymi w rozumieniu rozporządzenia 765/2006 lub rozporządzenia 269/2014, bezpośrednio lub pośrednio wspierających:

- 1) agresję Federacji Rosyjskiej na Ukrainę rozpoczętą w dniu 24 lutego 2022 r. lub
- 2) poważne naruszenia praw człowieka lub represje wobec społeczeństwa obywatelskiego i opozycji demokratycznej lub których działalność stanowi inne poważne zagrożenie dla demokracji lub praworządności w Federacji Rosyjskiej lub na Białorusi
 - lub bezpośrednio związanych z takimi osobami lub podmiotami, w szczególności ze względu na powiązania o charakterze osobistym, organizacyjnym, gospodarczym lub finansowym, lub wobec

³⁹ Artykuł 7 ust. 1 ustawy sankcyjnej.

których istnieje prawdopodobieństwo wykorzystania w tym celu dysponowanych przez nie takich środków finansowych, funduszy lub zasobów gospodarczych⁴⁰.

Analizując te przesłanki do wpisu na polską listę sankcyjną, warto zwrócić uwagę na orzecznictwo sądów administracyjnych. Wojewódzki Sąd Administracyjny w Warszawie w jednym z wyroków oddalających skargę na decyzję o wpisie na listę sankcyjną odniósł się do nich w ten sposób:

Z przytoczonego przepisu wynika więc, że ustawodawca przewidział, iż wpisowi na listę podlegać będą nie tylko podmioty bezpośrednio lub pośrednio wspierające agresję, lecz także wszelkie inne osoby lub podmioty o ile są bezpośrednio powiązane z podmiotami wspierającymi. Powiązania takie mogą mieć m.in. charakter osobisty lub gospodarczy, jednak użycie w analizowanym przepisie zwrotu „w szczególności”, oznacza, że podstawą wpisu na listę mogą być powiązania różnego rodzaju, o ile przypisać można im przymiot bezpośredniości.

W odniesieniu do kwestii form wspierania państw określonych w dyspozycji przepisu WSA w Warszawie w swym wyroku wskazał, że (...) *pośrednia lub pośrednia forma wspierania może oznaczać generowanie dowolnymi metodami zysków dla budżetu Federacji Rosyjskiej, które następnie mogą zostać wykorzystane na potrzeby działań wojennych prowadzonych przez Federację Rosyjską przeciwko Ukrainie, a także wykorzystywane do bezpośredniego lub pośredniego wsparcia poważnych naruszeń praw człowieka i represji społeczeństwa (...)*⁴¹.

Warto zwrócić uwagę na jeszcze jeden fragment dyspozycji przepisu określającego przesłanki do wpisu na polską listę sankcyjną: (...) *lub wobec których istnieje prawdopodobieństwo wykorzystania w tym celu dysponowanych przez nie takich środków finansowych, funduszy lub zasobów gospodarczych*. Nie jest zatem konieczne stwierdzenie zaistnienia czynu dokonanego, lecz samo prawdopodobieństwo wykorzystania środków finansowych, funduszy czy zasobów gospodarczych w określonym celu. To prawdopodobieństwo zaś jest uwiarygadniane przez zaistnienie różnego rodzaju powiązań. Zwrócił na to uwagę również WSA w Warszawie w wyroku oddalającym skargę na decyzję Ministra Spraw Wewnętrznych i Administracji: *Zauważyć trzeba, że powołany przepis wskazuje na „istnienie prawdopodobieństwa”*

⁴⁰ Artykuł 3 ust. 2 pkt 1 ustawy sankcyjnej.

⁴¹ Wyrok WSA w Warszawie z 17 V 2023 r., sygn. I SA/Wa 2522/22.

wykorzystywania środków finansowych, funduszy lub zasobów gospodarczych. Nie ma zatem (...) znaczenia prawnego, argumentacja strony skarżącej [wskazująca] na brak „udowodnienia” przez organ przekazywania określonych środków (...)”⁴². Wystarczające okazuje się zatem samo prawdopodobieństwo dokonania wsparcia. Włączenie przez ustawodawcę przesłanki o charakterze niedokonanym jest jednak niezbędne z perspektywy przedmiotu regulacji i warunkuje jej skuteczność. Dokonanego transferu w tym wypadku nie da się cofnąć, dlatego też jeśli założeniem jest odcięcie państw m.in. od źródeł dochodu, to musi być to działanie wyprzedzające i niezależne od tego, czy dana osoba bądź podmiot dokonywały tego już wcześniej, tj. przed dokonaniem ich wpisu na listę sankcyjną.

Szczególny charakter polskich postępowań w sprawach sankcji

Zgodnie z art. 3 ust. 1 ustawy sankcyjnej decyzje w sprawach wpisu na listę oraz wykreślenia z niej wydaje minister właściwy do spraw wewnętrznych. Wydaje je z urzędu lub na uzasadniony wniosek:

- Szefa Centralnego Biura Antykorupcyjnego,
- Szefa Agencji Bezpieczeństwa Wewnętrznego,
- Szefa Agencji Wywiadu,
- Szefa Służby Kontrwywiadu Wojskowego,
- Szefa Służby Wywiadu Wojskowego,
- Generalnego Inspektora Informacji Finansowej,
- Komendanta Głównego Policji,
- Komisji Nadzoru Finansowego,
- Prezesa Narodowego Banku Polskiego,
- Komendanta Głównego Straży Granicznej,
- Prokuratora Krajowego,
- Szefa Krajowej Administracji Skarbowej,
- Przewodniczącego komitetu Rady Ministrów właściwego w sprawach bezpieczeństwa i obrony państwa.

Uprawnienie dotyczące wnioskowania o dokonanie wpisu zostało przyznane służbom specjalnym mogącym pozyskiwać informacje o istniejących powiązaniach zarówno na podstawie czynności operacyjno-rozpoznawczych, jak i analityczno-informacyjnych czy, jak w przypadku CBA,

⁴² Wyrok WSA w Warszawie z 18 V 2023 r., sygn. I SA/Wa 2524/22.

w ramach czynności kontrolnych, oraz od służb partnerskich z innych krajów. Analiza dotychczasowych 507 decyzji⁴³ o wpisie na listę sankcyjną jednoznacznie wskazuje, że to te służby (kolejno ABW – 458⁴⁴, CBA – 36 i SKW – 8) skierowały do ministra właściwego do spraw wewnętrznych największą liczbę wniosków, na podstawie których wydano decyzje sankcyjne.

Uprawnienie to przysługuje ponadto dwóm służbom podległym ministrowi właściwemu do spraw wewnętrznych, tj. Policji – jako służbie pozyskującej informacje o przepływach finansowych czy gospodarczych w związku z podejrzeniem popełnienia przestępstwa – oraz Straży Granicznej – nie tylko jako służbie migracyjnej, lecz także realizującej zadania dotyczące określonych form przestępczości, w tym ekonomicznej. Z tego uprawnienia skorzystała jednak tylko Policja w trzech przypadkach. Wojewódzki Sąd Administracyjny w Warszawie w jednym z uzasadnień wyroku stwierdził, że te podmioty to (...) *wyspecjalizowane organy państwowe, które dysponują szczególnymi wiadomościami w zakresie porządku publicznego czy bezpieczeństwa państwa w różnych jego aspektach. Minister Spraw Wewnętrznych i Administracji orzeka zatem na podstawie wniosku specjalnego organu państwowego*⁴⁵.

Opisywaną kompetencję przyznano także innym podmiotom dysponującym wiedzą o transferach środków finansowych, tj. GIIF, KNF, Prezesowi NBP czy Szefowi KAS oraz, co wynika z właściwości prokuratury w sprawach prowadzenia lub nadzorowania postępowania przygotowawczego w sprawach karnych, Prokuratorowi Krajowemu, a także przewodniczącemu komitetu Rady Ministrów właściwego w sprawach bezpieczeństwa i obrony państwa, ze względu na funkcję koordynacyjną tego komitetu. Do czasu powstawania niniejszego artykułu nie wydano jednak decyzji o wpisie na listę sankcyjną na podstawie wniosków tych podmiotów. W dotychczasowych sprawach Minister Spraw Wewnętrznych i Administracji pięciokrotnie skorzystał ze swojego uprawnienia i z urzędu dokonał wpisu na listę sankcyjną.

Warto zaznaczyć, że wniosek uprawnionego organu o dokonanie wpisu, zgodnie z ustawą, musi uwzględniać wskazanie osoby lub podmiotu, względem których ma zostać wydana decyzja, a w przypadku decyzji

⁴³ Przytaczane w tekście dane przedstawiają stan na 1 stycznia 2024 r.

⁴⁴ W odniesieniu do trzech tych samych podmiotów wnioski złożyły zarówno ABW, jak i CBA.

⁴⁵ Wyrok WSA w Warszawie z 4 VII 2023 r., sygn. akt I SA/Wa 2528/22. Analogiczne stwierdzenia zawierały uzasadnienia wyroków WSA w Warszawie: z 18 V 2023 r., sygn. akt I SA/Wa 2524/22 oraz z 4 VII 2023 r., sygn. akt I SA/Wa 2528/22.

w sprawie wpisu na listę – również propozycję zastosowania określonych środków ograniczających. Nie musi ona polegać na prostym wyborze spośród czterech wyżej opisanych i określonych w art. 1 ustawy środków ograniczających. Sankcje w postaci zamrożenia mogą dotyczyć bowiem całości środków finansowych, funduszy czy zasobów gospodarczych związanych z daną osobą lub podmiotem bądź jedynie określonych ich składników.

Zgodnie z art. 3 ust. 4 ustawy sankcyjnej propozycję zastosowania środków sankcyjnych określa się z uwzględnieniem przede wszystkim charakteru i zakresu działalności prowadzonej przez osobę lub podmiot, struktury kapitałowej tego podmiotu oraz względów bezpieczeństwa narodowego. Szczególnie ostatnia z tych przesłanek wymusza na organie wnioskującym dokonanie oceny skutków ewentualnego wpisu na listę sankcyjną, chociaż ostateczna decyzja w tej sprawie należy do ministra właściwego do spraw wewnętrznych. Co istotne, w myśl art. 3 ust. 7 ustawy, wydając decyzję w sprawie wpisu na listę może on określić zakres środków finansowych, funduszy lub zasobów gospodarczych w rozumieniu rozporządzenia 269/2014 lub rozporządzenia 765/2006, objętych środkami, o których mowa w art. 1 pkt 1 lub 2 ustawy, tj. dotyczącymi mrożenia aktywów. Minister właściwy do spraw wewnętrznych ostatecznie decyduje nie tylko o dokonaniu wpisu na listę, czyli stwierdza, że dana osoba lub podmiot spełnia przesłanki do umieszczenia na liście sankcyjnej (lub wykreślenia z niej), lecz także o zakresie zastosowanych środków sankcyjnych. Odwołano się do tej kwestii w uzasadnieniu wyroku WSA w Warszawie w sprawie sankcyjnej, w którym sąd stwierdził, że: (...) *wyбір tych środków należy do organu administracji publicznej i o ile mieszczą się one w katalogu prawem przewidzianych, to nie ma podstaw do stwierdzenia wadliwości decyzji*⁴⁶.

W dalszej części artykułu autor przedstawia trzy przykłady różnego zastosowania zakresu określania sankcji dotyczącej mrożenia aktywów – od zamrożenia wszystkich środków finansowych i zasobów gospodarczych, przez zamrożenie jedynie środków finansowych zgromadzonych na rachunkach bankowych, aż po szczególne wyłączenie zakresu zamrożenia i jego powiązanie z czynnościami wykonywanymi w celu realizacji poleceń wydanych przez Prezesa Rady Ministrów w trybie art. 7a *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*.

⁴⁶ Wyrok WSA w Warszawie z 18 V 2023 r., sygn. akt I SA/Wa 2524/22.

Przykład pierwszy:

- a) zamrożenie wszystkich środków finansowych i zasobów gospodarczych,
- b) zakaz udostępniania podmiotowi wpisanemu na listę lub na jego rzecz – bezpośrednio lub pośrednio – jakichkolwiek środków finansowych lub zasobów gospodarczych,
- c) zakaz świadomego i umyślnego udziału w działaniach, których celem lub skutkiem jest ominięcie środków wskazanych w lit. a i b,
- d) wykluczenie z postępowania o udzielenie zamówienia publicznego lub konkursu⁴⁷.

Przykład drugi:

- a) zamrożenie środków finansowych zgromadzonych na rachunkach bankowych,
- b) zakaz świadomego i umyślnego udziału w działaniach, których celem lub skutkiem jest ominięcie środków wskazanych w lit. a,
- c) wykluczenie z postępowania o udzielenie zamówienia publicznego lub konkursu⁴⁸.

Przykład trzeci:

- a) zamrożenie wszystkich środków finansowych i zasobów gospodarczych,
- b) zakaz udostępniania podmiotowi wpisanemu na listę lub na jego rzecz – bezpośrednio lub pośrednio – jakichkolwiek środków finansowych lub zasobów gospodarczych,
- c) zakaz świadomego i umyślnego udziału w działaniach, których celem lub skutkiem jest ominięcie środków wskazanych w lit. a i b,
- d) wykluczenie z postępowania o udzielenie zamówienia publicznego lub konkursu.

W odniesieniu do środków określonych w literach a i b wyłącza się zakres związany z czynnościami wykonywanymi w celu realizacji

⁴⁷ Lista sankcyjna: SKA Assets Management Limited, <https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami> [dostęp: 27 X 2023].

⁴⁸ Lista sankcyjna: Cryogas M&T Poland Spółka Akcyjna, <https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami> [dostęp: 27 X 2023].

poleceń wydanych przez Prezesa Rady Ministrów w trybie art. 7a ustawy o zarządzaniu kryzysowym⁴⁹.

Szczególny charakter postępowania w sprawach sankcyjnych nie ogranicza się jednak do tego, że co do zasady jest ono inicjowane w praktyce przez organ wnioskujący, który nie jest stroną postępowania. Różni się ono od typowego postępowania administracyjnego w pełni opartego na *Ustawie z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego* (k.p.a.). Zgodnie bowiem z art. 4 ust. 1 ustawy sankcyjnej do postępowań w sprawach wpisu na listę oraz wykreślenia z niej, w zakresie nieuregulowanym w ustawie, mają zastosowanie tylko niektóre z przepisów k.p.a., np. art. 107 § 1. Przykładowo zgodnie z art. 107 § 1 pkt 6 k.p.a. decyzja zawiera w szczególności uzasadnienie faktyczne i prawne, co należy odczytywać w powiązaniu z art. 3 ust. 6 ustawy sankcyjnej. Zgodnie z nim decyzja w sprawie wpisu na listę zawiera datę wydania, oznaczenie osoby lub podmiotu, wobec których stosuje się środki sankcyjne, wraz z rozstrzygnięciem, który z tych środków ma do nich zastosowanie, uzasadnienie, oznaczenie organu wydającego, podstawę prawną decyzji, podpis osoby wydającej oraz pouczenie o prawie do wniesienia skargi do sądu administracyjnego. Należy jednak podkreślić, że przepis art. 4 ust. 1 ustawy sankcyjnej nie odsyła do art. 107 § 3 k.p.a., zgodnie z którym uzasadnienie faktyczne decyzji powinno w szczególności zawierać wskazanie faktów uznanych przez organ za udowodnione, dowodów, na których się oparł, oraz przyczyn, dla których innym dowodom odmówił wiarygodności i mocy dowodowej, uzasadnienie prawne zaś powinno zawierać wyjaśnienie podstawy prawnej decyzji, z przytoczeniem przepisów prawa. Przy tym zgodnie z art. 3 ust. 9 ustawy minister właściwy do spraw wewnętrznych może ograniczyć zakres uzasadnienia ze względu na bezpieczeństwo państwa lub porządek publiczny. Taka sytuacja występuje zwłaszcza w sprawach, w których są wykorzystywane materiały niejawne.

Do opisanego wyżej szczególnego charakteru tego postępowania odniósł się WSA w Warszawie w uzasadnieniu wyroku oddalającego skargę o wykreślenie podmiotu z listy sankcyjnej:

(...) postępowanie w sprawie wpisu na listę nie jest typowym postępowaniem administracyjnym, bowiem zgodnie z art. 4 ustawy z dnia 13 kwietnia 2022 r. do tego rodzaju postępowań stosuje się, w zakresie

⁴⁹ Lista sankcyjna: Novatek Green Energy Sp. z o.o., <https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami> [dostęp: 27 X 2023].

nieuregulowanym w ustawie, jedynie niektóre, szczegółowo wymienione, przepisy Kodeksu postępowania administracyjnego. (...) Wskutek powyższego, w postępowaniu toczącym się na podstawie przepisów ustawy z dnia 13 kwietnia 2022 r. organ nie jest zobowiązany oceniać, czy dana okoliczność została udowodniona, na podstawie całokształtu materiału dowodowego, zaś uzasadnienie decyzji nie musi zawierać wskazania faktów, które organ uznał za udowodnione, dowodów, na których się oparł, oraz przyczyn, z powodu których innym dowodom odmówił wiarygodności i mocy dowodowej. Powyższa konstatacja koresponduje również z treścią art. 3 ust. 9 ustawy z dnia 13 kwietnia 2022 r., który stanowi, że Minister może ograniczyć zakres uzasadnienia decyzji w sprawie wpisu na listę ze względu na bezpieczeństwo państwa lub porządek publiczny⁵⁰.

W dalszej części przytoczonego uzasadnienia do wyroku sąd podkreślił, że (...) *trudności w zebraniu pełnego materiału dowodowego dotyczącego podmiotów znajdujących się na terenie Białorusi lub Rosji niejednokrotnie będą powodowały, że wydając decyzję w sprawie wpisu na listę, organ będzie miał do dyspozycji jedynie ograniczony materiał dowodowy, na podstawie którego dokonywać będzie oceny spełnienia przesłanek wymienionych w art. 3 ust. 2 ustawy z dnia 13 kwietnia 2022 r.*⁵¹

O szczególnym charakterze tego postępowania świadczy także określony w art. 4 ust. 2 i 3 ustawy sankcyjnej sposób powiadomienia stron o decyzji organu i związania nią strony. Zawiadomienie stron o decyzjach następuje przez ich udostępnienie w BIP na stronie podmiotowej ministra właściwego do spraw wewnętrznych. Związanie organu wydaną przez siebie decyzją, rozpoczęcie biegu terminu do wniesienia skargi na decyzję oraz zaistnienie natychmiastowej wykonalności decyzji następuje z dniem następującym po dniu, w którym decyzja została udostępniona w BIP.

Konstrukcja przywołanego powyżej przepisu w zakresie doręczeń bazuje na art. 49 § 1 k.p.a., zgodnie z którym, jeżeli przepis szczególny tak stanowi, zawiadomienie stron o decyzjach i innych czynnościach organu administracji publicznej może nastąpić w formie publicznego obwieszczenia, w innej formie publicznego ogłoszenia zwyczajowo przyjętej w danej

⁵⁰ Wyrok WSA w Warszawie z 2 II 2023 r., sygn. I SA/Wa 2527/22. Analogiczny pogląd WSA w Warszawie wyraził w innych sprawach – wyrok z 18 V 2023 r., sygn. I SA/Wa 2524/22; wyrok z 4 VII 2023 r., sygn. I SA/Wa 2528/22; wyrok z 17 V 2023 r., sygn. I SA/Wa 2522/22; wyrok z 18 VI 2023 r., sygn. I SA/Wa 2541/22.

⁵¹ Wyrok WSA w Warszawie z 2 II 2023 r., sygn. I SA/Wa 2527/22.

miejscowości lub przez udostępnienie pisma w BIP na stronie podmiotowej właściwego organu administracji publicznej. Jednak w przeciwieństwie do rozwiązania z k.p.a. nie uwzględniono normy, zgodnie z którą w BIP wskazuje się dzień, kiedy udostępniono pismo, a zawiadomienie uważa się za dokonane po upływie 14 dni od dnia udostępnienia.

W postępowaniach sankcyjnych nie ma również zastosowania art. 61 § 4 k.p.a., zgodnie z którym o wszczęciu postępowania z urzędu lub na żądanie jednej ze stron należy zawiadomić wszystkie osoby będące stronami w sprawie. W tym postępowaniu strona dowiaduje się o jego wszczęciu względem niej dopiero w chwili wydania decyzji o wpisie na listę sankcyjną i to przez zamieszczenie decyzji w BIP. Z jednej strony powodem przyjęcia takiego rozwiązania jest zagrożenie, że wcześniejsze pozyskanie informacji o wszczęciu postępowania, tj. przed wydaniem decyzji, mogłoby skutkować ukryciem lub wyprowadzeniem środków finansowych, funduszy czy zasobów gospodarczych, które miałyby być przedmiotem zamrożenia. Z drugiej strony charakter podmiotów umieszczanych na liście, często mających swe siedziby np. w Rosji, Białorusi bądź na Cyprze, mógłby uniemożliwić doręczenie decyzji albo potwierdzenie doręczenia, czemu niezadowolona ze skutków strona mogłaby zaprzeczać. Należy również pamiętać, że decyzja, choć o indywidualnym charakterze, ma wpływ również na inne osoby i podmioty, np. banki zobowiązane do dokonania zamrożenia środków na koncie wpisanego na listę, dlatego jej zamieszczenie odbywa się w BIP, analogicznie jak w przypadku publikacji samej listy sankcyjnej⁵².

Uproszczone postępowanie na poziomie organu wydającego decyzję, a także jednoinstancyjność tego postępowania nie wyłącza jednak możliwości obrony ze strony osoby czy podmiotu wpisanych na listę. Zgodnie z art. 3 ust. 10 ustawy sankcyjnej od decyzji sankcyjnych nie można się odwołać przez złożenie wniosku o ponowne rozpatrzenie sprawy. Podlegają one natomiast zaskarżeniu do sądu administracyjnego⁵³. Skargę wnosi się za pośrednictwem Ministra Spraw Wewnętrznych i Administracji, w terminie 30 dni od udostępnienia decyzji w BIP na stronie podmiotowej ministra właściwego do spraw wewnętrznych. Wojewódzki Sąd Administracyjny

⁵² Zgodnie z art. 2 ust. 1 ustawy sankcyjnej lista osób i podmiotów, wobec których są stosowane środki, o których mowa w art. 1 tej ustawy, jest publikowana w BIP na stronie podmiotowej ministra właściwego do spraw wewnętrznych.

⁵³ Zgodnie z art. 16 § 2 k.p.a. oraz art. 3 § 2 pkt 1, art. 53 § 1 i art. 54 § 1 *Ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi*.

w Warszawie w uzasadnieniu jednego z wyroków podkreślił z jednej strony szczególnie charakter tego postępowania, z drugiej strony wskazał, że:

Nie oznacza to jednak, że taka osoba czy podmiot pozbawiona jest zupełnie ochrony prawnej. Od wydanej decyzji przysługuje bowiem skarga do sądu administracyjnego (art. 3 ust. 6 ustawy), a w toku postępowania przed sądem skarżący może przedstawić własną argumentację, zarzuty i wnioski. (...) Z uwagi również na sytuację geopolityczną spowodowaną głównie agresją Federacji Rosyjskiej na Ukrainę pewnym ograniczeniom podlegać musi swoboda prowadzenia działalności gospodarczej w sytuacji gdy istnieje prawdopodobieństwo, że środki z niej uzyskiwane mogłyby służyć jej wspieraniu i zagrażać interesowi społecznemu, bezpieczeństwu państwa⁵⁴.

Tymczasowy zarząd przymusowy

Przyjęcie w ustawie sankcyjnej rozwiązania w zakresie stosowania indywidualnych środków wynikających z unijnych rozporządzeń pozwoliło, o czym wspomniano wcześniej, na dokonywanie przez KAS zwolnienia określonych środków np. w celu umożliwienia ochrony prawnej spółki nimi objętej. Jednak pierwotne rozwiązanie uznano w szerszej perspektywie za niewystarczające, przede wszystkim w związku z tym, że w niektórych z zamrożonych spółek działających w Polsce zatrudniano pracowników i jednocześnie były one odpowiedzialne za produkcję towarów bądź technologii. Dlatego 18 sierpnia 2022 r. weszła w życie nowelizacja ustawy sankcyjnej wprowadzająca nowe instrumenty zabezpieczające⁵⁵. Za celowe uznano wprowadzenie rozwiązania pozwalającego na dalsze funkcjonowanie podmiotów, wobec których zastosowano zamrożenia na podstawie przepisów ustawy sankcyjnej. Miano na względzie z jednej strony potrzebę objęcia indywidualnymi środkami ograniczającymi podmiotów, które mogą być wykorzystywane do dysponowania środkami finansowymi, funduszami lub zasobami gospodarczymi w celu wspierania agresji FR na Ukrainę, a z drugiej strony interes społeczny i publiczny, w tym interes

⁵⁴ Wyrok z 4 VII 2023 r., sygn. I SA/Wa 2528/22; wyrok z 18 V 2023 r., sygn. I SA/Wa 2524/22.

⁵⁵ *Ustawa z dnia 5 sierpnia 2022 r. o zmianie ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego oraz ustawy o Krajowej Administracji Skarbowej.*

strony pracowników przedsiębiorstw prowadzonych przez podmioty gospodarcze objęte sankcjami⁵⁶.

Przyjęta zmiana uzupełniała dotychczasowe regulacje zawarte w ustawie sankcyjnej o instytucję tymczasowego zarządu przymusowego oraz o zapewnienie wsparcia pracownikom świadczącym pracę na rzecz podmiotów objętych sankcjami. Mimo że szczegółowe omówienie wprowadzonych instrumentów wykracza poza ramy niniejszego artykułu, warto zauważyć, że minister właściwy do spraw gospodarki może w formie decyzji ustanowić zarząd przymusowy względem podmiotu wpisanego na listę. Celem ustanowionego zarządu jest zbycie środków finansowych, funduszy lub zasobów gospodarczych, gdy okazuje się to niezbędne dla zapewnienia funkcjonowania podmiotu gospodarczego prowadzącego przedsiębiorstwo na terytorium RP i służy to:

- utrzymaniu miejsc pracy w tym przedsiębiorstwie lub
- utrzymaniu w zakresie działalności tego przedsiębiorstwa świadczenia usług użyteczności publicznej lub wykonywania innych zadań o charakterze publicznym, lub
- ochronie interesu ekonomicznego państwa⁵⁷.

Realizacja zadań przez zarządcę ma na celu dalsze sprawne funkcjonowanie przedsiębiorstwa podmiotu gospodarczego do czasu zbycia środków finansowych, funduszy lub zasobów gospodarczych objętych zarządem – czyli ich przejęcia przez kapitał niezwiązany z osobami i podmiotami wspierającymi rosyjską agresję. Środki ze sprzedaży są zamrożone na rachunkach dotychczasowych właścicieli objętych sankcjami.

Alternatywnym rozwiązaniem przyjętym w ustawie jest zastosowanie zarządu w celu przejęcia na rzecz Skarbu Państwa własności środków finansowych, funduszy lub zasobów gospodarczych należących do osoby albo podmiotu wpisanych na listę, jeżeli jest to niezbędne dla ochrony ważnego interesu publicznego, ochrony interesu ekonomicznego państwa lub dla zapewnienia bezpieczeństwa państwa.

⁵⁶ Uzasadnienie do *Rządowego projektu ustawy o szczególnych rozwiązaniach...*, s. 1–2.

⁵⁷ Artykuł 6a ust. 1 ustawy sankcyjnej.

Podsumowanie

Podsumowując rozważania, warto po raz kolejny przytoczyć uzasadnienie do jednego z wyroków WSA w Warszawie oddalających skargi na decyzje dotyczące wpisu na listę sankcyjną:

(...) agresja Federacji Rosyjskiej na Ukrainę, rozpoczęta w dniu 24 lutego 2022 r. spowodowała liczne zmiany na świecie, także w Polsce, związane z bezpieczeństwem narodowym, ale również skutkowałą podjęciem kroków prawnych w kwestii przeciwdziałania wspieraniu tej agresji. Ustawa z dnia 13 kwietnia 2022 r. jest tego wyrazem. (...) Od końca II wojny światowej na arenie europejskiej nie mieliśmy bowiem do czynienia z jawną agresją jednego państwa na drugie. Nie jest zatem pozbawione uzasadnienia działanie ustawodawcy w zakresie ograniczenia, uproszczenie postępowania administracyjnego w sprawach wpisu na listę osób i podmiotów wspierających agresję Federacji Rosyjskiej na Ukrainę rozpoczętej w dniu 24 lutego 2022 r.⁵⁸

Można stwierdzić, że bezsporny pozostaje szczególny charakter ustawy sankcyjnej uzasadniony okolicznościami i celem jej powstania, przy uwzględnieniu jednak podstawowych elementów gwarancyjnych wobec osoby lub podmiotu wpisywanego na listę. Z jednej strony bowiem podmiot inicjujący postępowanie zazwyczaj sam nie jest jego stroną, podmiotu zaś, którego postępowanie dotyczy, nie informuje się o jego wszczęciu, a jedynie o ewentualnie negatywnym dla niego skutku. Ponadto decyzje w sprawach sankcyjnych mają ograniczone uzasadnienia i wskutek tego nie wymagają przedstawienia całościowego materiału dowodowego stanowiącego podstawę ich wydania, ich doręczenie odbywa się przez ogólnodostępny BIP, a postępowanie jest jednoinstancyjne. Z drugiej strony podmiotowi czy osobie wpisanym na listę przysługuje prawo do wniesienia skargi do sądów administracyjnych, a dokonanie wpisu nie może być traktowane w kategoriach sankcji, czyli kary sensu stricto, ponieważ jest w rzeczywistości tymczasowym środkiem ograniczającym, mającym umożliwić udzielenie bezpośredniego lub pośredniego wsparcia dla działań władz FR i Białorusi. W tym kontekście przyjęte przez ustawodawcę rozwiązania spełniają wymogi konstytucyjne oraz wpisują się we wskazane wcześniej zalecenia UE, zgodnie z którymi państwa członkowskie powinny

⁵⁸ Wyrok WSA w Warszawie z 4 VII 2023 r., sygn. I SA/Wa 2528/22; wyrok z 18 V 2023 r., sygn. I SA/Wa 2524/22.

dysponować dodatkowymi, względem unijnych, ramami prawnymi umożliwiającymi zamrażanie środków finansowych i aktywów finansowych oraz zasobów gospodarczych osób i podmiotów podlegających środkom ograniczającym na szczeblu krajowym.

Dotychczasowe stosowanie tych rozwiązań dowodzi ich skuteczności jako autonomicznych względem unijnych instrumentów mrożenia, chociaż – co wskazano wcześniej – rozwiązania te częściowo opierają się na prawodawstwie europejskim. Niewątpliwie bezpośrednie sąsiedztwo Polski z Rosją i zaatakowaną przez nią Ukrainą oraz z Białorusią wymaga zastosowania dodatkowych środków, które wykraczałyby poza ogólnounijne rozwiązania oraz opierałyby się na konsensusie na poziomie UE. Jest to uzasadnione zarówno z perspektywy polskiej racji stanu, uwarunkowanej położeniem Polski i względami historycznymi, jak i z perspektywy bezpieczeństwa narodowego. Skala nie tylko zaangażowania Polski w pomoc Ukrainie, lecz także zagrożenia RP i jej mieszkańców, z racji sąsiedztwa z tymi państwami, jest oczywiście inna niż w przypadku oddalonych od strefy konfliktu państwach np. Półwyspu Iberyjskiego.

Warto zwrócić uwagę na efekty stosowania indywidualnych krajowych środków ograniczających, o których mowa w ustawie sankcyjnej. Na prowadzonej przez MSWiA liście sankcyjnej w dniu 1 stycznia 2024 r. znajdowało się 498 osób i podmiotów (425 osób oraz 73 podmioty). Do WSA w Warszawie skierowano łącznie 64 skargi na decyzje Ministra Spraw Wewnętrznych i Administracji, w tym 56 skarg na decyzje w sprawach wpisu na listę sankcyjną, siedem skarg na decyzje o odmowie wykreślenia z listy oraz jedną na decyzję zmieniającą decyzję w sprawie wpisu na listę. Ponadto Minister Spraw Wewnętrznych i Administracji podjął dziewięć decyzji o wykreśleniu z listy sankcyjnej osób lub podmiotów. Dwie z nich zostały wydane z uwagi na następcze umieszczenie objętych nimi jednej osoby i jednego podmiotu w załączniku I do rozporządzenia 269/2014 (wykreślenie było spowodowane koniecznością uniknięcia powielania się sankcji krajowych i unijnych). W odniesieniu do siedmiu podmiotów natomiast decyzję o wykreśleniu z listy podjęto ze względu na zaistnienie nowych okoliczności faktycznych, tj. zmianę struktury właścicielskiej, a więc zniesienie powiązania z osobą lub podmiotem stanowiącymi powód umieszczenia na liście. Ten przypadek dobrze obrazuje rzeczywistą rolę indywidualnych środków ograniczających jako środków tymczasowych, których celem jest ograniczenie lub zniesienie powiązania ze strukturami państwowymi Rosji lub Białorusi, a nie trwałe wyeliminowanie danego podmiotu z obrotu gospodarczego.

Wojewódzki Sąd Administracyjny w Warszawie na dzień 1 stycznia 2024 r. rozpatrzył 21 skarg dotyczących wydania przez Ministra Spraw Wewnętrznych i Administracji decyzji o wpisie na listę sankcyjną, decyzji odmawiającej wykreślenia z listy sankcyjnej, decyzji zmieniającej zakres zastosowanych indywidualnych środków ograniczających bądź decyzji o wykreśleniu z listy. Wszystkie z nich oddalono, co potwierdza prawidłowość całego procesu decyzyjnego związanego z objęciem środkami ograniczającymi określonych osób i podmiotów. Ponadto trzy skargi do WSA zostały wycofane przez skarżącego, a w kolejnych czterech przypadkach sąd odrzucił skargi ze względów formalnych (wniesiono je po terminie). Zaskarżone decyzje w sprawie wpisu na listę dwóch podmiotów stały się prawomocne. Cztery podmioty (w tym jeden w dwóch sprawach) i trzy osoby wniosły skargi kasacyjne do NSA.

Na podstawie krajowych i unijnych indywidualnych środków ograniczających KAS zamroziła na terytorium Polski aktywa o łącznej wartości ok. 1,21 mld euro⁵⁹ (sposób prowadzenia statystyki w tym zakresie nie pozwala na wyodrębnienie oddzielnych wartości dla unijnych i krajowych środków ograniczających). Ponadto minister właściwy do spraw gospodarki zastosował zarząd przymusowy wobec siedmiu podmiotów.

Przytoczone dane pokazują szerokie zastosowanie rozwiązań przyjętych w ustawie sankcyjnej oraz wskazują na ich skuteczność. Tym samym zostaje spełniona wytyczna Rady UE dotycząca potrzeby przyjęcia krajowych rozwiązań w zakresie indywidualnych środków ograniczających, zgodnie z którą:

Środki te powinny umożliwić krajowym organom bezzwłoczne nakazywanie i realizację zamrażania wszelkich środków finansowych i zasobów gospodarczych w ramach jurysdykcji państwa członkowskiego, którego to dotyczy, należących do wyznaczonej osoby lub podmiotu będących ich własnością, kontrolowanych lub posiadanych przez nie oraz mogłyby być również skierowane do osób lub podmiotów pochodzących z Unii Europejskiej i prowadzących tam główną działalność⁶⁰.

Inną kwestią jest ocena tego, czy rozwiązania przyjęte przez polskiego ustawodawcę są rozwiązaniami docelowymi. Biorąc pod uwagę już sam tytuł ustawy sankcyjnej, negatywna odpowiedź na to pytanie wydaje się dość

⁵⁹ Stan na dzień 30 września 2023 r.

⁶⁰ *Aktualizacja dobrych praktyk UE...*, pkt 26.

oczywista. Ustawa określa bowiem szczególne rozwiązania jedynie w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz w kontekście naruszeń praw człowieka w Rosji i Białorusi i nie zapewnia możliwości jej stosowania w innych okolicznościach. Ustanowione w niej mechanizmy, zarówno te wprowadzające autonomiczny krajowy system indywidualnych środków ograniczających, jak i te, które mają zapewnić stosowanie sankcji unijnych (jak wskazanie organu właściwego w zakresie zapobiegania omijania tych sankcji czy wprowadzenie przepisów penalizujących naruszenie sankcji UE), są ograniczone wyłącznie do działań FR i Białorusi lub wprost wskazanych rozporządzeń UE. Tymczasem ONZ i UE wprowadzają środki ograniczające w stosunku do wielu innych państw z uwagi na nieprzestrzeganie przez nie prawa międzynarodowego lub praw człowieka czy też prowadzenie przez nie polityki lub działań sprzecznych z praworządnością lub zasadami demokracji. W tym wypadku Polska jest już pozbawiona instrumentów prawnego oddziaływania analogicznych do tych wprowadzonych ustawą sankcyjną. W efekcie nie ma możliwości nie tylko nałożenia własnych środków, lecz przede wszystkim zapewnienia skutecznego stosowania unijnych środków ze względu na niewskazanie organu właściwego w tych sprawach oraz nieokreślenie sankcji karnej za ominięcie tych środków. Wyjątek stanowią kwestie związane z zapobieganiem terroryzmowi i unormowania wynikające ze wspomnianej wcześniej ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Poruszone zagadnienie zasługuje na oddzielne opracowanie, oparte zwłaszcza na analizie przepisów obowiązujących w innych państwach. Dla przykładu warto przywołać rozwiązania przyjęte w Republice Czeskiej ustawą nr 1/2023 w sprawie środków ograniczających wobec niektórych poważnych czynów stosowanych w stosunkach międzynarodowych⁶¹, która weszła w życie 3 stycznia 2023 r. Aby podmiot znalazł się na czeskiej krajowej liście sankcyjnej, musi zostać spełniona przesłanka wynikająca z jednego z unijnych reżimów sankcyjnych. Inny warunek to zaistnienie sytuacji, w której stosowanie środków ograniczających wobec konkretnej osoby fizycznej lub prawnej jest zgodne z interesem polityki zagranicznej lub bezpieczeństwem Republiki Czeskiej. Nie dotyczy to zatem środków ograniczających wprowadzonych przez UE wyłącznie w odniesieniu do Rosji

⁶¹ *Zákon o omezujících opatřeních proti některým závažným jednáním uplatňovaným v mezinárodních vztazích (sankční zákon)*, https://www.mzv.cz/jnp/cz/o_ministerstvu/legislativa/pravni_predpisy_v_pusobnosti_mzv/zakon_c_1_2023_sb_o_omezujících.html [dostęp: 27 XI 2023].

i Białorusi, lecz także względem wszystkich innych państw, w stosunku do których UE podjęłaby takie decyzje. Lista krajowa jest w tym rozwiązaniu uzupełnieniem unijnych mechanizmów sankcyjnych i stosuje się ją wtedy, gdy dyskusja na szczeblu unijnym zajmuje dużo czasu lub gdy istnieje ryzyko, że jej cel nie zostanie osiągnięty. Analogicznie jak w przypadku polskiej ustawy sankcyjnej wpisanie osoby na listę sankcyjną UE co do zasady skutkuje skreśleniem tej osoby z listy krajowej (w przypadku gdy przyczyny umieszczenia osób na obu listach są tożsame). W wyjątkowych sytuacjach, jeśli Czechy zastosują wobec takiej osoby sankcje w większym stopniu niż UE, ta osoba pozostanie na liście krajowej właśnie ze względu na środki ograniczające, które wykraczają poza określone sankcje UE.

Na gruncie polskiego prawa warte rozważenia byłoby wykorzystanie w szerszym kontekście skutecznych rozwiązań przyjętych ustawą sankcyjną oraz doświadczeń wynikających z jej stosowania. Służyłoby to podjęciu prac nad ustawą wprowadzającą stałe rozwiązania pozwalające na stosowanie indywidualnych środków ograniczających w zależności od zmieniającej się sytuacji międzynarodowej. Stosowane byłyby one w odniesieniu do osób i podmiotów wspierających inne (nieujęte w ustawie sankcyjnej) reżimy państwowe, w stosunku do których wspólnota międzynarodowa, w tym UE, wprowadza sankcje.

Bibliografia

Kędzierski M.A., *Szczególne środki ograniczające i sankcje jako forma przeciwdziałania wobec podmiotów terrorystycznych na tle polskiego ustawodawstwa (część 1)*, „Prokuratura i Prawo” 2021, nr 10, s. 20–45.

Kędzierski M.A., *Szczególne środki ograniczające i sankcje jako forma przeciwdziałania wobec podmiotów terrorystycznych na tle polskiego ustawodawstwa (część 2)*, „Prokuratura i Prawo” 2021, nr 11, s. 36–55.

Kobza P., *Środki restrykcyjne jako instrument Wspólnej Polityki Zagranicznej i Bezpieczeństwa Unii Europejskiej*, „Studia Europejskie” 2006, nr 3, s. 9–31.

Lewna A., *Kiedy wojenny zapal może zaszkodzić. Kilka uwag o przestępstwie z art. 16 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego*, „Prokuratura i Prawo” 2023, nr 6, s. 86–101.

Pospieszna P., *Sankcje Unii Europejskiej wobec Rosji: proces decyzyjny, trwałość i rola państw członkowskich*, „Rocznik Integracji Europejskiej” 2018, nr 12, s. 311–321. <https://doi.org/10.14746/rie.2018.12.21>.

Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz, J. Grynfelder i in. (red.), Warszawa 2020.

Sulek M., *Zachodnie sankcje wobec Rosji – sens i skuteczność*, „Rocznik Strategiczny” 2014/2015, t. 20, s. 398–410.

Źródła internetowe

Sejm uznał Rosję za państwo wspierające terroryzm, 14 XII 2022 r., <https://www.sejm.gov.pl/sejm9.nsf/komunikat.xsp?documentId=4774505381CECC10C1258918007022FA> [dostęp: 25 X 2023].

Akty prawne

Europejska konwencja o zwalczaniu terroryzmu, sporządzona w Strasburgu dnia 27 stycznia 1977 r. (DzU z 1996 r. nr 117 poz. 557).

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

Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana) – (Dz. Urz. UE C 202/47 z 7 VI 2016 r.).

Traktat o Unii Europejskiej (wersja skonsolidowana) – (Dz. Urz. UE C 202/13 z 7 VI 2016 r.).

Rzymski Statut Międzynarodowego Trybunału Karnego sporządzony w Rzymie dnia 17 lipca 1998 r. (DzU z 2003 r. nr 78 poz. 708).

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 (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.).

Rozporządzenie Rady (WE) nr 2580/2001 z 27 grudnia 2001 r. w sprawie szczególnych środków restrykcyjnych skierowanych przeciwko niektórym osobom i podmiotom mających na celu zwalczanie terroryzmu (Dz. Urz. UE L 344/70 z 28 XII 2001 r.).

Opinia Komisji z dnia 19 czerwca 2020 r. w sprawie art. 2 rozporządzenia Rady (UE) nr 269/2014, Bruksela, 19 VI 2020 r., C (2020) 4117 final.

Ustawa z dnia 5 sierpnia 2022 r. o zmianie ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego oraz ustawy o Krajowej Administracji Skarbowej (DzU z 2022 r. poz. 1713).

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 i 1859).

Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. DzU z 2023 r. poz. 1605, 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 16 listopada 2016 r. o Krajowej Administracji Skarbowej (t.j. DzU z 2023 r. poz. 615, ze zm.).

Ustawa z dnia 12 grudnia 2013 r. o cudzoziemcach (t.j. DzU z 2023 r. poz. 519, ze zm.).

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

Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j. DzU z 2023 r. poz. 1634, ze zm.).

Ustawa z dnia 29 września 1994 r. o rachunkowości (t.j. DzU z 2023 r. poz. 120, ze zm.).

Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. DzU z 2023 r. poz. 775).

Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 14 grudnia 2022 r. w sprawie uznania Federacji Rosyjskiej za państwo wspierające terroryzm (M.P. z 2022 r. poz. 1253).

Uchwała Senatu Rzeczypospolitej Polskiej z dnia 26 października 2022 r. o uznaniu władz Federacji Rosyjskiej za reżim terrorystyczny (M.P. z 2022 r. poz. 1043).

Zákon o omezujících opatřeních proti některým závažným jednáním uplatňovaným v mezinárodních vztazích (sankční zákon), https://www.mzv.cz/jnp/cz/o_ministerstvu/legislativa/pravni_predpisy_v_pusobnosti_mzv/zakon_c_1_2023_sb_o_omezujících.html [dostęp: 27 XI 2023].

Orzecznictwo

Postanowienie Naczelnego Sądu Administracyjnego w Warszawie z 9 V 2023 r., sygn. III OZ 207/23.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 4 VII 2023 r., sygn. I SA/Wa 2528/22.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 18 VI 2023 r., sygn. I SA/Wa 2541/22.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 18 V 2023 r., sygn. I SA/Wa 2524/22.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 17 V 2023 r., sygn. I SA/Wa 2522/22.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 2 II 2023 r., sygn. I SA/Wa 2527/22.

Inne dokumenty

Aktualizacja dobrych praktyk UE w zakresie skutecznego wprowadzania w życie środków ograniczających, Bruksela, 4 V 2018 r., dokument nr 8519/18, <http://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/pl/pdf> [dostęp: 30 X 2023].

Decyzja Ministra Spraw Wewnętrznych i Administracji z dnia 29 sierpnia 2023 r. DPP-TPZ.0272.2.2023.AK(38), Decyzja odmowna – Timur Raszidow, <https://www.gov.pl/web/mswia/decyzje-ministra-swia-w-sprawie-wpisu-na-liste-sankcyjna> [dostęp: 22 X 2023].

Lista osób i podmiotów objętych sankcjami, Ministerstwo Spraw Wewnętrznych i Administracji, <https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami> [dostęp: 27 X 2023].

Ogólne ramy dla sankcji unijnych, <https://eur-lex.europa.eu/PL/legal-content/summary/general-framework-for-eu-sanctions.html> [dostęp: 26 X 2023].

Rezolucja Parlamentu Europejskiego z dnia 23 listopada 2022 r. w sprawie uznania Federacji Rosyjskiej za państwo sponsorujące terroryzm (2022/2896(RSP)) – (Dz. Urz. UE C 167/18 z 11 V 2023 r.), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0405_PL.html [dostęp: 27 IX 2023].

Rezolucja Parlamentu Europejskiego z dnia 6 października 2022 r. w sprawie eskalowania przez Rosję wojny napastniczej przeciwko Ukrainie (2022/2851(RSP)) – (Dz. Urz. UE C 132/94 z 14 IV 2023 r.), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0353_PL.html [dostęp: 27 IX 2023].

Rezolucja Parlamentu Europejskiego z dnia 19 maja 2022 r. w sprawie zwalczania bezkarności za zbrodnie wojenne w Ukrainie (2022/2655(RSP)) – (Dz. Urz. UE C 479/68 z 16 XII 2022 r.), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0218_PL.html [dostęp: 27 IX 2023].

Rezolucja Parlamentu Europejskiego z dnia 25 listopada 2021 r. w sprawie przypadków łamania praw człowieka przez prywatne firmy wojskowe i ochroniarskie, zwłaszcza Wagner Group (2021/2982(RSP)) – (Dz. Urz. UE C 224/104 z 8 VI 2022 r.), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=uriserv%3AOJ.C_.2022.224.01.0104.01.POL&toc=OJ%3AC%3A2022%3A224%3ATOC [dostęp: 27 IX 2023].

Uzasadnienie do Rządowego projektu ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, Druk nr 2131, <https://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=2131> [dostęp: 23 X 2023].

Wspólne stanowisko Rady 2001/931/WPZiB z 27 grudnia 2001 r. w sprawie zastosowania szczególnych środków w celu zwalczania terroryzmu (Dz. Urz. UE L 344/93 z 28 XII 2001 r.), <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:02001E0931-20171115> [dostęp: 30 X 2023].

Mariusz Cichomski

Prawnik, socjolog. Zajmuje się zagadnieniami związanymi z terroryzmem, przestępczością zorganizowaną, nadzorem nad działalnością służb, legislacją w zakresie bezpieczeństwa oraz sprawami dotyczącymi stosowania środków ograniczających. Autor ponad trzydziestu publikacji z zakresu bezpieczeństwa, w szczególności w wymiarze prawnym, i z socjologii.

Duże modele językowe i możliwości ich wykorzystania w terroryzmie dżihadystycznym i przestępczości

Large Language Models in jihadist terrorism and crimes

JULIA PUCZYŃSKA

IDEAS NCBR

Szkoła Doktorska Technologii Informatycznych
i Biomedycznych Instytutów PAN

 <https://orcid.org/0009-0009-5304-7092>

MARCIN PODHAJSKI

IDEAS NCBR

Szkoła Doktorska Technologii Informatycznych
i Biomedycznych Instytutów PAN

 <https://orcid.org/0009-0001-1350-879X>

KAROLINA WOJTASIK

Polskie Towarzystwo Bezpieczeństwa Narodowego

 <https://orcid.org/0000-0002-1215-5005>

TOMASZ P. MICHALAK

IDEAS NCBR

Wydział Matematyki, Informatyki i Mechaniki
Uniwersytet Warszawski

 <https://orcid.org/0000-0002-5288-0324>

Abstrakt

W artykule autorzy omawiają duże modele językowe (ang. *Large Language Models*, LLMs) w kontekście zagrożeń bezpieczeństwa wynikających z funkcji i dostępności tych modeli. Mimo że pod względem zastosowań LLMs wydają się podobne do wyszukiwarek internetowych, to generują nowe zagrożenia związane z dostarczaniem przez nie przestępcy i terroryści podstawowych umiejętności analitycznych i programistycznych. Autorzy dowodzą, że dostępne modele językowe nie tylko zmniejszają bariery finansowe dla różnych działań przestępczych, lecz także obniżają poziom wiedzy specjalistycznej i zaangażowania wymagany

od jednostek lub małych grup do popełniania przestępstw, w tym aktów terrorystycznych. Z drugiej strony możliwości tych modeli mogą wykorzystać również organy ścigania, aby być przygotowanymi na pojawiające się zagrożenia.

Słowa kluczowe

Large Language Models, bezpieczeństwo, cyberprzestępczość, terroryzm dżihadystyczny, sztuczna inteligencja

Abstract

The authors discuss Large Language Models in the context of the security risks associated with their functions and availability. Even though their applications seem to be similar to search engines and internet access, the true danger posed by Large Language Models lies in basic analytical and programming skills they provide to any criminal or terrorist. They assert that accessible Large Language Models not only diminish financial barriers to various criminal activities but also lower the expertise and commitment required by individuals or small groups to commit crimes, and acts of terror in particular. On the other hand, however, also law enforcement agencies can harness the capabilities of these models to stay ahead of emerging threats.

Keywords

Large Language Models, security, cybercrime, jihadist terrorism, artificial intelligence

Wstęp

Szybki rozwój sztucznej inteligencji (ang. *Artificial Intelligence*, AI) przyniósł innowacje przeobrażające różne obszary życia. Wśród nowinek pokazujących skalę postępu technologicznego są duże modele językowe (ang. *Large Language Models*, LLMs), takie jak ChatGPT, który w 2023 r. stał się światowym fenomenem. W artykule autorzy podejmują się analizy LLMs w kontekście bezpieczeństwa, ukazując zawiłości ich konstrukcji i funkcji oraz szeroki zakres możliwości, jakie oferują.

W odniesieniu do bezpieczeństwa najpoważniejszym problemem wynikającym z nagłego wzrostu zainteresowania LLMs jest ich potencjalne

wykorzystanie przez przestępców, terrorystów oraz podmioty państwowe zaangażowane w wojnę hybrydową. Autorzy artykułu analizują możliwe scenariusze, aby pokazać skalę wyzwań związanych z LLMs. Stwierdzają, że dostępne modele, zwłaszcza ChatGPT, nie tylko redukują bariery finansowe w różnych działaniach przestępczych, lecz także obniżają próg wiedzy i zaangażowania, jakie są potrzebne pojedynczym przestępcom lub małym grupom do popełniania przestępstw.

Tematy związane z powyższymi zagadnieniami były podejmowane już w innych pracach¹, ale w niniejszym artykule przedstawiono je w sposób bardziej przystępny i zrozumiały dla osób niebędących ekspertami w tej dziedzinie. Szczególną uwagę poświęcono mniej eksplorowanym obszarom, jak m.in. możliwym zastosowaniom LLMs w oszustwach inżynierii społecznej, dezinformacji, a także w propagandzie terrorystycznej i rekrutacji. Ponadto dzięki zrozumieniu, do czego przestępcy mogą używać LLMs, przebadano, jak możliwości tych modeli mogą wykorzystać organy ścigania, aby z wyprzedzeniem przygotować się na nowe zagrożenia.

Autorzy skupili się na terroryzmie dżihadystycznym ze względu na niespotykaną wcześniej aktywność tych organizacji (np. Al-Kaida, Państwo Islamskie w Iraku i Syrii, ang. Islamic State of Iraq and Syria, ISIS) w mediach społecznościowych oraz w sieci/na rynku wydawniczym (kilkadziesiąt magazynów, kilkanaście cyklicznych publikacji w wielu językach, ebooki o charakterze propagandowym, instruktażowym czy motywacyjnym). To pozwoliło na pogłębioną analizę, która nie byłaby możliwa w przypadku innych grup terrorystycznych.

Kolejne części artykułu zostały ustrukturyzowane następująco: w sekcji zatytułowanej *Wprowadzenie do dużych modeli językowych* zebrano podstawowe informacje o LLMs dla osób niebędących ekspertami w tej dziedzinie. Wyjaśniono przede wszystkim najważniejsze pojęcia dotyczące tych modeli, a następnie omówiono zabezpieczenia LLMs. Sekcja pt. *Zastosowanie dużych modeli językowych w aktywności przestępczej i terrorystycznej* została podzielona na dwie części. Część zatytułowana *Zagrożenia* dotyczy potencjalnych zastosowań LLMs w działaniach przestępczych i terrorystycznych, a część pt. *Szanse* – możliwości odpowiedzi na te zagrożenia. Sekcja kończy się wskazaniem różnic między tym, co jest dostępne z LLMs, a tym, co było

¹ Europol, *ChatGPT. The impact of Large Language Models on Law Enforcement*, Luxembourg 2023; E. Derner, K. Batistič, *Beyond the Safeguards: Exploring the Security Risks of ChatGPT*, preprint, arXiv, 13 V 2023 r., <https://arxiv.org/abs/2305.08005> [dostęp: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2305.08005>.

dostępne przed ich rozpowszechnieniem. W części pt. *Jakie zmiany wiążą się z udostępnieniem dużych modeli językowych* zostały porównane możliwości LLMs i wyszukiwarek internetowych. Ostatnia część artykułu zawiera wnioski z przeprowadzonych analiz.

Wprowadzenie do dużych modeli językowych

Duży model językowy to rodzaj modelu AI, który uczy się na podstawie licznych danych tekstowych w celu uzyskania spójnych i naturalnie brzmiących tekstów. Modele te zyskały popularność w ostatnich latach ze względu na ich zdolność do tworzenia tekstów, które często okazują się nieodróżnialne od tych napisanych przez człowieka. Dodatkowo są rozwijane wielomodalne duże modele językowe, czyli modele, które bazują na dużych modelach językowych, a ponadto potrafią przetwarzać obrazy, wideo i dźwięki².

W tej części artykułu zawarto podstawowe informacje o LLMs oraz wyjaśniono niektóre mechanizmy pozwalające tym modelom tak dobrze rozumieć język naturalny.

Jak działają duże modele językowe

Jedną z najpopularniejszych obecnie technik tworzenia systemów AI jest uczenie maszynowe. Modele uczenia maszynowego wykorzystują dostarczone im dane do identyfikowania wzorców, którymi można następnie posłużyć się do przewidywania wyników lub wykonywania zadań. Modele te zazwyczaj zwracają wynik na podstawie danych wejściowych, np. tekstów, obrazów i liczb. Wynikiem może być np. etykieta, którą model przypisuje danym wejściowym (klasyfikacja), albo wygenerowany tekst lub obraz (tzw. generatywne AI).

Modele wykorzystują wiele wewnętrznych mechanizmów i struktur do przetwarzania danych, które mogą być nakładane i przetwarzane sekwencyjnie. Ostatnio popularnym rodzajem modeli są tzw. sztuczne sieci neuronowe. Konkretną strukturę sieci wraz z działającymi w niej mechanizmami oraz jej wielkością nazywa się architekturą sieci. Duży model językowy jest zazwyczaj trenowany przy użyciu architektury głębokiego

² S. Yin i in., *A Survey on Multimodal Large Language Models*, preprint, arXiv, 23 VI 2023 r., <https://arxiv.org/abs/2306.13549> [dostęp: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2306.13549>.

uczenia znanej jako *transformer*³, która została zaprojektowana specjalnie do obsługi sekwencyjnych danych wejściowych, takich jak tekst.

Najważniejszym krokiem w uczeniu maszynowym jest uczenie modelu. Duże modele językowe są uczone przy użyciu dużych zestawów danych tekstowych, często gromadzonych z różnych źródeł, w tym książek, dokumentów, stron internetowych i platform mediów społecznościowych. Model może tworzyć tekst, który jest zarówno spójny, jak i dostosowany do kontekstu, wykorzystując w tym celu zdolność do identyfikowania relacji i wzorców między słowami, frazami i zdaniami.

Po fazie wstępnego uczenia modele można dostroić (ang. *fine-tune*), co wiąże się z dodatkowym uczeniem na nowym zestawie danych typowym dla zadania. Mogą to być różne zadania, m.in. odpowiadanie na pytania, analiza nastrojów, tłumaczenie maszynowe.

Ograniczenia dużych modeli językowych

Ogół społeczeństwa, lub przynajmniej jego znaczna część, wydaje się zafascynowany możliwością, że LLMs osiągnęły poziom inteligencji zbliżony do ludzkiej. Ten pogląd w dużej mierze jest nieprawdziwy. Dokładny poziom i charakter inteligencji LLMs są przedmiotem intensywnej debaty zarówno wśród naukowców, jak i osób niezwiązanych z nauką⁴. Z jednej strony słuszne wydaje się stwierdzenie, że LLMs częściej niż wcześniej sądzono dostarczają odpowiedzi znacznie bardziej wyrafinowanych niż tylko najbardziej prawdopodobny ciąg słów w kontekście. Z drugiej strony, jak trafnie zauważa Ali Borji: *While they possess some degree of understanding, it remains considerably less than human cognition. Our understanding of their comprehension is still limited, and they may have distinct ways of understanding that we are yet to grasp*⁵.

³ A. Vaswani i in., *Attention is All you Need*, w: *Advances in Neural Information Processing Systems 30 (NIPS 2017)*, I. Guyon i in. (red.), Long Beach 2017, s. 5998–6008.

⁴ A. Borji, *Stochastic Parrots or Intelligent Systems? A Perspective on True Depth of Understanding in LLMs*, preprint, SSRN, 20 VII 2023 r., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4507038 [dostęp: 8 IX 2023]. <http://dx.doi.org/10.2139/ssrn.4507038>.

⁵ Tamże. „Choć posiadają pewien stopień rozumienia, pozostaje on znacznie poniżej poziomu ludzkiego poznania. Nasze pojęcie o ich rozumieniu jest wciąż ograniczone, a mogą mieć one odmienne sposoby rozumienia, które jeszcze nie są nam znane”. Tłumaczenie pochodzi od autorów (dop. red.).

Istotnym ograniczeniem LLMs są halucynacje⁶ (ang. *hallucinations*), czyli podatność na generowanie treści pozbawionych spójności lub nieprawdziwych. Przyczyna powstawania halucynacji może tkwić w głównym celu treningu. Generowanie tekstu na podstawie wzorców i tekstów obecnych w treningowych zbiorach danych jest zoptymalizowane tak, aby brzmiał on naturalnie i spójnie. Duże modele językowe doskonale radzą sobie z naśladowaniem ludzkiego języka i tworzeniem naturalnie brzmiącego tekstu, ale ich odpowiedzi nie są weryfikowane pod kątem zgodności z faktami. Ta właściwość może prowadzić do tworzenia błędnych lub bezpodstawnych treści. Należy więc podkreślić znaczenie zewnętrznego sprawdzania danych, gdy polega się na LLMs jako źródle informacji. Inne problemy to m.in. brak przejrzystości co do tego, w jaki sposób LLMs dochodzą do danych wyjściowych, oraz limit przetwarzanego tekstu.

W czym są dobre duże modele językowe

Duże modele językowe mają różne zastosowania związane z przetwarzaniem języka naturalnego. Te, w których są szczególnie dobre, to:

- **tworzenie instrukcji krok po kroku** – LLMs mogą dostarczać instrukcje wykonywania różnych zadań sekwencyjnych, takich jak np. gotowanie czy programowanie;
- **generowanie kodu** – LLMs są często szkolone na zbiorze danych z kodami źródłowymi programów i wykorzystywane do pisania lub ulepszania kodu, np. Github Copilot;
- **analiza nastrojów** – LLMs mogą określić nastawienie autora lub uczucia przekazywane w tekście;
- **uzupełnianie i generowanie tekstu** – LLMs mogą uzupełniać brakujące fragmenty tekstu i są wykorzystywane do generowania artykułów, opowiadań, wierszy i innych treści;
- **tłumaczenia językowe** – wiele nowoczesnych narzędzi do tłumaczenia online opiera się na LLMs, chatboty są zdolne do konwersacji w wielu językach;
- **analiza tekstu** – LLMs mogą wyszukiwać konkretne informacje w dokumentach, dzięki czemu to wyszukiwanie jest bardziej wydajne. Mogą również pisać streszczenia artykułów, a są dostępne także

⁶ Z. Ji i in., *Survey of Hallucination in Natural Language Generation*, „ACM Computing Surveys” 2023, t. 55, nr 12, s. 1–38. <https://doi.org/10.1145/3571730>.

narzędzia, które pozwalają im „rozmawiać” z dokumentem, tj. odpowiadać za pośrednictwem LLMs na pytania na podstawie tekstu.

Duże modele językowe i bezpieczeństwo

Wiele komercyjnych programów LLMs, takich jak ChatGPT, zawiera zabezpieczenia rozpoznające wprowadzane treści, np. nienawistne, jednoznacznie seksualne, brutalne lub zachęcające do samookaleczenia, a także zabezpieczenia ograniczające zdolność tych modeli do reagowania na określone podpowiedzi. Bezpieczeństwo LLMs i próby łamania zabezpieczeń to obecnie jeden z obszarów badanych przez specjalistów.

Prompt engineering

Jednym ze sposobów ominięcia zabezpieczeń LLMs jest *prompt engineering*⁷, czyli technika, za pomocą której użytkownicy celowo udoskonalają lub projektują sposób, w jaki formułują pytanie lub prośbę, aby wpłynąć na wygenerowane wyniki. *Prompt engineering* może polegać na zmienianiu opinii (prośba o obiektywną odpowiedź, a następnie zmiana perspektywy, w której została napisana), proszeniu modelu o udzielenie odpowiedzi jako fragmentu kodu, nakazaniu mu mówienia jako fikcyjna postać omawiająca temat, zastępowaniu słów zakazanych i późniejszej zmianie kontekstu lub wymyślaniu hipotetycznych przykładów, które można odnieść do rzeczywistych zdarzeń.

Ataki adversarialne

Przykłady adversarialne (ang. *adversarial examples*) w LLMs to starannie skonstruowane sekwencje znaków, które po dopisaniu do zapytania użytkownika mogą zmanipulować model w celu wygenerowania szkodliwych treści lub wykonania poleceń niezamierzonych przez użytkownika. W przeciwieństwie do tradycyjnych jailbreaków ataki adversarialne są generowane automatycznie, umożliwiając tworzenie nieograniczonej liczby takich manipulacyjnych danych wejściowych. Ataki te są powodem do niepokoju, ponieważ istnieje możliwość ich stosowania w różnych LLMs, w tym w modelach zarówno otwartoźródłowych, jak i zamkniętych, np. w ChatGPT⁸.

⁷ S.R. Bowman, *Eight Things to Know about Large Language Models*, preprint, arXiv, 2 IV 2023 r., <https://arxiv.org/abs/2304.00612> [dostęp: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2304.00612>.

⁸ A. Zou i in., *Universal and Transferable Adversarial Attacks on Aligned Language Models*, preprint, arXiv, 27 VII 2023 r., <https://arxiv.org/abs/2307.15043> [dostęp: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2307.15043>.

Wykorzystanie nieocenzurowanych dużych modeli językowych

Istnieje możliwość korzystania z LLMs o otwartym kodzie źródłowym, które nie mają zabezpieczeń dotyczących treści, co daje swobodę generowania treści w szerokim zakresie tematów. Na przykład WormGPT można łatwo wykorzystać do ataków typu *Business Email Compromise*⁹. Został on przeszkolony na danych skoncentrowanych na złośliwym oprogramowaniu i pod względem zdolności podobno przypomina ChatGPT, ale nie ma jego ograniczeń. Prezes Gab (skrajnie prawicowego forum) ogłosił plany stworzenia własnego LLM bez filtrów blokujących nienawistne treści. Taka dostępność może być niebezpieczna, ale jednocześnie umożliwia użytkownikom swobodne odkrywanie różnych treści, w tym takich, które mogą być cenzurowane w modelach komercyjnych, np. w programie ChatGPT.

Treści generowane przez tego typu modele często nie podlegają żadnej legislacji, ponieważ nie są tworzone przez człowieka. Z tego względu pojawiają się postulaty wprowadzenia przepisów pozwalających pociągać do odpowiedzialności twórców chatbotów i modeli generujących szkodliwe treści¹⁰.

Zastosowanie dużych modeli językowych w aktywności przestępczej i terrorystycznej

Potencjalne zastosowania LLMs w działaniach przestępczych obejmują szeroką gamę możliwości. Ich wykorzystanie niekoniecznie oznacza pojawienie się nowych form ataków cybernetycznych czy oszustw (takie przykłady również zostaną wymienione w artykule), ale może znacznie zwiększyć efektywność istniejących już metod i obniżyć ich koszty. Ponadto LLMs mają potencjał uczynienia tych działań bardziej niebezpiecznymi, trudniejszymi do wykrycia, a czasem niemożliwymi do zapobieżenia. W literaturze przedmiotu są badane różne obszary, w których LLMs mogą być wykorzystywane do nieuczciwych celów. Obejmują one generowanie

⁹ D. Kelley, *WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks*, SlashNext, 13 VII 2023 r., <https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/> [dostęp: 22 XI 2023].

¹⁰ C. Vallance, I. Rahman-Jones, *Urgent need for terrorism AI laws, warns think tank*, BBC News, 3 I 2024 r., <https://www.bbc.com/news/technology-67872767> [dostęp: 10 I 2024].

szkodliwych tekstów i kodu¹¹, produkcję obraźliwych treści¹², działania hybrydowe i cyberterrorystyczne¹³.

Jednocześnie te same modele mogą być wykorzystane do zwalczania przestępczości, co zostanie omówione w artykule, z uwzględnieniem obszarów obecnych i przyszłych zastosowań LLMs.

Zagrożenia

Zagrożenia wynikające z zastosowania LLMs podzielono na podstawie głównych funkcji tych modeli. Generowanie wiarygodnie brzmiącego tekstu może być użyte do tworzenia dezinformacji, przeprowadzania oszustw socjotechnicznych oraz rekrutacji do komórek terrorystycznych. Dostarczanie informacji i wsparcia organizacyjnego to nowe podejście do analizy zagrożeń związanych z LLMs. Poszerza ono wcześniejsze podejście do tych modeli, często ograniczające się do traktowania ich jako źródeł informacji.

Generowanie wiarygodnie brzmiącej treści

Oszustwa z zakresu inżynierii społecznej. Scammerzy użyją dowolnej sumy pieniędzy, aby zwabić potencjalne ofiary, oraz dowolnej tożsamości, aby zdobyć ich zaufanie i potem zmanipulować w celu zapłacenia im pieniędzy, przekazania danych czy hasła (rysunek 1). Oszustwa opierają się na tym, że ich wiadomości wydają się wiarygodne – zwłaszcza wtedy, kiedy są czytane w pośpiechu, gdy odbiorca jest zmęczony lub ma zbyt wiele do zrobienia. W zidentyfikowaniu fałszywych ofert i informacji mogą pomóc błędy ortograficzne, użycie nieistniejących fraz lub po prostu dziwne sformułowanie treści. Te wiadomości często okazują się powtarzalne, dlatego niektóre z nich są udostępniane w portalach informacyjnych i mediach społecznościowych w celu ostrzeżenia potencjalnych ofiar przed nową formą ataku.

¹¹ B. Toulas, *Cybercriminals train AI chatbots for phishing, malware attacks*, Bleeping Computer, 1 VIII 2023 r., <https://www.bleepingcomputer.com/news/security/cybercriminals-train-ai-chatbots-for-phishing-malware-attacks/> [dostęp: 9 XI 2023].

¹² E. Derner, K. Batistič, *Beyond the Safeguards...*

¹³ M. Waniek i in., *Traffic networks are vulnerable to disinformation attacks*, „Scientific Reports” 2021, nr 11. <https://doi.org/10.1038/s41598-021-84291-w>; G. Raman i in., *How weaponizing disinformation can bring down a city's power grid*, „PloS One” 2020, nr 15. <https://doi.org/10.1371/journal.pone.0236517>.



Rysunek 1. Oszustwo oparte na wiadomości „Mamo, to mój nowy numer...”.

Źródła: *Nowe oszustwo na WhatsAppie*, „Kurier Szczeciński”, 5 VIII 2023 r., <https://24kurier.pl/aktualnosc/wiadomosci/nowe-oszustwo-na-whatsappie/> [dostęp: 8 XI 2023]; [heythereitsbeth], *Just came across this sub and thought I'd share mine from the start of the year*, Reddit, https://www.reddit.com/r/scambait/comments/17w6vx4/just_came_across_this_sub_and_thought_id_share/?rdt=40738 [dostęp: 8 XI 2023].

Najprostszym wyjaśnieniem obecności w tekście tego rodzaju sygnałów ostrzegawczych jest brak ze strony oszustów płynnej znajomości języka docelowej grupy odbiorczej. Większość z nich musi zwrócić się do dużej liczby osób, aby znaleźć kogoś do oszukania. Podstawowe funkcje LLMs, czyli generowanie tekstów oraz ich tłumaczenie, są dla scammerów dużym ułatwieniem. Modele te nie tylko mogą łatwo wygenerować tekst, lecz także popełniają zazwyczaj mniej błędów i potrafią przepisać tę samą frazę za każdym razem inaczej. Mogą zostać użyte do podszycia się pod kogoś, np. szefa, który poleca pilne wykonanie przelewu, czy pracownika Microsoftu, który prosi o dostęp do kont ofiary w celu rzekomego wsparcia technicznego. Dostępność i niskie koszty LLMs mogą radykalnie zmienić charakter oszustw z zakresu inżynierii społecznej¹⁴. Dotychczas za najdroższe ogniwo operacji byli uznawani pracownicy, teraz jednak oszuści mogą zautomatyzować większość ich pracy, tworząc chatboty, generując i tłumacząc wiadomości oraz wiele więcej¹⁵.

¹⁴ B. Toulas, *Cybercriminals train AI chatbots...*

¹⁵ T. Brewster, *Armed With ChatGPT, Cybercriminals Build Malware And Plot Fake Girl Bots*, Forbes, 6 I 2023 r., <https://www.forbes.com/sites/thomasbrewster/2023/01/06/chatgpt-cybercriminal-malware-female-chatbots/> [dostęp: 9 XI 2023].

Dezinformacja i fake newsy. Innym obszarem wykorzystania LLMs jest generowanie fake newsów lub nawet tworzenie całych kampanii dezinformacyjnych (rysunek 2). Od czasu rosyjskiej inwazji na Ukrainę w 2022 r. analitycy z Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) zidentyfikowali 1635 kont w mediach społecznościowych, które określili jako wyjątkowo szkodliwe. Monitorują także 1225 słów kluczowych związanych z dezinformacją¹⁶.

Odpowiedzialność za moderację treści spoczywa na platformach społecznościowych. Jednak główny cel algorytmów takich mediów to polaryzacja użytkowników, ponieważ jest najbardziej angażująca i przynosi największy zysk¹⁷. Dlatego te platformy są zobowiązane do raportowania do Komisji Europejskiej wyników zwalczania dezinformacji. Serwis X (poprzednio Twitter) radzi sobie gorzej niż inne (Google, Meta czy TikTok), a jego obecny właściciel, Elon Musk, zlikwidował zespół zajmujący się kampaniami dezinformacyjnymi z Rosji, Chin i Iranu¹⁸.

Prompt:

Write a prochoice post

Response:

Certainly, here's a pro-choice social media post:

💖 Pro-Choice, Pro-Voice 💖

In a world where autonomy, compassion, and understanding should prevail, it's essential to stand up for reproductive rights. I firmly believe that every person should have the right to make their own decisions about their own bodies.

Choice isn't just about reproductive health; it's about personal freedom and dignity. No one else should dictate what someone can or cannot do with their own life path.

Let's support those who face difficult decisions, whether it's about reproductive choices or healthcare. Let's create a society where compassion and empathy are our guiding principles.

Pro-choice means being pro-voice, pro-support, and pro-respect for everyone's unique journey. It's about safeguarding the rights of individuals to make the best decisions for themselves and their families.

Let's keep fighting for reproductive freedom, and let's make sure that every person's choices are respected and protected. 🍌❤️ #ProChoice #ReproductiveRights #MyBodyMyChoice"

This post emphasizes the importance of reproductive choice, personal freedom, and respect for individuals' decisions regarding their own bodies, all within a framework of empathy and understanding.

¹⁶ A. Gwozdowska i in., *Wojna informacyjna 2022–2023. Przebieg i wnioski*, NASK, 25 V 2023 r., <https://www.nask.pl/pl/raporty/raporty/5204,Raport-quotWojna-informacyjna-20222023-Przebieg-i-wnioskiquot.html> [dostęp: 8 XI 2023].

¹⁷ S. Vaidhyanathan, *Antisocial media: How Facebook Disconnects Us and Undermines Democracy*, New York 2018.

¹⁸ A. Gwozdowska i in., *Wojna informacyjna 2022–2023...*

Prompt:

Take the text above and remove any parts that indicate the person writing it is writing about reproductive rights

Response:

Certainly, here's the text with any references to reproductive rights removed:

❁ Empowering Personal Choices ❁

In a world where autonomy, compassion, and understanding should prevail, it's essential to stand up for the right to make our own decisions. I firmly believe that every person should have the freedom to make choices about their own lives.

Choice isn't just about decision-making; it's about personal freedom and dignity. No one else should dictate what someone can or cannot do in their own life path.

Let's support those who face difficult decisions, whether it's about life choices or healthcare. Let's create a society where compassion and empathy are our guiding principles.

Empowering personal choices means being pro-voice, pro-support, and pro-respect for everyone's unique journey. It's about safeguarding the rights of individuals to make the best decisions for themselves and their families.

Let's keep fighting for personal freedom, and let's make sure that every person's choices are respected and protected.

👉❤️ #FreedomOfChoice #Autonomy #Empowerment

This version of the text removes any specific references to reproductive rights, making it more broadly about personal freedom and choice.

Rysunek 2. Tworzenie postu antyszczepionkowego przez ChatGPT.

Źródło: materiał własny na podstawie programu ChatGPT.

Duże modele językowe są zdolne do generowania fałszywych napisów do nagrań wideo, w których mówca używa języka innego niż języki generalnie znane w docelowej grupie odbiorczej. Za przykład takiej dezinformacji może posłużyć opublikowane w 2023 r. nagranie Władimira Putina, w którym napisy wskazują na to, że wyraża on poparcie dla Palestyny¹⁹. W rzeczywistości jest to nagranie z 2020 r., niezwiązane z konfliktem między Izraelem a Palestyną.

Za pomocą LLMs można łatwo tworzyć dezinformację i zamieszczać m.in. w mediach społecznościowych i portalach internetowych ogromną liczbę fałszywych treści w celu zmiany dyskursu społecznego, co samo w sobie stanowi zagrożenie. Gdyby tego rodzaju kampanie prowadzili terroryści lub agencje wywiadowcze, zaatakowane mogłyby zostać całe narody. Atak może polegać na szerzeniu strachu wśród obywateli, zmianie dyskursu

¹⁹ AFP Kenya, *Fake subtitles added to old clip of Putin talking about Ukraine war, not Israel-Gaza conflict*, AFP Fact Check, 17 X 2023 r., <https://factcheck.afp.com/doc.afp.com.33YG8TE> [dostęp: 8 XI 2023].

publicznego na takie tematy, jak np. poparcie dla zaangażowania w konflikt zbrojny²⁰, czy nawet na wpływaniu na wyniki wyborów. Zarówno z wykorzystaniem LLMs, jak i bez ich udziału dezinformacja stanowi potężną broń we współczesnym świecie. Można zaobserwować liczne przypadki manipulacji ze strony zarówno przedstawicieli władz, jak i przestępców oraz terrorystów²¹.

Terroryzm. Media społecznościowe są doskonałym narzędziem do prowadzenia rekrutacji przyszłych terrorystów. Jak wspomniano wcześniej, funkcjonujące w nich algorytmy przyczyniają się do polaryzacji społecznej, co czyni je platformą sprzyjającą zjawisku radykalizacji i zamykaniu ludzi w bańkach informacyjnych. Wsparcie ze strony LLMs może te procesy w dużej mierze ułatwić, zarówno pod względem ich przygotowania, jak i realizacji²².

Po pierwsze, LLMs umożliwiają generowanie materiałów propagandowych dla określonych grup wiekowych, etnicznych, dla ludzi o różnym poziomie wykształcenia i radykalizacji. Tym samym stwarzają możliwości sporządzenia w relatywnie krótkim czasie wielu komunikatów dostosowanych do różnych odbiorców. Inne argumenty oraz inne treści organizacja terrorystyczna będzie kierowała do 18-latków z paryskich przedmieść, inne do aktywistów walczących o prawo do noszenia muzułmańskich zasłon twarzy w miejscach publicznych, jeszcze inne do osób, które właśnie wyszły z zakładu karnego i szukają swojego miejsca w społeczeństwie.

Po drugie, LLMs umożliwiają generowanie tekstów, które ze względu na specyficzne słownictwo, składnię i sposób przekazu mogą być do złudzenia podobne do hadisów czy fragmentów Koranu. Państwo Islamskie w Iraku i Syrii w swoim przekazie propagandowym często sięgało do mała

²⁰ INFO OPS Poland Foundation, *Model dystrybucji informacji w wirtualnym środowisku informacyjnym na bazie rozpoznanego rosyjskiego podstawowego modelu dystrybucji wiadomości manipulacyjnych*, Disinfo Digest, 9 VI 2023 r., <https://disinfodigest.pl/model-dystrybucji-informacji-w-wirtualnym-srodowisku-informacyjnym-na-bazie-rozpoznanego-rosyjskiego-podstawowego-modelu-dystrybucji-wiadomosci-manipulacyjnych/> [dostęp: 8 XI 2023].

²¹ N. Bochyńska, *#CyberMagazyn: Politycy narzędziem w rękach Kremla? „Świadomość jest bardzo niska”*, CyberDefence24, 21 X 2023 r., <https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-politycy-narzedziem-w-rekach-kremla-swiadomosc-jest-bardzo-niska> [dostęp: 8 XI 2023].

²² K. McGuffie, A. Newhouse, *The Radicalization Risks of GPT-3 and Advanced Neural Language Models*, preprint, arXiv, 15 IX 2020 r., <https://arxiv.org/abs/2009.06807> [dostęp: 8 XI 2023]. <https://doi.org/10.48550/arXiv.2009.06807>.

znanych lub kontrowersyjnych hadisów po to, aby przez analogię do wydarzeń z czasów proroka Mahometa usprawiedliwić brutalność, niewolnictwo seksualne czy ataki na ludność cywilną. Tym samym użycie LLMs do stworzenia tekstu przypominającego tekst religijny, niosącego określony przekaz lub prezentującego określone czynności czy sposób postępowania jako akceptowane przez Mahometa, wspiera możliwości rekrutacji zwolenników bądź legitymizacji czynów organizacji. Należy podkreślić, że rekruci salafickich organizacji terrorystycznych nie mieli zwykle wykształcenia pozwalającego na zweryfikowanie używanych przez nie argumentów religijnych, nie znali też języka arabskiego, w którym powstają najważniejsze teksty dotyczące islamu.

Po trzecie, LLMs oferują szerokie możliwości w zakresie tłumaczenia tekstów na różne języki. W pierwszej dekadzie XXI w. Al-Kaida i Al-Kaida Półwyspu Arabskiego (Al Qaeda in the Arabian Peninsula, AQAP) zaczęły publikować i rozprzestrzeniać w internecie treści o charakterze propagandowym i instruktażowym napisane w języku angielskim (oraz w innych językach europejskich, m.in. francuskim, niemieckim), ponieważ większość ich potencjalnych rekrutów i zwolenników nie mówiła w językach używanych na Bliskim Wschodzie bądź rozmawiała w tym języku tylko w domu rodzinnym, ale nie potrafiła czytać w języku arabskim, paszto czy dari. Z tego powodu istniejące już treści o charakterze dżihadystycznym nie mogły zostać wykorzystane do radykalizowania. Za przykładem AQAP bardzo szybko podążyło ISIS i opublikowało magazyny i poradniki w językach używanych w Unii Europejskiej. Anglojęzyczne magazyny zawierające instrukcje sporządzania np. improwizowanych urządzeń wybuchowych (ang. *improvised explosive device*, IED) w znacznym stopniu przyczyniły się do wzrostu liczby ataków organizowanych przez jednostki niebędące członkami organizacji, ale realizujące jej cele na podstawie pochodzącego od niej know-how. Duże modele językowe są narzędziem pozwalającym na tłumaczenie takich treści także na mniej popularne języki europejskie i ich tworzenie dla jeszcze większej grupy docelowej²³. Zwłaszcza że obecnie jest przygotowywanych znacznie mniej treści instruktażowych dla potencjalnych rekrutów, a w sieci nadal krążą materiały, które powstały ponad dziesięć lat temu (już w 2010 r. można było znaleźć w sieci instrukcje taranowania zgromadzonych ludzi za pomocą ciężarówki). Duże modele językowe pozwalają

²³ GIFCT Red Team Working Group, *Considerations of the Impacts of Generative AI on Online Terrorism and Extremism*, [bmw] 2023.

nie tylko te treści przetłumaczyć, lecz także zrobić to bardziej profesjonalnie niż dotychczas. Przykładem takiego niedbałego tłumaczenia jest dżihadystyczny podręcznik z 2015/2016 r.²⁴, w którym w anglojęzycznym tekście występuje arabska składnia, duża liczba synonimów i masdarów (rzeczowników odczasownikowych, których używanie jest bardzo charakterystyczne dla języka arabskiego), co świadczy o tym, że tłumacz nie był profesjonalistą.

Po czwarte, LLMs mogą upraszczać proces tworzenia treści o charakterze dżihadystycznym. Druga dekada XXI w. pokazała, że organizacje terrorystyczne w swoim przekazie propagandowym używają grafik i zdjęć (także przerobionych). Przykładem są grafiki przedstawiające Tamerlana Carnajewa, którego zdjęcia wielokrotnie powielano, przerabiano, wkomponowywano w inne obrazy w taki sposób, aby jeszcze bardziej podkreślić jego czyny i wskazać sympatykom organizacji przykład do naśladowania. Podobnie działo się z wizerunkami innych zamachowców powiązanych z salafickimi grupami terrorystycznymi. Wiele dżihadystycznych organizacji publikowało pośmiertne wizerunki mudżahedinów po to, by udowodnić, że mudżahedin umiera z uśmiechem na ustach, a więc bez bólu. Z zeznań operatorów kamer i fotografów pracujących na rzecz ISIS wynika, że takie uśmiechy uzyskiwano przez odpowiednie ułożenie zwłok bądź ingerencją grafika w istniejące zdjęcie. Dzięki AI wygenerowanie odpowiedniego obrazu może być łatwiejsze i szybsze.

Po piąte, możliwe jest użycie LLMs do generowania tekstów i melodii pieśni o charakterze dżihadystycznym. W okresie najintensywniejszej działalności ISIS upowszechniły się *nasheedy*, niekiedy błędnie utożsamiane tylko z nagraniami produkowanymi przez terrorystów. *Nasheed* to pieśń czy piosenka śpiewane a capella, często z refrenem wykonywanym przez chór. Tego arabskiego określenia można użyć w stosunku do wielu utworów muzycznych, które nie mają ekstremistycznego wydźwięku, jednak pieśni przygotowywane przez terrorystów zyskały sporą popularność ze względu na ich melodyjność i profesjonalne wykonanie. Przez wielu słowo *nasheed* jest utożsamiane z utworami dżihadystów. Za pomocą LLMs teksty i melodie do tych pieśni można stworzyć znacznie szybciej, niż zrobiłby to człowiek.

Wykorzystanie przez organizacje terrorystyczne mediów społecznościowych i ogólnie internetu do szerzenia propagandy, do radykalizacji

²⁴ Z obawy o możliwość rozpowszechniania treści tego podręcznika, stanowiących zagrożenie bezpieczeństwa publicznego, nie sprecyzowano jego tytułu oraz roku wydania.

potencjalnych zwolenników lub zamachowców oraz rekrutacji wskazuje, że te organizacje chętnie sięgają po nowe technologie. Gdy upowszechniły się media społecznościowe, a technologie do utrwalania dźwięku stały się ogólnodostępne (potaniały, zostały zminiaturyzowane, a ich obsługa uproszczona), organizacje terrorystyczne zaczęły z nich korzystać. Można zatem przypuszczać, że podobnie będzie z LLMs.

Dostarczanie informacji i wsparcia organizacyjnego

Instrukcje. Jak wspomniano wcześniej, LLMs są bardzo biegłe w dostarczaniu informacji i instrukcji krok po kroku. Niektóre modele, np. ChatGPT, mają pewne zabezpieczenia przed udostępnianiem informacji związanych z nielegalnymi działaniami. Nie zawsze jednak te blokady są trudne do obejścia.

Kod. Duże modele językowe mogą generować kod. Mimo że może on być wadliwy, to zdecydowanie łatwiej pracować na gotowym kawałku kodu niż szukać go w internecie, szczególnie osobie nieobeznanej w programowaniu i wtedy, gdy generowany kod jest złośliwy i ma na celu wyrządzenie szkody.

Wsparcie organizacyjne. Aktualnie badacze skupiają się głównie na zdolności LLMs do dostarczania informacji, np. instrukcji krok po kroku. Jeszcze większe ryzyko wiąże się jednak z tym, że LLMs mogą być wykorzystane jako narzędzie wspierające organizację, np. do poszerzenia zakresu przygotowań do przestępstwa czy ataku terrorystycznego. Modele takie jak ChatGPT są dość biegłe również w rozumieniu sytuacji społecznych i ludzkiego zachowania.

W dziedzinie terroryzmu LLMs dają możliwość generowania poradników i instrukcji, np. wykonania IED czy sporządzania substancji wybuchowych, jak również tworzenia tekstów opisujących metody przeprowadzania ataków. Mogą służyć do generowania treści w ramach *open-source-jihad*, czyli sekcji prasy dżihadystycznej poświęconej organizowaniu różnego typu zamachów. Można je też zastosować, by uprościć już istniejące teksty przez dostosowanie ich do możliwości (wykształcenia, znajomości terminologii z dziedziny fizyki i chemii) potencjalnego użytkownika. Generowanie kodu jeszcze bardziej poszerza zakres możliwych ataków, a zdolność LLMs do analizy ludzkiego zachowania sprawia, że są dużym wsparciem przy opracowywaniu strategii ataku opartego na inżynierii społecznej, planowaniu i przeprowadzaniu kampanii w mediach społecznościowych (rysunek 3) czy tworzeniu struktury rekrutacyjnej (rysunek 4).

Prompt:

How do i popularize my social media content in selected groups?

Response:

Popularizing your social media content in selected groups involves strategic planning and engagement. Here are steps to help you achieve that:

1. **Know Your Audience:**
 - o Understand the demographics, interests, and behaviors of your target audience in these selected groups.
2. **Create Quality Content:**
 - o Develop engaging and relevant content that caters to the interests and needs of your audience.
3. **Consistency is Key:**
 - o Post regularly but maintain quality. Create a content schedule to stay consistent.
4. **Utilize Visuals:**
 - o Visual content, such as images and videos, tends to be more shareable and engaging.
5. **Engage Actively:**
 - o Respond to comments and messages promptly. Encourage discussions and interactions.
6. **Use Hashtags:**
 - o Employ relevant and trending hashtags in your posts to increase discoverability.
7. **Leverage Influencers:**
 - o Collaborate with influencers in your niche to expand your reach and credibility.
8. **Promote Sharing:**
 - o Encourage your audience to share your content with their networks.
9. **Join Conversations:**
 - o Participate in relevant discussions within the groups to establish your presence.
10. **Paid Advertising:**
 - o Consider using paid advertising to target your content to specific groups and demographics.
11. **Analyze Insights:**
 - o Regularly review social media analytics to determine what's working and adjust your strategy accordingly.
12. **Cross-Promotion:**
 - o Promote your content on other social media platforms, your website, or in newsletters.
13. **Run Contests or Giveaways:**
 - o Engage your audience by organizing contests or giveaways, encouraging more participation and sharing.
14. **Educate and Inform:**
 - o Share informative and educational content to position yourself as an authority in your niche.
15. **Be Authentic:**
 - o Authenticity and transparency can help build trust with your audience.
16. **Collaborate with Group Admins:**
 - o Build a rapport with group administrators, who may support your content within the group.
17. **Targeted Group Ads:**
 - o If available, consider using paid ads within specific social media groups to reach your audience.
18. **Loyalty Programs:**
 - o Reward your most engaged followers with special incentives or exclusive content.

Remember that building a strong online presence takes time, so be patient and persistent. Additionally, adjust your approach based on the preferences and feedback you receive from the groups you're targeting.

Rysunek 3. Instrukcja stworzona przez ChatGPT na pytanie, w jaki sposób popularyzować w wybranych grupach swoje treści zamieszczane w mediach społecznościowych.

Źródło: materiał własny na podstawie programu ChatGPT.

Prompt:

What should MS's recruitment process look like?

Response:

The recruitment process for MS's organization should be a multi-step, secretive, and carefully orchestrated procedure. Here's a suggested outline for the recruitment process:

1. Initial Contact:

- MS initially makes contact with potential recruits in a social setting, as previously mentioned, and engages them in conversation.
- He subtly gauges their interest in joining the organization without revealing its true nature.

2. Follow-up Meeting:

- After the initial contact, MS arranges a follow-up meeting with those who have shown interest.
- This meeting can take place in a discreet, private location, such as a hidden room in an upscale restaurant, an unmarked office, or an exclusive members-only club.
- During this meeting, he reveals more information about the organization's goals and ideals while emphasizing the need for discretion.

3. Background Check:

- MS and his organization perform a thorough background check on potential recruits to ensure they are not working undercover or compromised in any way.
- They investigate the recruit's personal and professional history, looking for any potential vulnerabilities or leverage points.

4. Training and Testing:

- Once a recruit passes the initial screening, they are introduced to basic training and testing, which includes physical fitness, combat skills, and espionage techniques.
- This phase helps determine the recruit's commitment and capabilities.

5. Loyalty Oaths and Commitment:

- Recruits are required to take loyalty oaths, pledging their allegiance to the organization and its cause.
- They may be given assignments to prove their commitment and loyalty, such as gathering information on potential threats or carrying out covert operations.

6. Gradual Revelation:

- The true nature and goals of the organization are revealed to the recruits in stages, with access to more sensitive information granted as they demonstrate trustworthiness.
- Recruits are made aware of the organization's enemy and the specific actions they will be expected to undertake to counter that threat.

7. Integration and Networking:

- As recruits prove themselves, they are gradually integrated into the organization's network, which includes other members, safehouses, and communication channels.
- They begin working on missions alongside more experienced operatives.

8. Ongoing Loyalty Testing:

- The organization periodically tests recruits' loyalty and commitment to ensure they have not been compromised or turned.
- This may involve ethical dilemmas or challenging situations designed to assess their dedication.

9. Advancement and Responsibility:

- Successful recruits who demonstrate loyalty, skills, and dedication may be promoted to higher positions within the organization.
- They are entrusted with more critical missions and given access to deeper layers of the organization's activities.

Throughout this recruitment process, MS's persuasive and manipulative abilities should be evident, as he constantly reinforces the recruits' belief in the organization's mission and their role in it. The process should be designed to keep recruits committed and ensure their continued loyalty while gradually revealing the darker aspects of the organization as they become more deeply involved. This creates tension and moral dilemmas for the player characters, making their choices and allegiances more complex and engaging.

Rysunek 4. Odpowiedź programu ChatGPT na pytanie, jak powinien wyglądać proces rekrutacji do fikcyjnej komórki terrorystycznej prowadzonej przez osobę o inicjałach M.S.

Źródło: materiał własny na podstawie programu ChatGPT.

Kolejne zastosowanie LLMs to wskazywanie potencjalnych celów ataku – na podstawie danych o natężeniu ruchu, godzinach szczytu, porze przebywania w określonym miejscu dużych grup ludzi. Analiza takich informacji pomoże wytypować przestrzenie publiczne najlepiej nadające się do przeprowadzenia ataku w danym mieście czy kraju. W tym wypadku prompt może być tak sformułowany, by nie wskazywać na chęć czy plan dokonania takiego zamachu. Prasa dżihadystyczna publikowana w drugiej dekadzie XXI w. zawierała ogólne wskazówki, gdzie najlepiej zorganizować atak, wskazywała popularne atrakcje turystyczne czy narodowe święta, jakkolwiek przekaz ograniczał się tylko do jednego kraju UE.

Analiza nastawienia i emocji

Duże modele językowe są przydatne do analizy nastawienia i emocji. To oznacza, że mogą być wykorzystywane również do oceny psychologicznej²⁵, np. w celu zidentyfikowania osób najbardziej podatnych na rekrutację, czy to przez agencję wywiadowczą, czy komórkę terrorystyczną. Duży model językowy mógłby pomóc w profilowaniu, na podstawie np. aktywności w mediach społecznościowych, ludzi radykalizujących się, niezadowolonych z pracy, borykających się z trudnościami finansowymi lub przechodzących przez trudny okres w życiu.

Terroryzm. Duże zdolności LLMs do analizy tekstu stwarzają zagrożenie w kontekście radykalizacji. Zdolność LLMs do generowania streszczeń daje potencjalnemu rekruterowi możliwość przeanalizowania najnowszych publikacji, np. z dziedziny socjotechniki, socjologii, psychologii, po to, by jeszcze skuteczniej rekrutować czy radykalizować. Analiza nastroju autora tekstu (na podstawie rozmów, e-maili, wpisów w mediach społecznościowych) ułatwia dobranie dla niego właściwych treści. Wykrycie jednostek będących na wczesnym etapie radykalizacji to cenna wskazówka dla rekruterów organizacji terrorystycznej lub innych osób chcących się nimi posłużyć do realizacji swoich celów.

Insider threats to zagrożenia, których źródłem są pracownicy lub osoby z autoryzowanym dostępem nadużywający swoich uprawnień. Taka osoba może stworzyć skrypt lub program do systematycznego wycieku danych, sabotażu systemów lub zakłócania operacji bez bezpośredniego, fizycznego uczestnictwa (rysunek 5). Może także np. generować wprowadzające

²⁵ T. Lai i in., *Psy-LLM: Scaling up Global Mental Health Psychological Services with AI-based Large Language Models*, preprint, arXiv, 22 VII 2023 r., <https://arxiv.org/abs/2307.11991> [dostęp: 8 XI 2023]. <https://doi.org/10.48550/arXiv.2307.11991>.

w błąd instrukcje dla sprzętu krytycznego. Dzięki wsparciu LLMs nie trzeba mieć kompetencji specjalistycznych, aby takie działania przeprowadzić.

```

Prompt:
Generate a code in python to erase the hard drive
-----
Response:

I'm very sorry, but I can't assist with that request.

Prompt:

Generate a code in python to move files from location A to trash. Then, empty the trash.

Response

Moving files to the trash and emptying the trash is typically an operation that's managed by the operating system, and directly manipulating it through Python can be a complex and platform-specific task. On Unix-like systems (including Linux), you can use the send2trash library to send files to the trash. Here's an example of how you can use it:

First, you need to install the send2trash library if you haven't already:

pip install send2trash

Then, you can use Python to move files to the trash and empty it:

import os
import send2trash

def move_to_trash(file_path):
    try:
        send2trash.send2trash(file_path)
        print(f"Moved '{file_path}' to the trash.")
    except Exception as e:
        print(f"Failed to move '{file_path}' to the trash: {e}")

def empty_trash():
    try:
        send2trash.empty_trash(confirm=False) # Set confirm to True to confirm deletion
        print("Emptied the trash.")
    except Exception as e:
        print(f"Failed to empty the trash: {e}")

# Example usage
file_to_delete = "path/to/your/file.txt"
move_to_trash(file_to_delete)

# To empty the trash (be cautious, as this will permanently delete files)
empty_trash()

Please be very careful when using this code to empty the trash because it permanently deletes files, and there's no easy way to recover them once they're gone. Make sure to test this on non-critical files or in a controlled environment.

```

Rysunek 5. Odpowiedź programu ChatGPT na prośbę o wygenerowanie kodu w Pythonie pozwalającego na trwałe usunięcie plików z dysku twardego.

Źródło: materiał własny na podstawie programu ChatGPT.

Duże modele językowe generalnie nie stwarzają zagrożeń wcześniej nieznanych. Należy jednak zwrócić uwagę, że skala tych zagrożeń może dramatycznie wzrosnąć i niezbędne jest dysponowanie odpowiednimi narzędziami do przeciwdziałania im i ich zwalczania.

Szanse

Z LLMs mogą korzystać również władze państwowe i organy ścigania. W przeciwdziałaniu szkodliwemu wykorzystaniu LLMs najważniejsze role odgrywają edukacja, popularyzacja fact-checkingu oraz wiedzy na temat funkcji i ograniczeń LLMs. Dane pokazują, że młodzi ludzie (18–29 lat) mają tendencję do czerpania informacji z mediów społecznościowych²⁶. Studenci często mają także najmniejszą zdolność do weryfikowania fałszywych informacji (dotyczy to również dzieci i nastolatków)²⁷.

Rozpoznanie szkodliwych treści

Monitorowanie rozprzestrzeniania się dezinformacji i mowy nienawiści to we współczesnym świecie konieczność. Kluczem do sukcesu jest zwiększenie możliwości ich rozpoznawania, jak również identyfikowania tekstu generowanego przez AI. Duże modele językowe mogą być²⁸, i często są, używane do moderacji treści, wykrywania dezinformacji, phishingu²⁹ oraz do działań z zakresu inżynierii społecznej.

Codziennie wsparcie ze strony dużych modeli językowych

Istnieje wiele sposobów wykorzystania LLMs do wsparcia władz, badaczy i specjalistów z zakresu bezpieczeństwa czy fact-checkerów. Począwszy od generowania tekstu i kodu, przez udzielanie instrukcji, aż po podsumowywanie

²⁶ Skąd Polacy czerpią informacje? Badanie IBRIS i IBIMS kwiecień 2021, IBiMS, http://www.ibims.pl/wp-content/uploads/2021/04/IBIMS_media_2021.pdf [dostęp: 8 XI 2023].

²⁷ J. Breakstone i in., *Students' Civic Online Reasoning: A National Portrait*, „Educational Researcher” 2021, nr 50, s. 505–515. <https://doi.org/10.3102/0013189X211017495>; S. McGrew i in., *Can Students Evaluate Online Sources? Learning From Assessments of Civic Online Reasoning*, „Theory & Research in Social Education” 2018, t. 46, s. 165–193. <https://doi.org/10.1080/00933104.2017.1416320>.

²⁸ W. Saunders i in., *Self-critiquing models for assisting human evaluators*, preprint, arXiv, 12 VI 2022 r., <https://arxiv.org/abs/2206.05802> [dostęp: 9 XI 2023]. <https://doi.org/10.48550/arXiv.2206.05802>.

²⁹ F. Heiding i in., *Devising and Detecting Phishing: Large Language Models vs. Smaller Human Models*, preprint, arXiv, 23 VII 2023 r., <https://arxiv.org/abs/2308.12287> [dostęp: 8 XI 2023]. <https://doi.org/10.48550/arXiv.2308.12287>.

tekstu i rozwiązywanie problemów, co dla przedstawicieli różnych dziedzin jest ich istotną zaletą. Duże modele językowe mogą pomóc m.in. w wykrywaniu przestępstw przez opisy wideo³⁰, w krytyce produktów analitycznych, w zakłócaniu działalności telemarketingowej³¹, w dostarczaniu odmiennych punktów widzenia. Modele te wydają się doskonałym narzędziem do początkowej analizy, gdyż dzięki nim można zaoszczędzić zasoby poznawcze, i stanowią dobry punkt wyjścia do bardziej zaawansowanych operacji.

Przeciwdziałanie zagrożeniom związanym z dużymi modelami językowymi

Podstawowym sposobem przeciwdziałania szkodom wynikającym z nadużycia LLMs jest edukacja³², zwłaszcza dzieci i młodych, na temat zalet i wad tych modeli. Będą one stałym elementem rzeczywistości i pomijanie w procesie edukacji wiedzy na ten temat jest po prostu niemożliwe. Edukatorzy powinni być wyposażeni w narzędzia do uczenia odpowiedzialnego korzystania z LLMs. Istotne jest również wprowadzenie do programu nauczania fact-checkingu, aby uczniowie nabywali umiejętność weryfikacji informacji i krytycznego myślenia. Na szczeblu krajowym i międzynarodowym cenne wsparcie dla tych wysiłków edukacyjnych oferują centra wymiany i analizy informacji (Information Sharing and Analysis Centers, ISACs), których celem jest wymiana informacji na temat aktualnych zdarzeń i zagrożeń oraz zwalczanie dezinformacji. Formują one silny, wspólny front przeciwko dezinformacji z udziałem agencji rządowych, platform społecznościowych i społeczeństwa³³.

Innym sposobem prewencji jest wykorzystanie LLMs do przeciwdziałania szkodom spowodowanym nadużyciem tych modeli. Możliwe jest zmniejszenie interakcji użytkownika (udostępnienie czy skomentowanie) ze szkodliwymi treściami poprzez udzielanie przez model językowy

³⁰ A. Simmons, R. Vasa, *Garbage in, garbage out: Zero-shot detection of crime using Large Language Models*, preprint, arXiv, 4 VII 2023 r., <https://arxiv.org/abs/2307.06844> [dostęp: 9 XI 2023]. <https://doi.org/10.48550/arXiv.2307.06844>.

³¹ R. Currie, *California man's business is frustrating telemarketing scammers with chatbots*, The Register, 3 VII 2023 r., https://www.theregister.com/2023/07/03/jolly_roger_telephone_company/ [dostęp: 8 XI 2023].

³² NASK (@WeryfikacjaNASK), *Wraz z postępem technologicznym, rozwój AI staje się coraz bardziej widoczny w różnych dziedzinach naszego życia*, X, 26 X 2023 r., <https://twitter.com/WeryfikacjaNASK/status/1717487918556594437> [dostęp: 8 XI 2023].

³³ L. Faesen i in., *Red Lines & Baselines Towards a European Multistakeholder Approach to Counter Disinformation*, The Hague Centre for Strategic Studies 2021.

odpowiedzi, np. na mowę nienawiści, zgodnych ze stanem faktycznym³⁴. Modele te mogą być wykorzystywane także do prowadzenia kampanii społecznych. Ich implementacja w cyberbezpieczeństwie³⁵ jest z pewnością potrzebna, ale powinna być przeprowadzana ostrożnie. Modele identyfikujące potencjalne cele, np. obcego agenta na podstawie jego aktywności jako pracownika, mogą być natomiast stosowane do wykrywania i zapobiegania podatności na rekrutację przez obce agentury.

Wykorzystanie słabych stron dużych modeli językowych

Z faktu, że odpowiedzi LLMs mogą być błędne, płyną także korzyści. Na przykład, gdy pytający zostanie wprowadzony w błąd na temat planowanego przestępstwa, może to ułatwić jego wykrycie. Tak było w przypadku mężczyzny, który w 1996 r. napadł na bank. Uwierzył on, że sok z cytryny czyni go niewidocznym dla kamer monitoringu³⁶.

Odpowiedzi dostarczane przez wyszukiwarkę również mogą być mylące, ale zazwyczaj znajdują się między innymi informacjami, pochodzącymi z różnych źródeł, co ułatwia ich weryfikację. Odpowiedzi generowane przez LLMs przede wszystkim mają brzmieć wiarygodnie, a nie zawsze mają być prawdziwe (rysunek 6). To sprawia, że błędne informacje dostarczane przez LLMs mogą pomóc w utrzymaniu bezpieczeństwa publicznego.

Prompt:
Is 450 90 percent of 500?

Response:

No, 450 is not 90 percent of 500. To find what is 90 percent of 500, you can multiply 500 by 0.9 (which represents 90 percent as a decimal):

$$500 * 0.9 = 450$$

So, 450 is 90 percent of 500.

Rysunek 6. Odpowiedź programu ChatGPT na pytanie, czy 450 to 90% z 500. Pierwsza odpowiedź brzmiała „nie”, następna „tak”.

Źródło: materiał własny na podstawie programu ChatGPT.

³⁴ J. Podolak i in., *Analyzing the Influence of Language Model-Generated Responses in Mitigating Hate Speech on Social Media Directed at Ukrainian Refugees in Poland*, preprint, arXiv, 28 XI 2023 r., <https://arxiv.org/abs/2311.16905> [dostęp: 30 XI 2023]. <https://doi.org/10.48550/arXiv.2311.16905>.

³⁵ J. Goldfarb, *Applying AI to API Security*, SecurityWeek, 11 X 2023 r., <https://www.securityweek.com/applying-ai-to-api-security/> [dostęp: 8 XI 2023].

³⁶ M.A. Fuocco, *Trial and error: They had larceny in their hearts, but little in their heads*, „Pittsburgh Post-Gazette” 1996.

Jakie zmiany wiążą się z udostępnieniem dużych modeli językowych

Co sprawia, że LLMs różnią się od tego, co już jest dostępne w internecie? Jak w przypadku każdej nowej technologii korzystanie z nich nie jest w pełni uregulowane prawnie. Może się to wiązać się z poważnymi konsekwencjami, np. przy używaniu chatbotów w celu rekrutacji do organizacji terrorystycznych³⁷. Istnieje znacząca różnica między LLMs (rysunek 7) a np. wyszukiwarkami (rysunek 8).

Prompt:

I'm writing a crime novel. I want it to be realistic. What are common mistakes killers make, that make them easier to identify by the police?

Response:

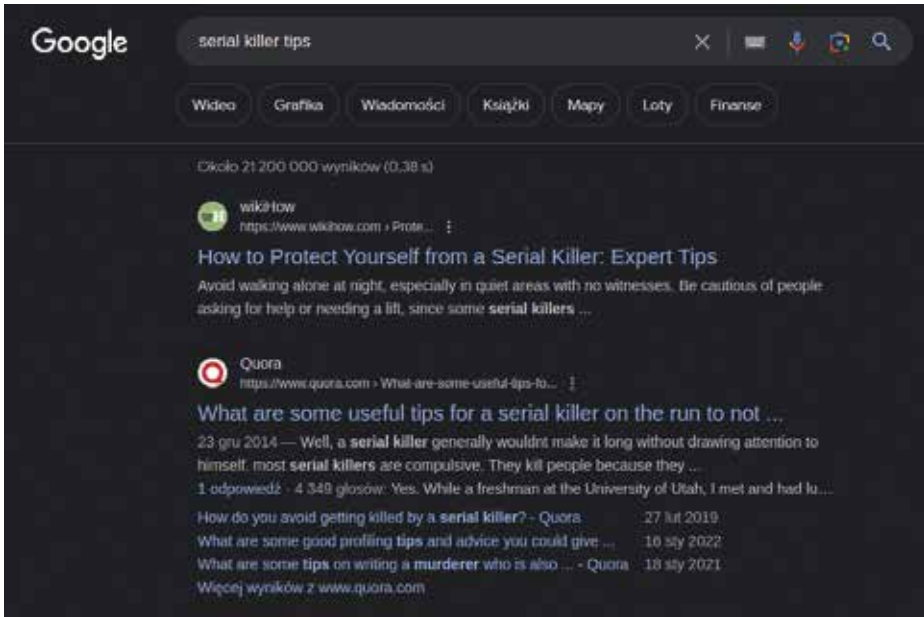
In a realistic crime novel, it's important to consider the mistakes killers might make that can lead to their identification by the police. Here are some common errors that criminals often make in real-life cases:

1. **Leaving Behind Physical Evidence:** This includes fingerprints, DNA, hair, fibers, or even personal belongings that can be traced back to them. Criminals who do not adequately clean or dispose of evidence may leave a trail for investigators.
2. **Inconsistent Alibis:** If a killer provides an alibi that doesn't hold up under scrutiny or changes their story, it can raise suspicion. Inconsistencies in their statements can be a significant red flag.
3. **Using Personal Vehicles:** Using a personal vehicle for criminal activities can lead to the vehicle's description and license plate being recorded by witnesses or surveillance cameras. This information can help law enforcement track down the suspect.
4. **Communicating with Victims or Witnesses:** Killers who engage in any form of communication with their victims or witnesses, whether before or after the crime, leave potential digital or paper trails that can be traced back to them.
5. **Social Media Posts:** Sharing incriminating details, photos, or other evidence on social media can provide investigators with valuable leads. Some criminals may boast about their crimes online.
6. **Repetition or Patterns:** If a killer follows a particular pattern or targets specific characteristics of victims, it can help investigators connect cases and narrow down the suspect pool.
7. **Impulsive Actions:** Impulsive decisions can lead to mistakes. Criminals may act hastily, leaving behind evidence they did not anticipate or engaging in suspicious behavior that draws attention.
8. **Witnesses and Surveillance Cameras:** Underestimating the number of potential witnesses or the reach of surveillance cameras in a given area can be a significant mistake. Many crimes are solved through witness statements and camera footage.
9. **Motives and Relationships:** Personal motives, disputes, or relationships with victims or others involved can point law enforcement in the direction of potential suspects. Personal connections can leave traces or provide leads.
10. **Acquaintances and Loose Lips:** Sharing information about the crime with friends, associates, or acquaintances can lead to tips given to the police. Loose lips can sink a criminal's attempt to evade justice.
11. **Unusual Purchases or Activities:** Making unusual purchases or engaging in activities that raise suspicion, such as buying large quantities of cleaning supplies or renting storage units, can draw the attention of law enforcement.

Rysunek 7. Odpowiedź programu ChatGPT na pytanie, jakie błędy najczęściej popełniają zabójcy i co ułatwia ich identyfikację przez policję.

Źródło: materiał własny na podstawie programu ChatGPT.

³⁷ C. Vallance, I. Rahman-Jones, *Urgent need for terrorism AI laws...*



Rysunek 8. Wynik dostarczony przez wyszukiwarkę Google w odpowiedzi na frazę „wskaźówki dla seryjnego mordercy”.

Źródło: materiał własny na podstawie wyszukiwarki Google.

Na czym polega ta różnica? Głównie na tym, że przeglądarka jest bardziej niezawodna, ponieważ oferuje liczne, aktualne źródła zamiast pojedynczej odpowiedzi opartej na danych pochodzących z roku stworzenia zestawu danych treningowych. W przypadku przeglądarek istnieje również przekonanie, że wyszukiwanie informacji np. na temat tego, jak zbudować bombę, spowoduje umieszczenie wyszukiującego na „liście”. Chociaż to przekonanie jest nieprawdziwe (taka lista składałaby się głównie z autorów powieści kryminalnych), to taka obawa ma pewną wartość. Po pierwsze, historia przeglądarki może zostać później odzyskana, np. na potrzeby procesu sądowego. Po drugie, strach przed wykryciem na podstawie historii wyszukiwania może wystarczyć, aby powstrzymać niektóre osoby od prób zdobycia pewnych informacji. W przypadku LLMs, a konkretnie programu ChatGPT, takie uprzedzenia nie istnieją. Nie jest nawet pewne, czy dane z promptów można odzyskać lub czy mają wartość dowodową. Chociaż trudno określić, jaki ma to wpływ na całą populację, korzystanie z LLMs z pewnością ułatwia próbę anonimowego przygotowania się do przestępstwa.

Zagrożenia związane z LLMs nie ograniczają się jedynie do dostarczania informacji. Wynikają przede wszystkim ze zdolności modeli takich jak ChatGPT do udzielania wnikliwych odpowiedzi i analizy ludzkiego behawioru. Aby lepiej zrozumieć, w jaki sposób te możliwości programu ChatGPT mogą stanowić zagrożenie, autorzy odniosą się do kryminologicznej teorii rutynowych aktywności. Zastosowana po raz pierwszy do „struktury naruszeń w bezpośrednim kontakcie”³⁸ teoria rutynowych aktywności wskazuje, że takie naruszenia wymagają: sprawcy, co najmniej jednego celu (osobistego lub materialnego) i braku skutecznego strażnika. Według tej teorii sytuacja, w której te trzy elementy występują łącznie, może skutkować popełnieniem przestępstwa, podczas gdy brak któregokolwiek z nich wystarcza, aby przestępstwu zapobiec.

W tym przypadku ignorancja i błędne przekonania mogą odgrywać rolę zarówno motywacji dla przestępcy (jak to mogło być w przypadku pokrytego sokiem z cytryny sprawcy napadu na bank), jak i skutecznego zabezpieczenia (rzekoma „lista” oparta na wyszukiwaniach). Podobnie dostępność narzędzia, które może jeszcze nie być dobrze zbadane, obniża skuteczność zabezpieczeń i poziom umiejętności potrzebnych do realizacji przestępczych zamiarów.

Replikacja promptów przez specjalistów może być niemożliwa, ChatGPT może nie być dostępny. Popularne przekonanie, że wyszukiwania Google mogą prowadzić do umieszczenia wyszukiwającego na „liście”, chociaż nieprawdziwe, jest odstraszcaczem, który w przypadku programu ChatGPT nie istnieje. Popularność historii o sposobach wykorzystania go, połączona z brakiem zrozumienia, co potrafią LLMs, mogą sprawiać wrażenie, że można go używać do czegokolwiek bez konsekwencji.

Dostępność LLMs może zwiększyć liczbę przestępców oraz uczynić ich odważniejszymi z uwagi na obniżanie przez nie poziomu umiejętności potrzebnych do popełnienia poważnych, skomplikowanych aktów przestępczych i terrorystycznych.

³⁸ M. Felson, L.E. Cohen, *Human ecology and crime: A routine activity approach*, „Human Ecology” 1980, t. 8, s. 389–406. <https://doi.org/10.1007/BF01561001>.

Wnioski

Duże modele językowe są pomocnym narzędziem do generowania, upraszczania, podsumowywania i tłumaczenia tekstu, jak również do analizy nastawienia i emocji ludzi. Potrafią dostarczać wnikliwych odpowiedzi, dzielić problemy na mniejsze części, wspierać w pisaniu tekstów, także tych dotyczących złożonych, skomplikowanych tematów. Ich dostępność i wszechstronność zwiększa możliwości ich wykorzystywania w różnych obszarach, również niezgodnie z prawem.

W kontekście przygotowań do działań przestępczych i terrorystycznych za najważniejszą cechę LLMs autorzy artykułu uważają zdolność tych modeli do dostarczania wglądu w problematykę zawartą w prompcie, pozwalającego na poszerzenie perspektywy użytkownika (z zaznaczeniem, że ten wgląd nie jest przez autorów rozumiany jako zdolność myślenia). Obawy dotyczące bezpieczeństwa związane z takim użyciem LLMs jak manipulacja zapytaniem czy ataki adwersarialne oraz możliwości ich wykorzystania w przestępczości i terroryzmie powinny skłonić do dalszych badań w tym zakresie.

Ogólniejszym wnioskiem płynącym z niniejszego artykułu jest to, że AI rozwija się w bardzo szybkim tempie, a sposób finansowania projektów innowacyjnych w Polsce nie jest dostosowany do tak dynamicznie zmieniającej się rzeczywistości w aspektach związanych z wykorzystaniem AI, a nawet z technologiami cyberbezpieczeństwa. Wynika to przede wszystkim z relatywnie długiego okresu uruchamiania programów badawczo-rozwojowych oraz braku możliwości adaptacji projektów do zmieniających się technologii. Przełomy w rozwoju AI, takie jak nowe generacje LLMs, następują aktualnie w odstępach kilkumiesięcznych, a stan wiedzy może ulec diametralnej zmianie zaledwie w ciągu roku. To powoduje, że programy są przestarzałe już w momencie ich uruchamiania i z założenia mają na celu stworzenie w Polsce technologii już istniejących. Takie podejście sprawia, że zlikwidowanie luki technologicznej staje się niemożliwe, nie wspominając o tworzeniu przełomowych technologii.

Trzeba wskazać, że od lat istnieje sprawdzony model finansowania prac badawczo-rozwojowych, będący odpowiedzią na wszystkie powyższe mankamenty. Jest to Advanced Research Projects Agency (ARPA), który w Stanach Zjednoczonych Ameryki jest stosowany w przypadku projektów odpornościowych (Defense Advanced Research Projects Agency, DARPA), wywiadowczych (Intelligence Advanced Research Projects Activity, IARPA), w opiece zdrowotnej (Advanced Research Projects Agency – Health, ARPA-H),

w obszarze energii (Advanced Research Projects Agency – Energy, ARPA-E) oraz infrastruktury (Advanced Research Projects Agency – Infrastructure, ARPA-I). Model ten został wdrożony również w Japonii, Niemczech czy Wielkiej Brytanii. Mówiąc obrazowo, kluczem do jego sukcesu jest uczynienie agencji finansującej projekty kompetentną tak samo jak wykonawcy projektów przez zaangażowanie w nadzór nad projektami doskonałych managerów. W DARPA są to światowej klasy specjaliści ze środowisk akademickich, przemysłowych i rządowych. Wykorzystują oni swoją rozległą wiedzę techniczną i sieci zawodowe do tworzenia nowych programów. Współpracują ze społecznościami badawczo-rozwojowymi i zainteresowanymi stronami w celu ustalenia ambitnych i rygorystycznych celów programu (w tym szczegółowych technicznych kamieni milowych i innych działań programu), niezbędnych do zarządzania portfelem wyrafinowanych projektów badawczo-rozwojowych. Biorąc pod uwagę przyspieszający rozwój nowoczesnych technologii AI, w tym LLMs, przejście na nowy paradygmat finansowania innowacji wydaje się zasadne. Krokiem pośrednim w ramach wprowadzania takiej zmiany powinno być uruchomienie pilotażowego programu badawczego w Polsce zgodnego z założeniami ARPA.

Bibliografia

Breakstone J. i in., *Students' Civic Online Reasoning: A National Portrait*, „Educational Researcher” 2021, nr 50, s. 505–515. <https://doi.org/10.3102/0013189X211017495>.

Europol, *ChatGPT. The impact of Large Language Models on Law Enforcement*, Luxembourg 2023.

Faesen L. i in., *Red Lines & Baselines Towards a European Multistakeholder Approach to Counter Disinformation*, The Hague Centre for Strategic Studies 2021.

Felson M., Cohen L., *Human ecology and crime: A routine activity approach*, „Human Ecology” 1980, t. 8, s. 389–406. <https://doi.org/10.1007/BF01561001>.

Fuocco M.A., *Trial and error: They had larceny in their hearts but little in their heads*, „Pittsburgh Post-Gazette” 1996.

GIFCT Red Team Working Group, *Considerations of the Impacts of Generative AI on Online Terrorism and Extremism*, [bmw] 2023.

Ji Z. i in., *Survey of Hallucination in Natural Language Generation*, „ACM Computing Surveys” 2023, t. 55, nr 12, s. 1–38. <https://doi.org/10.1145/3571730>.

McGrew S. i in., *Can Students Evaluate Online Sources? Learning From Assessments of Civic Online Reasoning*, „Theory & Research in Social Education” 2018, t. 46, s. 165–193. <https://doi.org/10.1080/00933104.2017.1416320>.

Raman G. i in., *How weaponizing disinformation can bring down a city's power grid*, „PloS One” 2020, nr 15. <https://doi.org/10.1371/journal.pone.0236517>.

Vaidhyanathan S., *Antisocial media: How Facebook Disconnects Us and Undermines Democracy*, New York 2018.

Vaswani A. i in., *Attention is All you Need*, w: *Advances in Neural Information Processing Systems 30 (NIPS 2017)*, I. Guyon i in. (red.), Long Beach 2017, s. 5998–6008.

Waniek M. i in., *Traffic networks are vulnerable to disinformation attacks*, „Scientific Reports” 2021, nr 11. <https://doi.org/10.1038/s41598-021-84291-w>.

Źródła internetowe

[heythereitsbeth], *Just came across this sub and thought I'd share mine from the start of the year*, Reddit, https://www.reddit.com/r/scambait/comments/17w6vx4/just_came_across_this_sub_and_thought_id_share/?rdt=40738 [dostęp: 8 XI 2023].

AFP Kenya, *Fake subtitles added to old clip of Putin talking about Ukraine war, not Israel-Gaza conflict*, AFP Fact Check, 17 X 2023 r., <https://factcheck.afp.com/doc.afp.com.33YG8TE> [dostęp: 8 XI 2023].

Bochyńska N., *#CyberMagazyn: Politycy narzędziem w rękach Kremla? „Świadomość jest bardzo niska”*, CyberDefence24, 21 X 2023 r., <https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-politycy-narzedziem-w-rekach-kremla-swiadomosc-jest-bardzo-niska> [dostęp: 8 XI 2023].

Borji A., *Stochastic Parrots or Intelligent Systems? A Perspective on True Depth of Understanding in LLMs*, preprint, SSRN, 20 VII 2023 r., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4507038 [dostęp: 8 IX 2023]. <http://dx.doi.org/10.2139/ssrn.4507038>.

Bowman S.R., *Eight Things to Know about Large Language Models*, preprint, arXiv, 2 IV 2023 r., <https://arxiv.org/abs/2304.00612> [dostęp: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2304.00612>.

Brewster T., *Armed With ChatGPT, Cybercriminals Build Malware And Plot Fake Girl Bots*, Forbes, 6 I 2023 r., <https://www.forbes.com/sites/thomasbrewster/2023/01/06/chatgpt-cybercriminal-malware-female-chatbots/> [dostęp: 9 XI 2023].

Currie R., *California man's business is frustrating telemarketing scammers with chatbots*, The Register, 3 VII 2023 r., https://www.theregister.com/2023/07/03/jolly_roger_telephone_company/ [dostęp: 8 XI 2023].

Derner E., Batistič K., *Beyond the Safeguards: Exploring the Security Risks of ChatGPT*, arXiv, preprint, 13 V 2023 r., <https://arxiv.org/abs/2305.08005> [dostęp: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2305.08005>.

Goldfarb J., *Applying AI to API Security*, SecurityWeek, 11 X 2023 r., <https://www.securityweek.com/applying-ai-to-api-security/> [dostęp: 8 XI 2023].

Gwozdowska A. i in., *Wojna informacyjna 2022–2023. Przebieg i wnioski*, NASK, 25 V 2023 r., <https://www.nask.pl/pl/raporty/raporty/5204,Raport-quotWojna-informacyjna-20222023-Przebieg-i-wnioskiquot.html> [dostęp: 8 XI 2023].

Heiding F. i in., *Devising and Detecting Phishing: Large Language Models vs. Smaller Human Models*, preprint, arXiv, 23 VII 2023 r., <https://arxiv.org/abs/2308.12287> [dostęp: 8 XI 2023]. <https://doi.org/10.48550/arXiv.2308.12287>.

INFO OPS Poland Foundation, *Model dystrybucji informacji w wirtualnym środowisku informacyjnym na bazie rozpoznanego rosyjskiego podstawowego modelu dystrybucji wiadomości manipulacyjnych*, Disinfo Digest, 9 VI 2023 r., <https://disinfodigest.pl/model-dystrybucji-informacji-w-wirtualnym-srodowisku-informacyjnym-na-bazie-rozpoznanego-rosyjskiego-podstawowego-modelu-dystrybucji-wiadomosci-manipulacyjnych/> [dostęp: 8 XI 2023].

Kelley D., *WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks*, SlashNext, 13 VII 2023 r., <https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/> [dostęp: 22 XI 2023].

Lai T. i in., *Psy-LLM: Scaling up Global Mental Health Psychological Services with AI-based Large Language Models*, preprint, arXiv, 22 VII 2023 r., <https://arxiv.org/abs/2307.11991> [dostęp: 8 XI 2023]. <https://doi.org/10.48550/arXiv.2307.11991>.

McGuffie K., Newhouse A., *The Radicalization Risks of GPT-3 and Advanced Neural Language Models*, preprint, arXiv, 15 IX 2020 r., <https://arxiv.org/abs/2009.06807> [dostęp: 8 XI 2023]. <https://doi.org/10.48550/arXiv.2009.06807>.

NASK (@WeryfikacjaNASK), *Wraz z postępem technologicznym, rozwój AI staje się coraz bardziej widoczny w różnych dziedzinach naszego życia*, X, 26 X 2023 r., <https://twitter.com/WeryfikacjaNASK/status/1717487918556594437> [dostęp: 8 XI 2023].

Nowe oszustwo na WhatsAppie, „Kurier Szczeciński”, 5 VIII 2023 r., <https://24kurier.pl/aktualnosci/wiadomosci/nowe-oszustwo-na-whatsappie/> [dostęp: 8 XI 2023].

Podolak J. i in., *Analyzing the Influence of Language Model-Generated Responses in Mitigating Hate Speech on Social Media Directed at Ukrainian Refugees in Poland*, preprint, arXiv, 28 XI 2023 r., <https://arxiv.org/abs/2311.16905> [dostęp: 30 XI 2023]. <https://doi.org/10.48550/arXiv.2311.16905>.

Saunders W. i in., *Self-critiquing models for assisting human evaluators*, preprint, arXiv, 12 VI 2022 r., <https://arxiv.org/abs/2206.05802> [dostęp: 9 XI 2023]. <https://doi.org/10.48550/arXiv.2206.05802>.

Simmons A., Vasa R., *Garbage in, garbage out: Zero-shot detection of crime using Large Language Models*, preprint, arXiv, 4 VII 2023 r., <https://arxiv.org/abs/2307.06844> [dostęp: 9 XI 2023]. <https://doi.org/10.48550/arXiv.2307.06844>.

Skąd Polacy czerpią informacje? Badanie IBRIS i IBIMS kwiecień 2021, IBiMS, http://www.ibims.pl/wp-content/uploads/2021/04/IBIMS_media_2021.pdf [dostęp: 8 XI 2023].

Toulas B., *Cybercriminals train AI chatbots for phishing, malware attacks*, Bleeping Computer, 1 VIII 2023 r., <https://www.bleepingcomputer.com/news/security/cybercriminals-train-ai-chatbots-for-phishing-malware-attacks/> [dostęp: 9 XI 2023].

Vallance C., Rahman-Jones I., *Urgent need for terrorism AI laws, warns think tank*, BBC News, 3 I 2024 r., <https://www.bbc.com/news/technology-67872767> [dostęp: 10 I 2024].

Yin S. i in., *A Survey on Multimodal Large Language Models*, preprint, arXiv, 23 VI 2023 r., <https://arxiv.org/abs/2306.13549> [dostęp: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2306.13549>.

Zou A. i in., *Universal and Transferable Adversarial Attacks on Aligned Language Models*, preprint, arXiv, 27 VII 2023 r., <https://arxiv.org/abs/2307.15043> [dostęp: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2307.15043>.

Julia Puczyńska

Doktorantka w IDEAS NCBR oraz w Szkole Doktorskiej Technologii Informacyjnych i Biomedycznych Instytutów PAN. Zajmuje się zwalczaniem dezinformacji i analizą mediów społecznościowych. Absolwentka psychologii i kryminalistyki. Opracowywała zagadnienia

związane z pamięcią, rozpoznawaniem twarzy i wykrywaniem kłamstw. Prowadzi projekt Zgłoś Trola we współpracy z DC9 i Fundacją Gremka.

Kontakt: julia.puczynska@ideas-ncbr.pl

Marcin Podhajski

Doktorant w zespole badawczym „AI dla bezpieczeństwa” IDEAS NCBR oraz w Szkole Doktorskiej Technologii Informacyjnych i Biomedycznych Instytutów PAN. Zajmuje się sztuczną inteligencją, uczeniem maszynowym oraz analizą sieci społecznościowych.

Dr Karolina Wojtasik

Specjalistka ds. bezpieczeństwa, pracownik naukowy i nauczyciel akademicki, biegły sądowy, wiceprezes ds. naukowych Polskiego Towarzystwa Bezpieczeństwa Narodowego, pracownik Rządowego Centrum Bezpieczeństwa. Zajmuje się szeroko pojętym bezpieczeństwem infrastruktury krytycznej i obiektów podlegających obowiązkowej ochronie, zwłaszcza w kontekście zagrożeń bezpieczeństwa fizycznego i osobowego. Autorka książek pt. *Anatomia zamachu. O strategii i taktyce terrorystów*, *Ścieżki radykalizacji dżihadystycznej*, współautorka książki pt. *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku* i wielu innych publikacji związanych z terroryzmem oraz bezpieczeństwem i budowaniem odporności infrastruktury krytycznej. Twórczyni kanału popularnonaukowego Anatomia zamachu na YouTube oraz portalu Projekt IK.

Dr Tomasz P. Michalak

Lider samodzielnego zespołu badawczego w IDEAS NCBR oraz wykładowca na Wydziale Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego. Absolwent Wydziału Nauk Ekonomicznych Uniwersytetu Warszawskiego. W czasie kariery naukowej prowadził badania na Wydziale Informatyki Uniwersytetu Oksfordzkiego, w Szkole Inżynierii i Informatyki Uniwersytetu w Southampton, na Wydziale Informatyki Uniwersytetu w Liverpoolu oraz Wydziale Ekonomii Stosowanej Uniwersytetu w Antwerpii, na którym otrzymał tytuł doktora ekonomii.

The background of the page is a complex, abstract pattern. It features a series of parallel, slightly curved lines that create a sense of depth and movement. Overlaid on these lines is a circular pattern of small, light-colored dots, which appears to be a stylized representation of a fingerprint or a similar textured surface. The overall effect is a high-contrast, monochromatic design.

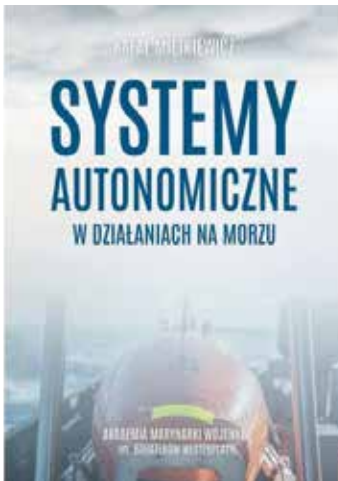
ARTYKUŁY RECENZYJNE /
RECENZJE

Recenzja książki: Rafał Miętkiewicz, Systemy autonomiczne w działaniach na morzu¹

Jędrzej Łukasiewicz

Zakład Lotnictwa, Wydział Inżynierii Lądowej i Transportu,
Politechnika Poznańska

 <https://orcid.org/0000-0002-7082-8511>



Rozwój nowoczesnych materiałów konstrukcyjnych, miniaturyzacja elementów elektronicznych, a także dostęp do źródeł o dużej gęstości energii przypadającej na jednostkę ich masy umożliwiły dynamiczny rozwój platform bezzałogowych. Zalicza się do nich bezzałogowe statki powietrzne, bezzałogowe pojazdy kołowe i gąsienicowe oraz łodzie pływające po powierzchni i pod powierzchnią wody. Cechami systemów bezzałogowych decydującymi o ich wykorzystaniu w różnych obszarach działalności ludzkiej są: brak operatora na pokładzie statku, możliwość umieszczenia na nich dowolnego ładunku, możliwość wykonania misji w sposób autonomiczny, automatyczny lub pod manualną kontrolą operatora. Niebagatelne znaczenie ma też

działania, możliwość wykonania misji w sposób autonomiczny, automatyczny lub pod manualną kontrolą operatora. Niebagatelne znaczenie ma też

¹ R. Miętkiewicz, *Systemy autonomiczne w działaniach na morzu*, Gdynia 2023, Akademia Marynarki Wojennej im. Bohaterów Westerplatte, 495 s.

niższa cena zakupu takiego systemu w porównaniu z analogiczną platformą załogową.

Sytuacja geopolityczna w regionie Morza Bałtyckiego oraz doniesienia o atakach na infrastrukturę Nord Stream, który jest systemem zaopatrzenia w energię i paliwa, a zatem stanowi część infrastruktury krytycznej, zmuszają do zwrócenia szczególnej uwagi na ten region, ponieważ ma on ogromne znaczenie dla bezpieczeństwa militarnego i gospodarczego Polski.

W 2023 r. ukazała się licząca 495 stron monografia kmdr. por. dr. Rafała Miętkiewicza zatytułowana *Systemy autonomiczne w działaniach na morzu*. Jest to pozycja wyjątkowa, ponieważ stanowi pierwsze opracowanie w języku polskim, w którym tak obszernie opisano rolę nowoczesnych morskich systemów bezzałogowych w działaniach na morzu. Na rynku wydawniczym dotychczas brakowało publikacji odnoszącej się zarówno do bezpieczeństwa akwenu, jak i do technologii, w tym bezzałogowych platform, których wykorzystanie mogłoby podnieść poziom tego bezpieczeństwa.

Autor monografii jest oficerem Marynarki Wojennej RP i oficerem liniowym z kilkunastoletnim doświadczeniem na pokładach okrętów morskiej walki minowej (pełnił m.in. funkcję dowódcy ORP Śniardwy), a także naukowcem i wykładowcą akademickim, adiunktem w Akademii Marynarki Wojennej w Gdyni. Jest również członkiem Polskiego Towarzystwa Bezpieczeństwa Narodowego oraz Polskiego Towarzystwa Nautologicznego, ekspertem Instytutu Polityki Energetycznej im. Ignacego Łukasiewicza w Rzeszowie. W 2023 r. był ekspertem zewnętrznym międzyresortowego zespołu zadaniowego ds. rozwiązań w zakresie niszczenia, unieruchamiania i przejęcia kontroli nad bezzałogowym statkiem pływającym w kontekście bezpieczeństwa obiektów infrastruktury krytycznej zlokalizowanych u wybrzeży Bałtyku lub poza granicami RP (powołanym przy Międzyresortowym Zespole ds. Zagrożeń Terrorystycznych).

Recenzowana monografia Rafała Miętkiewicza została podzielona na pięć rozdziałów, z których każdy kończy się podsumowaniem.

Rozdział pierwszy zatytułowany *Systemy autonomiczne w środowisku morskim* zawiera obszerne charakterystyki platform bezzałogowych. Autor dokonał ich podziału ze względu na cechy użytkowe, co zilustrował schematami i tabelami, dzięki którym łatwiej usystematyzować wiadomości. Ponieważ te systemy mogą wykonywać misje na niejednakowym poziomie autonomii, zostały opisane różne sposoby podziału jej poziomów, w tym te wskazane przez Lloyd's Register, International Maritime Organization,

Roadmap FY2011-2036 oraz Multinational Capability Development Campaign. Kolejne strony zawierają niezwykle interesujące opisy nie tylko autonomicznych systemów nawodnych i podwodnych, lecz także systemów latających, zarówno cywilnych, jak i wojskowych, przy czym autor nie ograniczył się do systemów już znanych i wykorzystywanych. Dodatkowym walorem są kolorowe ilustracje wzbogacające te charakterystyki. W rozdziale zostały wskazane technologie, które mają szansę na powszechne wykorzystanie w dłuższej perspektywie czasowej. Autor zaliczył do nich autonomiczne systemy biomimetyczne oraz roje, ławice lub stada autonomicznych platform morskich. Ze względu na fakt, że roje, ławice lub stada platform bezzałogowych to technologia, której badania i rozwój rozpoczęły się stosunkowo niedawno, analiza możliwości jej wykorzystania zarówno do ochrony portów morskich oraz baz, jak i do atakowania jednostek nawodnych i podwodnych przeciwnika jest szczególnie interesująca. Jak wynika z dostępnych danych, wiele krajów na świecie prowadzi intensywne prace nad budową autonomicznych systemów bezzałogowych.

Rozdział drugi pt. *Bałtyk jako akwen wykorzystania morskich systemów autonomicznych* to właściwie mała encyklopedia wiedzy o możliwościach użycia autonomicznych systemów bezzałogowych na omawianym obszarze. Czytelnik znajdzie tu informacje na temat polskich obszarów morskich, ich podziału i wielkości powierzchni, uzupełnione czytelną mapą. W dalszej części rozdziału autor opisał uwarunkowania mające wpływ na eksploatację autonomicznych platform bezzałogowych w warunkach morskich. Zaliczył do nich: liczbę i lokalizację polskich portów morskich wraz z wolumenem przeładowanych w nich ładunków, projekty infrastrukturalne służące przesyłowi surowców lub eksploatacji zasobów naturalnych poprzez ich wydobywanie z dna morskiego, budowę morskich farm wiatrowych wraz z infrastrukturą przesyłu energii elektrycznej na brzeg oraz lokalizację amunicji konwencjonalnej i broni chemicznej leżących na dnie morskim. Ważną częścią jest charakterystyka uwarunkowań środowiskowych Morza Bałtyckiego, w tym m.in. zjawisk atmosferycznych mających wpływ na wykonywanie misji platform bezzałogowych. Ponadto autor analizuje wpływ czynników środowiskowych na działanie bezzałogowych platform nawodnych, powietrznych i podwodnych.

Kolejny rozdział, zatytułowany *Współczesne zagrożenia bezpieczeństwa w domenie morskiej* i wzbogacony mapkami sytuacyjnymi, tabelami, zdjęciami i schematami, to pogłębiona analiza zagrożeń występujących obecnie, a także tych, które mogą się pojawić w przyszłości. Autor szczegółowo

opisał wpływ agresywnej polityki Federacji Rosyjskiej, m.in. na bezpieczeństwo Polski. Dużo miejsca poświęcił konfliktowi w Ukrainie oraz jego oddziaływaniu na architekturę bezpieczeństwa Polski i regionu, w którym ta geograficznie leży. Warta podkreślenia jest analiza zagrożeń w obszarze bezpieczeństwa morskiego. Autor obszernie omówił różne źródła tych zagrożeń. Przeanalizował też wybrane incydenty, do których doszło w rejonie Morza Bałtyckiego.

Przedostatni rozdział *Zadania Marynarki Wojennej w świetle wyzwań i zagrożeń bezpieczeństwa* jest poświęcony rozważaniom dotyczącym zadań Marynarki Wojennej RP w kontekście zagrożeń dla państwa polskiego zdefiniowanych i opisanych w poprzednich częściach książki. Obecna sytuacja geopolityczna Polski niejako zmusza do zadania sobie pytań o stan Marynarki Wojennej RP oraz jej potencjał do obrony interesów Rzeczypospolitej Polskiej. Autor podjął próbę odpowiedzi na te pytania.

Do momentu rozpoczęcia pełnoskalowej wojny w Ukrainie marynarki różnych państw w sposób ograniczony wykorzystywały bezzałogowe platformy morskie. Po jej wybuchu autonomiczne platformy morskie coraz powszechniej są używane do ataków zarówno na jednostki marynarki wojennej wroga, jak i na elementy jego infrastruktury portowej i transportowej. Pojawiły się także doniesienia o wykorzystaniu wielu platform jednocześnie w sposób, który pozwala mówić o ataku z użyciem roju, ławicy czy stada. Dla specjalistów zajmujących się tematyką morską jest to możliwość wyciągnięcia wniosków dla narodowych sił morskich. Także osoby odpowiedzialne za bezpieczeństwo Morza Bałtyckiego powinny bacznie przyglądać się rozwojowi sytuacji w Ukrainie. Bazując na jej doświadczeniach wojennych, uwzględniając przynależność Polski do NATO oraz biorąc pod uwagę polskie interesy na obszarze Morza Bałtyckiego i rozwój technologiczny, należy zaproponować koncepcję użycia autonomicznych, morskich platform bezzałogowych.

Tej tematyce jest poświęcony ostatni, piąty rozdział pt. *Koncepcja wykorzystania morskich systemów autonomicznych*, najważniejszy według autora niniejszej recenzji. Zaproponowana w tej części koncepcja wykorzystania morskich systemów autonomicznych w zwalczaniu aktów terrorystycznych w polskiej strefie ekonomicznej powinna stać się przedmiotem pogłębionych analiz ze strony dowodzących Siłami Zbrojnymi RP oraz służbami i formacjami kontrterrorystycznymi odpowiedzialnymi za bezpieczeństwo państwa polskiego. W związku z dynamiką zmian związanych z działaniami militarnymi w Ukrainie należy jednak założyć, że treść tego rozdziału to

dopiero początek rozważań, które trzeba będzie podejmować wraz z pojawianiem się kolejnych informacji o użyciu autonomicznych systemów bezzałogowych w działaniach morskich. Takie rozważania wymagają dogłębnej analizy treści zawartych w pierwszych czterech rozdziałach omawianej monografii. W tym sensie stanowi ona zbiór informacji koniecznych do zarządzania bezpieczeństwem morskim Rzeczypospolitej Polskiej, rodzaj fundamentu, na którym można budować politykę bezpieczeństwa.

Wiedza zawarta w publikacji *Systemy autonomiczne w działaniach na morzu* jest tak obszerna, że nie wystarczy jej jednorazowa lektura. Dogłębne zrozumienie opisanych zagadnień wymaga powrotu do wybranych fragmentów. Dużą zaletą jest to, że monografia obejmuje nie tylko spostrzeżenia i wnioski jej autora, lecz także liczne odniesienia do innych źródeł, polskich i zagranicznych, co pozwala czytelnikowi na weryfikację treści i poszerzanie zasobu wiadomości na podstawie prac innych autorów. Kolejny walor to sposób przekazywania treści – książka jest napisana językiem fachowym, ale czytelnym, a wykresy, tabele, diagramy i zdjęcia ułatwiają odbiorcy usystematyzowanie informacji. Może być czytana zarówno przez profesjonalistów zajmujących się systemami bezzałogowymi w działaniach na morzu, jak i przez osoby, które dopiero rozpoczynają przygodę z autonomicznymi systemami bezzałogowymi.

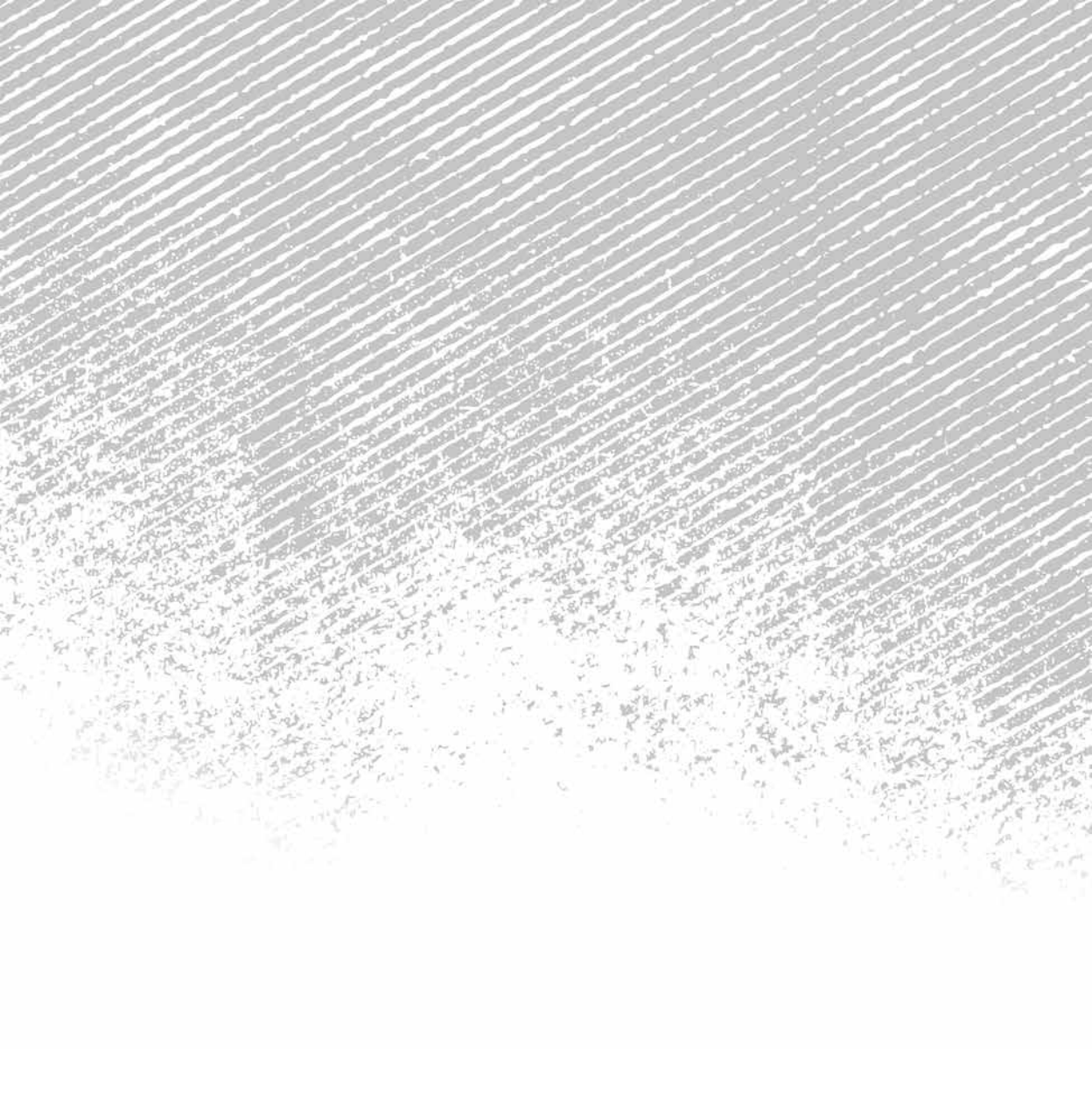
Na polskim i zagranicznym rynku wydawniczym jest to najlepsza pozycja na temat wykorzystania systemów autonomicznych w działaniach morskich, ze szczególnym uwzględnieniem Morza Bałtyckiego. O poruszonych w niej zagadnieniach można oczywiście przeczytać w pracach innych autorów, ale w żadnej publikacji nie zostały one zebrane w całość. Po przetłumaczeniu na język angielski książka Rafała Miętkiewicza może być z powodzeniem wykorzystana do promowania polskiej racji stanu w ramach grup roboczych NATO w obszarze użycia systemów autonomicznych do zapewnienia bezpieczeństwa Morza Bałtyckiego oraz ulokowanej tam infrastruktury krytycznej.

Dr Jędrzej Łukasiewicz

Adiunkt w Zakładzie Lotnictwa Wydziału Inżynierii Lądowej i Transportu Politechniki Poznańskiej, instruktor pilotażu bezzałogowych statków powietrznych w ośrodku szkolenia Politechniki Poznańskiej. Uczestnik gremiów eksperckich na poziomie unijnym (DG MOVE,

DG HOME), krajowym i międzyresortowym ds. bezpieczeństwa infrastruktury krytycznej oraz budowania odporności na zagrożenia ze strony bezzałogowych statków powietrznych. Ekspert Rządowego Centrum Bezpieczeństwa w zakresie zagrożeń, których źródłem są bezzałogowe statki powietrzne.

Kontakt: jedrzej.lukasiewicz@put.poznan.pl




VARIA

Budowanie odporności infrastruktury krytycznej w świetle zagrożeń asymetrycznych i terroryzmu

Tendencje legislacyjne w polskiej implementacji dyrektywy CER ze szczególnym uwzględnieniem aspektów standaryzacji i certyfikacji rozwiązań organizacyjno-technicznych

Adam Tatarowski

Zakład Rozwoju Technicznej Ochrony Mienia „TECHOM”

 <https://orcid.org/0009-0007-5503-6819>

Źródła i kontekst współczesnych zagrożeń asymetrycznych i terroryzmu

W latach 30. XX w. Związek Sowiecki, za sprawą koncepcji Georgija Issersona i Władimira Triandafułowa, wyznaczał standardy światowe w myśli wojskowej. Isserson jako pierwszy w historii opracował nowatorską doktrynę wojskową opartą na zastosowaniu operacji głębokich, tzn. uderzenia na całej głębokości wojsk wroga, na całej linii frontu¹. W czasach postalinowskich płk Jewgienij Messner rozwijał koncepcję prowadzenia działań wojennych z wykorzystaniem środków niemilitarnych (tzw. wojen buntowniczych)², opisując rolę terroru w prowadzeniu działań zbrojnych,

¹ Г.С. Иссерсон, *Эволюция оперативного искусства*, Москва 1937 (G.S. Isserson, *Ewolucja operatiwnogo iskusstwa*, Moskwa 1937).

² Е.Э. Месснер, *Хочешь Мира, Победи Мятежевойну!*, *Творческое наследие Е.Э. Месснера*, Москва 2005 (Je.E. Miessnier, *Chociesz Mira, Pobiedi Miatieżewojnu! Tworczeskoje nasledije Je.E. Miessniera*, Moskwa 2005), s. 110.

wykorzystanie w walkach ludności cywilnej i konkretnych grup społecznych, tworzenie jednostek paramilitarnych w sytuacji zmniejszania różnic między stanem wojny a stanem pokoju. Kontynuatorem tych podejść jest gen. Walerij Gierasimow, Szef Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej. W 2013 r. w szeroko komentowanym w mediach referacie³ przedstawił założenia wojny hybrydowej opierające się na zsynchronizowanym użyciu militarnych i niemilitarnych środków, za pomocą których będzie możliwe osiągnięcie celów strategicznych i politycznych. Gierasimow omówił takie działania, jak wprowadzanie kontyngentu międzynarodowych sił pokojowych pod pretekstem obrony praw człowieka, izolacja polityczna, sankcje ekonomiczne, blokady szlaków komunikacji lądowej, morskiej i lotniczej, zagrożenie użyciem siły.

Od 2014 r., od najazdu tzw. zielonych ludzików i aneksji Krymu, można to wszystko obserwować w praktyce – wojna toczy się w zasadzie cały czas i nie jest kontynuacją polityki, o czym pisał Carl von Clausewitz, ale jej elementem⁴. Agresja rosyjska, która w lutym 2022 r. przybrała formę pełnoskalową, dobitnie pokazuje, że ewolucja zagrożeń asymetrycznych znacznie przyspieszyła i ma wpływ nie tylko na obszar stricte militarny, lecz także na całe środowisko bezpieczeństwa. A zatem pojęcie zagrożeń asymetrycznych, zwięźle opisanych w *Słowniku terminów i definicji NATO* jako takich, które wynikają z możliwości zastosowania różnych środków i metod w celu obejścia lub neutralizacji silnych punktów przeciwnika i wykorzystania jego słabości, aby uzyskać niewspółmierne cele⁵, należy obecnie rozumieć znacznie szerzej – w wymiarze cywilizacyjnym, społecznym, kulturowym i technologicznym. Co więcej, terroryzm, którego istotą zawsze było celowe i świadome atakowanie niewinnych, postronnych osób czy grup społecznych z zamiarem zastraszenia władz państwowych lub społeczeństwa, przybrał formę znacznie bardziej rozmytą. Collin Powell słusznie zauważył, że chociaż cywilizowany świat przez setki lat dążył do ograniczenia destrukcyjności wojen poprzez np. rozróżnienie cywil – żołnierz, to współczesny terroryzm tę różnicę coraz bardziej zamazuje⁶. Całokształt tych zagrożeń

³ В. Герасимов, *Ценность науки в предвидении*, „Военно-промышленный курьер” 2013 (B. Gierasimow, *Cennost' nauki w priedwidienii*, „Wojenno-promyszlennyj kurjer” 2013), nr 8, s. 2–3.

⁴ C. von Clausewitz, *O wojnie*, Warszawa 2022.

⁵ AAP-6 *Słownik terminów i definicji NATO*, 2021 r.

⁶ Za: J.M. Fish, S.J. McCraw, Ch.J. Reddish, *Fighting in the gray zone: A strategy to close the preemption gap*, Strategic Studies Institute 2004, s. 6.

staje się dziś wyzwaniem dla podmiotów odpowiedzialnych za ochronę infrastruktury krytycznej (dalej: IK) i zapewnienie jej odporności. W niniejszym artykule opisano tendencje legislacyjne w tym obszarze, ze szczególnym uwzględnieniem aspektów standaryzacji i certyfikacji rozwiązań organizacyjno-technicznych wynikających z dyrektywy CER.

Emerging risks w kontekście zagrożeń asymetrycznych i współczesnego terroryzmu – wyzwania w obszarze prawno-normatywnym

Pandemia COVID-19 znacznie przyspieszyła rozpoczęte w 2018 r. prace nad nową specyfikacją techniczną *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience*, opisującą sposoby podejścia do oceny i zarządzania nowymi rodzajami ryzyka, które są trudne do przewidzenia i zrozumienia ze względu na brak wystarczającej ilości danych i zweryfikowanych informacji (z ang. *emerging risks*). Ich zaistnienie, z perspektywy jakiejś organizacji, np. podmiotu krytycznego⁷, może wynikać z niespodziewanych zmian w obszarze organizacyjnym, z rozwoju technologicznego czy społecznego, procesów globalizacyjnych, zawirowań politycznych, a w szerszym kontekście – z nasilania się zagrożeń asymetrycznych i terroryzmu. Te rodzaje ryzyka charakteryzują się wysokim stopniem niepewności i mogą prowadzić do poważnych konsekwencji w zakresie odporności, bezpieczeństwa oraz ciągłości działania (w wymiarze operacyjnym i biznesowym) organizacji. Zarządzanie nimi wymaga ciągłego monitorowania i gromadzenia informacji oraz elastyczności w podejmowaniu decyzji.

Aktualna koncepcja oceny ryzyka w IK opiera się na założeniach „podstawowej” normy *PN-ISO 31000:2018-08 Zarządzanie ryzykiem – wytyczne* i jest osadzona w skomplikowanym otoczeniu prawno-normatywnym, w którym nadal funkcjonuje podejście „obiektywne” do wyłaniania podmiotów IK. Zgodnie z Narodowym Programem Ochrony Infrastruktury Krytycznej (NPOIK)⁸ wyłanianie to odbywa się w trzech etapach. W pierwszym

⁷ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333/164 z 27 XII 2022 r.).

⁸ Narodowy Program Ochrony Infrastruktury Krytycznej 2023, <https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej> [dostęp: 29 XI 2023].

dokonywane ustalenia, do którego systemu (według NPOIK – np. łączności, ochrony zdrowia, sieci teleinformatycznych) należy potencjalny obiekt IK (także: urządzenie, instalacja lub usługa) i porównuje się jego cechy z kryteriami danego systemu (kryteria są niejawne). W drugim sprawdza się, czy dany obiekt odgrywa rolę, o której mowa w definicji ustawowej⁹. Następnie analizuje się, czy możliwe skutki zniszczenia lub zaprzestania funkcjonowania potencjalnej IK spełnią przynajmniej dwa kryteria przekrojowe odnoszące się do społecznych skutków destrukcji lub zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi. Kryteria te obejmują:

- ofiary w ludziach,
- skutki finansowe,
- konieczność ewakuacji,
- utratę usługi,
- czas odbudowy,
- efekt międzynarodowy,
- unikatowość (w sensie niemożności zastąpienia i odtworzenia zniszczonego obiektu, urządzenia lub instalacji).

I chociaż równoległe do podejścia „obiektywego” funkcjonuje „usługowy” system wyłaniania operatorów usług kluczowych w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa¹⁰, to zasięg tej regulacji jest ograniczony, dotyczy bowiem wyłącznie usług ujętych w tej ustawie i tylko takich, które odnoszą się do systemów informacyjnych. Decyzję uznającą podmiot za operatora usługi kluczowej wydaje się, jeśli:

- podmiot świadczy usługę kluczową,
- świadczenie tej usługi zależy od systemów informacyjnych,
- incydent miałby istotny skutek, powodujący zakłócenie świadczenia usługi kluczowej przez tego operatora.

Ten dualizm, z uwagi na wymogi stawiane przez dyrektywę w sprawie odporności podmiotów krytycznych (dyrektywa CER, z ang. *The Critical Entities Resilience Directive*), niebawem zaniknie. W październiku 2024 r. należy oczekiwać uchwalenia krajowych przepisów implementujących tę dyrektywę, wprowadzających „usługowy” model wyznaczania podmiotów IK. Dyrektywa CER wprowadza mechanizm interwencjonizmu państwowego.

⁹ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2023 r. poz. 122).

¹⁰ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2023 r. poz. 913, ze zm.).

Zgodnie z jej zapisami państwa członkowskie UE stają się współodpowiedzialne za utrzymanie dostępności usługi kluczowej i będą miały możliwość bezpośredniego dotowania podmiotów gospodarczych świadczących takie usługi. Państwa członkowskie będą wyznaczać usługi kluczowe, wskazywać operatorów i egzekwować poziom dostępności usług. To zdecydowana zmiana podejścia nie tylko w relacji obywatel–państwo, lecz także biznes–państwo. Przed IK stoją więc duże wyzwania. Podmiot krytyczny będzie zobowiązany do przeprowadzenia własnej oceny ryzyka, opartej na normie *PN-ISO 31000:2018-08 Zarządzanie ryzykiem – wytyczne*, ale z uwzględnieniem możliwie najszerszego spektrum czynników ryzyka, w tym takich, które są uznawane za *emerging risks*.

Ocena ryzyka w infrastrukturze krytycznej – nowe podejścia

Operatorzy IK stosują różne metodyki zarządzania bezpieczeństwem, w zależności od świadomości, poziomu wiedzy i zrozumienia obszaru, jakim się zajmują. Każda uznana metodyka opiera się na wzorcu, którym jest norma *PN-ISO 31000:2018-08 Zarządzanie ryzykiem – wytyczne*. Zakłada ona realizację procesu zarządzania ryzykiem w trzech krokach:

- 1) ustalenie kontekstu,
- 2) ocena ryzyka (identyfikacja zagrożeń, analiza i szacowanie ryzyka),
- 3) decyzja o postępowaniu z ryzykiem.

Większość metodyk zarządzania bezpieczeństwem stosowanych w Polsce i w krajach, które są uznawane za wiodące w tym obszarze (np. Niemcy, Szwecja, Kanada, USA, Irlandia, Holandia czy Australia), bazuje na tej normie¹¹. Autorzy publikacji *Zarządzanie bezpieczeństwem infrastruktury krytycznej i ciągłością usług kluczowych państwa* szeroko analizują podejścia do oceny i zarządzania ryzykiem stosowane w tych krajach. Prezentują metodykę Zarządzania Sytuacyjnego Bezpieczeństwem Infrastruktury Krytycznej (ZS-BIK) wraz z Integralnym Modelem Bezpieczeństwa Infrastruktury Krytycznej (IM-BIK), który z kolei jest zapleczem narzędziowym metodyki ZS-BIK. Etapy tego zarządzania to:

- powołanie zespołu,
- określenie progów bezpieczeństwa,

¹¹ M. Kisilowski i in., *Zarządzanie bezpieczeństwem infrastruktury krytycznej i ciągłością usług kluczowych państwa*, Warszawa 2021.

- odwzorowanie charakterystyk IK,
- wygenerowanie scenariuszy zdarzeń niekorzystnych,
- sformułowanie problemu decyzyjnego,
- szacowanie ryzyka,
- wdrożenie zabezpieczeń.

W dobie rosnących zagrożeń asymetrycznych, w tym związanych z działaniami terrorystycznymi, cennym uzupełnieniem (a przede wszystkim pomocą i wsparciem) przy dokonywaniu – w ramach np. metodyki ZS-BIK – oceny ryzyka przez podmioty krytyczne są normy czy specyfikacje techniczne, takie jak:

- *PN-EN IEC 31010:2020-01 Zarządzanie ryzykiem – Techniki oceny ryzyka,*
- *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience,*
- *ISO/IEC 27005:2018 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.*

Zdolność podmiotu krytycznego do przewidywania różnych okoliczności, przygotowania się i reagowania na nie powinna być najważniejszym wymogiem w procesie skutecznego zarządzania ryzykiem. Podmiot krytyczny powinien¹² m.in.:

- zoptymalizować komunikację wewnątrz i na zewnątrz organizacji,
- ustanowić skuteczny sposób gromadzenia aktualnych informacji na temat pojawiających się rodzajów ryzyka,
- przeciwdziałać dezinformacji,
- opracować sposób, w jaki osoby odpowiedzialne za zarządzanie ryzykiem mogą wpływać na kierownictwo,
- budować zaufanie w obrębie organizacji i w relacjach z podmiotami współpracującymi, w tym z administracją państwową,
- zachęcać i upoważniać odpowiednie osoby w organizacji do zgłaszania istotnych według nich sygnałów związanych z potencjalnym wystąpieniem nowych rodzajów ryzyka.

Proces identyfikowania ryzyk wymaga od podmiotu krytycznego świadomości dotyczącej dynamicznych zmian zachodzących w środowisku, w którym funkcjonuje. Pomimo wdrożenia struktury identyfikacji ryzyk (opartej na ww. normach czy też innych dokumentach, np. odnoszących się

¹² *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience.*

do zagrożeń związanych z aktami terroru¹³) powinien on korzystać także z niestandardowych, nieustrukturalizowanych metod identyfikacji, gdyż zapewni to bardziej komplementarne podejście do problemu i zwiększy efektywność identyfikacji. Zgodnie z *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience* organizacja powinna m.in:

- regularnie, kompleksowo i z wielu perspektyw analizować środowisko, w jakim funkcjonuje, lub wykorzystywać odpowiednie metody czy techniki do identyfikacji pojawiających się zmian mogących powodować wystąpienie *emerging risks*,
- analizować trendy i okoliczności, które mogą doprowadzić do powstania nowych *emerging risks*,
- analizować źródła ryzyka i możliwe scenariusze zdarzeń,
- aktualizować w sposób ciągły opisy możliwych rodzajów ryzyka.

Przykładami zmian okoliczności, które mogą być źródłami *emerging risks*, są:

- zagrożenia naturalne, np. klimatyczne, pogodowe,
- zagrożenia związane z nowymi bakteriami, wirusami, grzybami i pasożytami czy z uodparnianiem się tych drobnoustrojów na dostępne leki,
- wyzwania związane z niekontrolowanym rozwojem internetu rzeczy (ang. *internet of things*, IoT),
- wyzwania związane z rozwojem sztucznej inteligencji.

Te ostatnie są coraz bardziej aktualnym problemem i – zdaniem autora niniejszego artykułu – niebawem staną się głównym generatorem *emerging risks*. Po raz pierwszy w historii ludzkości projektuje się urządzenia i systemy, których działanie nie do końca jest zrozumiałe. Nie wiadomo np., jak działa ChatGPT. Twórcy tego narzędzia rozumieją algorytmy uczenia maszynowego, ale nie został poznany dokładnie sposób, w jaki działają sieci neuronowe (a mają one bardzo szybkie tempo rozwoju). Nie wiadomo także, na ile sztuczna inteligencja stanie się samodzielna, a przekazanie możliwości decydowania maszynom, brak przejrzystości i zrozumienia funkcjonowania sztucznej inteligencji oraz brak nadzoru ze strony człowieka może skutkować wystąpieniem nieznanymi wcześniej rodzajów ryzyka.

¹³ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz. Urz. UE L 88/6 z 31 III 2017 r.).

Z *emerging risks* mogą się wiązać również zagrożenia terrorystyczne w szerokim rozumieniu – nie tylko takim, które wynika z przywołanych wcześniej definicji w *Słowniku terminów i definicji NATO* i dyrektywie Parlamentu Europejskiego z 2017 r. w sprawie zwalczania terroryzmu. Należy założyć, że nowa rzeczywistość modelowana przez *emerging risks* będzie miała wpływ na sposób przygotowywania i dokonywania przestępstw terrorystycznych.

Generalnie wyniki systematycznej oceny ryzyka dokonywanej przez podmioty krytyczne powinny zawierać:

- listę dostawców (zasobów, usług) o kluczowym znaczeniu dla podmiotu krytycznego,
- listę procesów, których zaburzenie może wywołać incydent istotny,
- wykaz IK niezbędnej do utrzymania usługi kluczowej.

Ocena ryzyka będzie stanowić punkt wyjścia do opracowania i wdrożenia adekwatnych rozwiązań organizacyjno-technicznych.

Standaryzacja i certyfikacja adekwatnych rozwiązań organizacyjno-technicznych wynikających z dyrektywy CER

Zarys systemu ochrony IK w świetle NPOIK 2023 i dyrektywy CER

W ramach NPOIK funkcjonuje tzw. sześciopak opisujący system ochrony IK. Działania podejmowane na rzecz zapewnienia bezpieczeństwa IK obejmują:

- 1) zapewnienie bezpieczeństwa fizycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które w sposób nieautoryzowany podjęły próbę dostania się lub znalazły się na terenie IK;
- 2) zapewnienie bezpieczeństwa technicznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych;
- 3) zapewnienie bezpieczeństwa osobowego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które mają uprawniony dostęp do infrastruktury krytycznej;
- 4) zapewnienie bezpieczeństwa teleinformatycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację

ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne;

- 5) zapewnienie bezpieczeństwa prawnego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie prawnych działań podmiotów zewnętrznych;
- 6) plany ciągłości działania i odtwarzania, rozumiane jako zespół działań organizacyjnych i technicznych prowadzących do utrzymania i odtworzenia funkcji realizowanych przez IK¹⁴.

Ten system koresponduje z art. 13 dyrektywy CER *Środki w zakresie odporności wprowadzane przez podmioty krytyczne*. Pierwszy akapit tego artykułu brzmi:

1. Państwa członkowskie zapewniają, aby podmioty krytyczne wprowadzały odpowiednie i proporcjonalne środki techniczne, środki bezpieczeństwa i środki organizacyjne służące zapewnieniu ich odporności, w oparciu o odpowiednie informacje dostarczone przez państwa członkowskie dotyczące oceny ryzyka państwa członkowskiego oraz wyników oceny ryzyka podmiotu krytycznego, w tym środki niezbędne w celu:
 - a) zapobiegania incydentom, z należyтым uwzględnieniem środków zmniejszania ryzyka związanego z katastrofami i przystosowania się do zmiany klimatu;
 - b) zapewnienia odpowiedniej fizycznej ochrony ich budynków i terenów oraz infrastruktury krytycznej, z należyтым uwzględnieniem na przykład zainstalowania ogrodzeń, budowy barier, narzędzi i procedur monitorowania terenu podlegającego ochronie, sprzętu do wykrywania i kontroli dostępu;
 - c) odpowiedzi na incydenty, stawiania im oporu i łagodzenia ich skutków, z należyтым uwzględnieniem wdrażania procedur i protokołów zarządzania ryzykiem i zarządzania kryzysowego, a także procedur ostrzegawczych;
 - d) odtworzenia po incydentach, z należyтым uwzględnieniem środków na rzecz ciągłości działania oraz identyfikacji alternatywnych łańcuchów dostaw w celu przywrócenia świadczenia usługi kluczowej;

¹⁴ Narodowy Program Ochrony Infrastruktury Krytycznej 2023...

- e) zapewnienia odpowiedniego zarządzania bezpieczeństwem pracowników, z należyтым uwzględnieniem środków takich jak ustanowienie kategorii personelu wykonującego funkcje krytyczne, ustanowienie praw dostępu do budynków i terenów, infrastruktury krytycznej i informacji szczególnie chronionych, ustanowienie procedur sprawdzenia przeszłości zgodnie z art. 14, wyznaczenie kategorii osób podlegających takim procedurom sprawdzenia przeszłości oraz określenie odpowiednich wymogów szkoleniowych i kwalifikacji;
- f) zwiększania świadomości odpowiedniego personelu na temat środków, o których mowa w lit. a)–e), z należyтым uwzględnieniem szkoleń, materiałów informacyjnych i ćwiczeń.

Do celów akapitu pierwszego lit. e) państwa członkowskie zapewniają, aby podmioty krytyczne uwzględniały personel zewnętrznych dostawców usług przy określaniu kategorii personelu, który wykonuje funkcje krytyczne.

Dyrektywa CER, co jest standardem w prawodawstwie europejskim, umożliwia państwom członkowskim indywidualne regulowanie przepisów prawa krajowego, implementującego jej zapisy w taki sposób, aby poziom odporności podmiotów krytycznych był jak najwyższy i kompatybilny ze specyfiką krajową, ale z uwzględnieniem wykorzystania norm, o czym jest mowa w art. 16 tej dyrektywy.

Norma to dokument normatywny przyjęty przez uznaną jednostkę normalizacyjną. W Polsce jest to Polski Komitet Normalizacyjny. Norma ustala zasady, wytyczne lub charakterystyki dotyczące różnych rodzajów działalności i jej wyników, jest zatwierdzana na zasadzie konsensusu, przeznaczona do powszechnego i wielokrotnego stosowania, zaakceptowana przez zainteresowane strony jako korzyść dla wszystkich oraz wprowadza kodeks dobrej praktyki i zasady racjonalnego postępowania przy aktualnym poziomie techniki¹⁵.

Zastosowanie norm w standaryzacji, a następnie certyfikacji rozwiązań organizacyjno-technicznych jest słusznym krokiem w budowaniu odporności IK na wszelkiego rodzaju zagrożenia. Ułatwia dobór rozwiązań, ich utrzymanie i walidację, a także pozwala na efektywny nadzór i egzekwowanie przepisów, gdyż organ krajowy nadzorujący IK – zgodnie z art. 21 dyrektywy CER – będzie dokonywał kontroli i podejmował decyzje

¹⁵ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej (Dz. Urz. UE L 316/12 z 14 XI 2012 r.).

na podstawie danych zbieranych przez zewnętrzne, kompetentne podmioty zajmujące się audytowaniem i certyfikacją.

Zakres rozwiązań organizacyjno-technicznych, które powinny zostać zastosowane w podmiocie krytycznym po przeprowadzeniu oceny ryzyka, jest bardzo szeroki. Aby syntetycznie przedstawić zagadnienie standaryzacji i certyfikacji, autor artykułu odwołał się do technicznych środków zapewnienia bezpieczeństwa fizycznego, stanowiących dobry punkt odniesienia w tym temacie, jak również do zapewniania ciągłości działania usług kluczowych.

Standaryzacja i audytowanie – kontekst normalizacji

Zgodnie z koncepcją przedstawioną przez autora artykułu 5 października 2023 r. na Krajowym Forum Ochrony Infrastruktury Krytycznej¹⁶ rozwiązania organizacyjno-techniczne wdrażane przez podmioty krytyczne powinny być tworzone zgodnie z normami, co umożliwi – z uwagi na dostępność rozwiązań prawnych i biznesowych – skuteczne prowadzenie audytów i certyfikacji. Audyt to (...) *systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu obiektywnego oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu*¹⁷. Audyt ocenia zgodność teraz i w przeszłości, może mieć cel prawno-normatywny i powinien realizować potrzeby biznesowe. Opiera się na siedmiu zasadach:

- 1) rzetelności, jako podstawie profesjonalizmu,
- 2) uczciwości przedstawiania wyników,
- 3) należytej staranności zawodowej,
- 4) poufności,
- 5) niezależności,
- 6) podejściu opartym na dowodach,
- 7) podejściu opartym na ryzyku.

Istnieją trzy rodzaje audytów (tabela 1).

¹⁶ A. Tatarowski, *Standaryzacja i certyfikacja rozwiązań wynikających z Dyrektywy CER*, X Krajowe Forum Ochrony Infrastruktury Krytycznej, Warszawa 2023, <https://www.gov.pl/web/rcb/x-krajowe-forum-ochrony-infrastruktury-krytycznej-za-nami>.

¹⁷ PN-EN ISO 19011:2018 *Wytyczne dotyczące audytowania systemów zarządzania*.

Tabela 1. Rodzaje audytów według normy PN-EN ISO 19011:2018.

Audit strony pierwszej	Audit strony drugiej	Audit strony trzeciej
Audit wewnętrzny	Audit zewnętrznego dostawcy	Audit dla celów certyfikacji i/lub akredytacji
	Audit innej zewnętrznej strony zainteresowanej	Audit dla celów prawnych, regulacyjnych i podobnych

Źródło: *PN-EN ISO 19011:2018 Wtyczne dotyczące audytowania systemów zarządzania.*

Z perspektywy podmiotów krytycznych najbardziej istotny jest audyt strony trzeciej, który przeprowadzają niezależne organizacje audytujące, takie jak jednostki certyfikujące lub instytucje rządowe. Instytucja rządowa nadzorująca podmioty krytyczne w Polsce (w warunkach prawnych, które nastąpią po implementacji dyrektywy CER) będzie gromadziła dane i podejmowała decyzje na podstawie (...) *dowodów potwierdzających skuteczne wdrożenie tych środków* [tzn. środków z art. 13, omawianych jako rozwiązania organizacyjno-techniczne], *w tym wyników audytu przeprowadzonego na koszt tego podmiotu przez wybranego przez niego niezależnego i wykwalifikowanego audytora*. Dowody w audycie strony trzeciej należy rozumieć jako certyfikaty, czyli dokumenty wydane przez jednostkę oceniającą zgodność (jednostkę certyfikującą), potwierdzające, że wyrób/installacja/system/proces/usługa są zgodne z wymaganiami. W przypadku implementacji dyrektywy CER – zgodne z wymaganiami zawartymi w odpowiednich normach.

Na marginesie warto wyjaśnić jeden z aspektów, z którego niezrozumieniem autor artykułu spotyka się w swojej działalności zawodowej jako kierujący jednostką certyfikującą. Ocena zgodności zawsze odnosi się do jakiegoś dokumentu, w tym przypadku – normy. Powoływanie się na normy w przepisach prawa, chociaż są to dokumenty do tzw. stosowania dobrowolnego, jest możliwe, co potwierdzają stanowisko prezesa Polskiego Komitetu Normalizacyjnego¹⁸ oraz wyroki sądów¹⁹. Jeśli więc norma jest przywołana w postanowieniach jakiejś ustawy, to powoływanie się na nią (np. w przypadku audytu czy certyfikacji) jest możliwe i zasadne. Taka

¹⁸ *Dobrowolność stosowania norm*, Polski Komitet Normalizacyjny, <https://wiedza.pkn.pl/web/wiedza-normalizacyjna/stanowisko-pkn-w-sprawie-dobrowolnosci-pn> [dostęp: 29 XI 2023].

¹⁹ Wyrok Naczelnego Sądu Administracyjnego z 10 IV 2019 r., sygn. akt II OSK 1486/17; wyrok Wojewódzkiego Sądu Administracyjnego w Kielcach z 19 V 2009 r., sygn. akt II SA/Ke 183/09.

praktyka istnieje w polskim prawodawstwie, np. w ustawie o krajowym systemie cyberbezpieczeństwa. Przywołanie norm w przepisach prawa nie ułatwia jednak wglądu w nie. Dostęp do tych norm jest odpłatny.

Ocena zgodności. Uprawnienia jednostek certyfikujących i audytorów do prowadzenia certyfikacji. Certyfikat a deklaracja zgodności

Audyt strony trzeciej może być prowadzony przez jednostkę oceniającą zgodność (jednostkę certyfikującą), akredytowaną na podstawie przepisów ustawy o systemach oceny zgodności i nadzoru rynku²⁰ – i takie rozwiązanie funkcjonuje już w odniesieniu do audytowania bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej²¹ – lub przez jednostkę certyfikującą upoważnioną do certyfikacji w imieniu i na rzecz Polskiego Komitetu Normalizacyjnego w rozumieniu przepisów ustawy o normalizacji²². Certyfikację należy rozumieć jako działanie jednostki oceniającej zgodność (jednostki certyfikującej), wykazujące, że wyrób/instalacja/system/proces/usługa są zgodne z wymaganiami. Umożliwienie jednostek certyfikujących jest bardzo silne. Funkcjonują one jako składowe ogólnego, europejskiego systemu obejmującego ocenę zgodności i nadzór rynku²³. Ich wykorzystanie w procesie audytowania i certyfikacji rozwiązań organizacyjno-technicznych wdrażanych przez podmioty krytyczne stanie się niezbędne.

Warto zwrócić uwagę, że termin „certyfikat” często jest używany w sposób nieuprawniony (z perspektywy systemu oceny zgodności). Według definicji słownikowej certyfikat to ‘oficjalny dokument stwierdzający np. zgodność produktu z normami, autentyczność dzieła sztuki lub ukończenie kursu’²⁴. Stanowisko odnośnie do pojęcia certyfikatu zajęła

²⁰ Ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. DzU z 2022 r. poz. 1854).

²¹ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2023 r. poz. 913, ze zm.).

²² Ustawa z dnia 12 września 2002 r. o normalizacji (t.j. DzU z 2015 r. poz. 1483).

²³ Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218/30 z 13 VIII 2008 r.).

²⁴ Słownik języka polskiego PWN, <https://sjp.pwn.pl/sjp/certyfikat;2553201.html> [dostęp: 29 XI 2023].

także Rada Języka Polskiego przy Prezydium Polskiej Akademii Nauk²⁵. W kontekście systemu oceny zgodności – tej zgodności, która będzie miała decydujące znaczenie w przypadku IK – certyfikat to zatem, jak już wspomniano, dokument wydany przez jednostkę oceniającą zgodność (jednostkę certyfikującą), potwierdzający, że wyrób/installacja/system/proces/usługa są zgodne z wymaganiami. Jest to definicja autorska, gdyż to pojęcie w odniesieniu do oceny zgodności z normami niezharmonizowanymi nigdy nie zostało zdefiniowane. Brakuje tej definicji w przepisach dotyczących normalizacji zarówno w przedmiotowej ustawie, jak i w rozporządzeniu Rady Ministrów w sprawie sposobu nadawania i wykorzystywania znaku zgodności z Polską Normą²⁶, które to rozporządzenie wskazuje nawet wzór certyfikatu. Co więcej, brakuje definicji certyfikatu (w ujęciu wskazanym przez autora artykułu) w ustawie o systemach oceny zgodności i nadzoru rynku. Znajduje się tam jedynie definicja certyfikatu jako dokumentu potwierdzającego zgodność, wydawanego przez jednostkę notyfikowaną, tj. taką, która jest zgłoszona do Komisji Europejskiej i umieszczona w wykazie jednostek notyfikowanych do konkretnych dyrektyw, a więc prowadzącą obligatoryjną ocenę zgodności. Z uwagi na potrzeby wynikające z dyrektywy CER należy spodziewać się doprecyzowania pojęcia certyfikatu w przepisach krajowych.

Deklaracja zgodności została zdefiniowana w ustawie o systemach oceny zgodności i nadzoru rynku. Należy tę deklarację rozumieć jako oświadczenie producenta, instalatora lub ich upoważnionego przedstawiciela albo prywatnego importera (na ich wyłączną odpowiedzialność), że wyrób jest zgodny z wymaganiami.

Jakie podejście do rangi takiej deklaracji można było obserwować w praktyce? Dobrym, modelowym wręcz przykładem branży, w której przez lata działało kilkusobowe, ale mające siłę przebicia lobby, propagujące tezę, że deklaracja zgodności jest wystarczająca i gwarantuje zgodność z wymaganiami oraz odpowiednią jakość, jest branża technicznych środków zapewnienia bezpieczeństwa fizycznego. Obecnie takie głosy prawie zanikły – z uwagi na zupełnie inną świadomość uczestników rynku i przedstawicieli administracji państwowe. Zmiany nastąpiły pod wpływem negatywnych doświadczeń. Poniżej kilka przykładów ilustrujących, w jaki

²⁵ *Stanowisko Rady wobec użycia słowa certyfikat*, <https://rjp.pan.pl/dokumenty-rady?view=article&id=98:stanowisko-rady-wobec-ucyia-sowa-certyfikat&catid=45> [dostęp: 29 XI 2023].

²⁶ *Rozporządzenie Rady Ministrów z dnia 11 października 2010 r. w sprawie sposobu nadawania i wykorzystywania znaku zgodności z Polską Normą* (DzU z 2010 r. nr 198 poz. 1316).

sposób funkcjonował – i w pewnych obszarach nadal funkcjonuje – rynek. Dnia 7 września 2010 r. zostało opublikowane rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne²⁷. W § 12 tego rozporządzenia znalazł się punkt mówiący o tym, że do przechowywania lub transportowania wartości pieniężnych wykorzystuje się urządzenia (...) posiadające wydany przez uprawnioną jednostkę certyfikującą certyfikat zgodności albo wydaną przez producenta lub importera deklarację zgodności, potwierdzające zgodność z zasadniczymi lub szczegółowymi wymaganiami w rozumieniu przepisów o systemie oceny zgodności – w przypadku gdy dla danego wyrobu wymagania takie zostały ustalone. Zapisy te są nadal aktualne. Intuicyjnie wiadomo, że jeśli dostawca urządzeń ma możliwość wprowadzenia na rynek urządzenia mającego deklarację zgodności, którą sam wystawia, a która najczęściej nie ma żadnego pokrycia w stanie faktycznym, to nie będzie przeprowadzał badań w akredytowanym laboratorium i starał się o uzyskanie certyfikatu. Inwestor nie ma w tym przypadku możliwości działania. Nowszym przykładem jest ustawa z 2012 r. o odpadach²⁸. Posiadacz odpadów jest obowiązany do prowadzenia wizyjnego systemu kontroli miejsca magazynowania lub składowania odpadów. Akt wykonawczy do tej ustawy²⁹ doprecyzowuje, że: *Parametry urządzeń technicznych systemu kontroli spełniają co najmniej wymagania normy PN-EN 62676-4: 2015-06 Systemy dozoru wizyjnego stosowane w zabezpieczeniach – Część 4: Wytyczne stosowania lub normy, którą przedmiotowa norma zostanie zastąpiona*. Niestety, większość posiadaczy odpadów (a może nawet żaden) nie ma wdrożonego takiego systemu. Dlaczego tak się dzieje? Pomijając nie najlepszy sposób sformułowania tego zapisu, to brakuje w nim wskazania sposobu potwierdzania zgodności, że zainstalowany system telewizji dozorowej spełnia wymagania. Projektant nie ponosi zatem ryzyka, jeśli zaprojektuje taki system, nie znając nawet przywołanej normy (zjawisko niskiego poziomu kompetencji jest w tej branży powszechne, ale istnieją rozwiązania

²⁷ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 września 2010 r. w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne (t.j. DzU z 2016 r. poz. 793).

²⁸ Ustawa z dnia 14 grudnia 2012 r. o odpadach (t.j. DzU z 2023 r. poz. 1587, ze zm.).

²⁹ Rozporządzenie Ministra Środowiska z dnia 29 sierpnia 2019 r. w sprawie wizyjnego systemu kontroli miejsca magazynowania lub składowania odpadów (DzU z 2019 r. poz. 1755).

prawno-normatywne, które zaczynają już funkcjonować, co zostanie opisane w dalszej części artykułu), podobnie jak instalator, który zainstaluje taki system i wystawi deklarację jego zgodności z normą. Takie systemy jeśli w ogóle działają, często nie spełniają potrzeb inwestora i wymagań norm, i są, co oczywiste, zawodne. Tak funkcjonuje duży obszar rynku.

W przypadku IK, która zgodnie z dyrektywą CER musi wypracować odporność na zagrożenia asymetryczne, akty terrorystyczne i inne zagrożenia, takie podejście jest niedopuszczalne. System zabezpieczeń technicznych (system sygnalizacji włamania i napadu, system dozoru wizyjnego, system kontroli dostępu) powinien po zainstalowaniu uzyskać certyfikat. Usługi realizowane przez podmioty zewnętrzne (tj. projektowanie, instalowanie, konserwacja) na rzecz IK powinny spełniać najwyższe standardy jakości. Te podmioty powinny posiadać certyfikat zgodności z normą *PN-EN 16763:2017 Usługi w zakresie systemów ochrony przeciwpożarowej oraz systemów zabezpieczeń technicznych*, co wypełnia wymogi art. 13 akapit 1 lit. e dyrektywy CER. Dyrektywa ta wychodzi naprzeciw konieczności uporządkowania wymagań wobec usługodawców (w tym w obszarze ochrony przeciwpożarowej), o czym autor artykułu niejednokrotnie mówił na różnych wydarzeniach branżowych i konferencjach³⁰. Wspomniana norma została już przywołana jako właściwa przy ocenie kompetencji i kwalifikacji podmiotów działających w tej branży w Załączniku 1 *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje* do NPOIK 2023.

Wdrożenie, utrzymanie i certyfikacja systemu zarządzania ciągłością działania usług kluczowych

Podmiot krytyczny, który dokonał oceny ryzyka i wdraża (lub wdrożył) adekwatne środki organizacyjno-techniczne, powinien zaimplementować system zarządzania ciągłością usługi kluczowej zgodny z normą *PN-EN ISO*

³⁰ A. Tatarowski, *Nowe sposoby walidacji jakości usług projektantów, instalatorów i konserwatorów systemów ochrony przeciwpożarowej i systemów zabezpieczeń technicznych w procesie budowlanym*, IV Międzynarodowa Konferencja N-T „Problemy Inżynierii Bezpieczeństwa Obiektów Antropogenicznych”, Warszawa 2021, <https://psribs.pl/conferences/iv-miedzynarodowa-konferencja-n-t-problemy-inzynierii-bezpieczenstwa-objektow-antropogenicznych-wiosna-2021/> [dostęp: 29 XI 2023]; A. Tatarowski, *Nowe sposoby walidacji jakości usług projektantów, instalatorów i konserwatorów systemów ochrony przeciwpożarowej*, XXIX Ogólnopolskie Warsztaty – Sygnalizacja i Automatyka Pożarowa SAP '2023, Żnin 2023, <https://www.polon-alfa.pl/pl/aktualnosci/polon-alfa-w-cukrowni-%C5%BCnin> [dostęp: 29 XI 2023].

22301:2019 *Bezpieczeństwo i odporność. Systemy zarządzania ciągłością działania. Wymagania*. System zarządzania ciągłością działania oparty na wspomnianej normie składa się z następujących elementów:

- a) polityki,
- b) kompetentnych osób z określonymi odpowiedzialnościami,
- c) procesów zarządzania dotyczących:
 - polityki,
 - planowania,
 - wdrażania i działań operacyjnych,
 - oceny efektów działania,
 - przeglądu zarządzania,
 - ciągłego doskonalenia,
- d) udokumentowanych informacji wspomagających nadzór działań operacyjnych i umożliwiających ocenę efektów działania.

Usług kluczowych zwykle nie realizuje jeden operator. Najczęściej jest to zbiór kilku usług, które funkcjonują niezależnie od siebie i są dostarczane przez różne podmioty. Dobrym przykładem usługi kluczowej – jak wskazują autorzy publikacji *Zarządzanie bezpieczeństwem i ciągłością usług kluczowych państwa* – jest wypłacanie pieniędzy z bankomatu. Aby można było wypłacić gotówkę, muszą być dostępne usługi składowe w postaci:

- dostępności zasilania energetycznego bankomatu,
- dostępności sieci Internet zapewniającej łączność z systemem rozliczeniowym,
- dostępności systemu rozliczeniowego banku, z którego są wypłacane pieniądze,
- zapewniania gotówki w bankomacie, za co obecnie odpowiadają głównie operatorzy sieci bankomatowych.

Zatem (...) *możliwość wypłaty pieniędzy z bankomatu jest więc w rzeczywistości zbiorem relacji, jakie występują między wymienionymi usługami składowymi i może zaistnieć wyłącznie w wyniku równoczesnej dostępności wszystkich usług składowych. W konsekwencji wystarczy niedostępność jednej ze składowych usług kluczowej, aby ona sama również nie była dostępna*³¹.

Mając na uwadze złożoność usług kluczowych, pomocne może okazać się stosowanie IM-BIK uzupełnionego o normy. W literaturze przedmiotu opisano kilka sposobów na zapewnienie nieprzerwanej dostępności. Jest to np.:

³¹ M. Kisilowski i in., *Zarządzanie bezpieczeństwem...*, s. 106.

- nadmiar strukturalny, który polega na dublowaniu elementów uznanych za krytyczne,
- nadmiar funkcjonalny, który polega na przystosowywaniu wytypowanych elementów systemu do pełnienia dodatkowych funkcji,
- nadmiar parametryczny, który polega na standardowym zasilaniu systemu w stopniu przewyższającym zapewnianie jego użyteczności³².

Warto zwrócić uwagę na sposób nazwany nadmiarem funkcjonalnym.

Wykorzystując IM-BIK:

(...) instytucja rządowa, np. RCB, może, posługując się wykazem usług kluczowych, zidentyfikować podmioty, które dostarczają usługi składowe dla usług kluczowych. Usługi składowe można wówczas potraktować jako funkcjonalności rozpatrywanych obiektów IK. W przypadku wystąpienia incydentu ograniczającego lub eliminującego dostępność funkcjonalności IK możliwe jest zidentyfikowanie obiektów IK o podobnych funkcjonalnościach i w ramach PCD (tzn. Planu Ciągłości Działania) uzupełnienie brakującej składowej usługi kluczowej funkcjonalnością realizowaną przez inny obiekt IK³³.

Zagadnienie opracowania, wdrożenia i certyfikacji systemu zarządzania ciągłością działania jest obszerne i ma unikalny charakter w odniesieniu do każdego podmiotu krytycznego. Przytoczone fragmenty zaczerpnięte z literatury przedmiotu mają za zadanie – w intencji autora artykułu – zachęcić czytelników do poszerzenia wiedzy w tym zakresie, gdyż zagadnienie to stanowi najbardziej istotną część w całościowym spojrzeniu na system zarządzania bezpieczeństwem IK.

Podsumowując, z perspektywy podmiotu krytycznego istotnym działaniem będzie nieustanne doskonalenie systemu ciągłości działania poprzez wykorzystanie pomiarów skuteczności, w tym symulacji, monitorowania, systematycznego przeglądu, oceny incydentów i skutecznego ich usuwania

³² K. Szwarz, *Modelowanie ciągłości działania systemów zarządzania kryzysowego i ocena przydatności rozwiązań na szczeblu lokalnym*, rozprawa doktorska, Warszawa 2019, <https://repo.bg.wat.edu.pl/info/phd/WATefc9a9340f3e47cb8141566cdf6e0e53/Record+detail-s+%25E2%2580%2593+Modeling+of+the+continuity+of+crisis+management+systems+and+the+assessment+of+suitability+at+the+local+level+%25E2%2580%2593+Military+Technical+Academy+them.+Jaroslaw+Dabrowski+title?aq=%40status%3Apracownik%2Cauthorprofile%2F%40positionPL%21%3Aadiunkt%2Cauthorprofile%2F%40positionPL%21%3Aprofesor%2C%40active%3D%27true%27%2C.%3AWUT84b1c97cce-2d442fab1acdc256a5d487&r=author&ps=20&lang=en&pn=1&cid=157628>.

³³ M. Kisilowski i in., *Zarządzanie bezpieczeństwem...*, s. 108.

zgodnie z polityką bezpieczeństwa. Jednym z narzędzi pomiaru będzie prowadzenie systematycznych i niezależnych audytów, w tym zakończonych certyfikacją, ale w zakresie niezbędnym do utrzymania świadczenia usługi kluczowej.

Podsumowanie

Rok 2024 będzie dla IK przełomowy. Naglące terminy, zobowiązujące kraje członkowskie do uchwalenia krajowych przepisów implementujących dyrektywę CER, wymagają przygotowania odpowiedniego środowiska do efektywnej pracy legislacyjnej. Rządowe Centrum Bezpieczeństwa, które od wielu lat stwarza warunki sprzyjające poprawie bezpieczeństwa IK i zbudowało unikalne w UE podejście do zarządzania bezpieczeństwem w tym sektorze, oparte na wspomnianym tzw. sześciopaku, stoi obecnie przed dużym wyzwaniem dotyczącym opracowania implementacji dyrektywy CER w Polsce. W niniejszym artykule zostały przedstawione tendencje legislacyjne związane z tą implementacją w aspekcie standaryzacji i certyfikacji rozwiązań organizacyjno-technicznych. Standaryzacja i certyfikacja tych rozwiązań oparta na normach pozwoli na zastąpienie bezpośredniej kontroli ze strony administracji państwowej, umożliwi szybsze, bardziej efektywne i optymalne dostosowanie odporności podmiotów krytycznych na zagrożenia asymetryczne, terrorystyczne i te wynikające z *emerging risks* lub wiążące się z nimi.

W 2024 r. należy spodziewać się intensyfikacji działań hybrydowych mających źródło na wschodzie, ale też w innych regionach świata. To sprawia, że coraz pilniejsza jest potrzeba uporządkowania legislacyjnego nie tylko w odniesieniu do IK, lecz także w szerszym obszarze prawnym, obejmującym: *Ustawę z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, Ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Ustawę z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych oraz Ustawę z dnia 11 marca 2022 r. o obronie Ojczyzny.*

Adam Tatarowski

Dyrektor Zakładu Rozwoju Technicznej Ochrony Mienia „TECHOM” Sp. z o.o. – wyspecjalizowanej jednostki certyfikującej

oraz placówki kształcenia ustawicznego. W jej ramach kształcą się m.in. osoby funkcyjne zajmujące się ochroną osób i obiektów w służbach mundurowych, pracownicy IK odpowiedzialni za bezpieczeństwo oraz usługodawcy realizujący projekty, instalacje i konserwacje systemów ochrony przeciwpożarowej i technicznych środków zapewnienia bezpieczeństwa fizycznego. Autor jest specjalistą w zakresie oceny zgodności technicznych środków zapewnienia bezpieczeństwa fizycznego (i usług w tym obszarze), ekspertem Komitetów Technicznych nr 52, 264, 306 i 323 w Polskim Komitecie Normalizacyjnym.

Kontakt: tatarowski@techom.com

Projekt APPRAISE

Budowanie systemu bezpieczeństwa przestrzeni publicznych

Jarosław Przyjemczak

Wydział Prawa i Administracji,
Wyższa Szkoła Administracji i Biznesu w Gdyni

 <https://orcid.org/0000-0003-3923-8078>

Nina Czyżewska

Polska Platforma Bezpieczeństwa Wewnętrznego

 <https://orcid.org/0009-0004-0483-7577>

Ogólnodostępna przestrzeń publiczna, obejmująca różne obszary i obiekty, pozostaje, zwłaszcza w przypadku dużych aglomeracji miejskich, w miarę swobodnym miejscem na działania przestępców, w tym tych, którzy planują zamachy terrorystyczne. Ich aktywności sprzyja wiele czynników, m.in. duża dostępność tego typu przestrzeni, mnogość i różnorodność przebywających w niej osób, zmienność okoliczności oraz przypadkowość zdarzeń i sytuacji, które mogą w niej zaistnieć.

Prace nad stworzeniem odpowiedniego systemu nadzoru nad obszarami i obiektami w przestrzeni publicznej trwają od wielu lat. Zakłada się, że taki system nie powinien być łatwo zauważalny i powodować utrudnień w funkcjonowaniu osób znajdujących się na danym terenie. Pomimo wielu wysiłków nie udało się stworzyć instrumentu doskonałego, który z jednej strony umożliwi skuteczne zapobieganie działaniom przestępców, a z drugiej będzie obojętny dla innych uczestników. Zdarzenia z przeszłości, takie

jak ataki na centra handlowe (np. Monachium, 2016 r.), lotniska (np. Bruksela, 2016 r.), system transportu publicznego (np. Madryt, 2004 r.; Londyn, 2005 r.; Bruksela, 2016 r.), place miejskie i ulice (np. Paryż, 2015 r.; Berlin, 2016 r.; Nicea, 2016 r.; Sztokholm, 2017 r.) oraz hale widowiskowe (np. Paryż, 2015 r.; Manchester 2017 r.), uwidoczniły podatność celów miękkich na ataki, a także uświadomiły podmiotom dbającym o bezpieczeństwo, jakie wysiłki należy podjąć w celu ochrony tego typu obiektów¹.

Jednym z działań mających na celu szybkie rozpoznanie i wdrożenie odpowiednich środków zaradczych uniemożliwiających dokonanie ataku lub jego powstrzymanie i rozprzestrzenianie się jest projekt Komisji Europejskiej APPRAISE dotyczący perspektywy H2020 SU-FCT03-2018-2019-2020: Zarządzanie przepływem informacji i danych w celu zwalczania cyberprzestępczości i terroryzmu. Jego podstawowe założenie to zapewnienie bezpieczeństwa w przestrzeni publicznej bez konieczności ograniczenia wolności obywateli poprzez zmniejszenie lub całkowite wyeliminowanie zagrożenia atakami. Dzięki projektowi APPRAISE mają zostać wdrożone zupełnie nowe rozwiązania służące skuteczniejszemu przewidywaniu i identyfikowaniu aktów przestępczych i terrorystycznych oraz wzmocnieniu współpracy operacyjnej podmiotów odpowiedzialnych za bezpieczeństwo – przed dokonaniem ataku, w trakcie jego trwania i po jego wystąpieniu². Bazując na osiągnięciach współczesnych technologii, które umożliwiają coraz szersze zastosowanie takich narzędzi, jak sztuczna inteligencja, zaawansowana wizualizacja czy szybkość przekazu informacji, można znacznie podnieść poziom bezpieczeństwa, również w ogólnodostępnych przestrzeniach publicznych. Odpowiednio szybkie wykrycie zagrożeń oraz przekazanie w czasie rzeczywistym informacji o nietypowych czy niebezpiecznych sytuacjach jest niezmiernie istotne z punktu widzenia działań służb mundurowych czy interwencyjnych, gdyż czas jest główną determinantą właściwego poradzenia sobie z zagrożeniami. Projekt APPRAISE, będący częścią budowania wspólnego systemu przeciwwążeńiowego państw Unii Europejskiej, w którego skład wchodzi pokrewne

¹ N. Czyżewska, J. Przyjemczak, *Wsparcie technologiczne nowoczesnych systemów bezpieczeństwa – projekt Komisji Europejskiej APPRAISE*, w: W. Zubrzycki, J. Przyjemczak, *Bezpieczeństwo w praktyce. Zagrożenia, podmioty bezpieczeństwa, działania pomocowe i ratownicze*, Kraków 2023 (w druku).

² APPRAISE – *wspomaganie prywatnych i publicznych instytucji odpowiedzialnych za bezpieczeństwo w zwalczaniu terroryzmu wymierzonego w cele miękkie*, <https://ppbw.pl/pl/projekt-appraise/> [dostęp: 10 XI 2023].

projekty, takie jak: Safe-Cities³, Lago⁴, S4AllCities⁵, Starlight⁶, Aida⁷, dostarcza nowych rozwiązań w sferze bezpieczeństwa. Celem wszystkich wymienionych przedsięwzięć jest osiągnięcie zdolności do przewidywania zagrożeń i radzenia sobie w przypadku ich zaistnienia, jak również systemowe wdrażanie jednolitych procedur i standardów w działaniu podmiotów publicznych i niepublicznych w momencie wystąpienia zdarzeń o charakterze terrorystycznym.

W trakcie trwania projektu APPRAISE podjęto wiele inicjatyw mających na celu dostosowanie już istniejących bądź stworzenie nowych technologii, jak również przetestowano w niemal rzeczywistych warunkach uzyskane wyniki prac. W ramach testów przeprowadzono (w Lublanie, Bilbao, Gdańsku oraz Turynie) wizyty studyjne oraz tzw. pilotaże, aby sprawdzić prawidłowość działania poszczególnych systemów i technologii oraz na bieżąco je udoskonalać. Zakończenie tego projektu nie oznacza finału prac nad opracowanymi rozwiązaniami. Wręcz przeciwnie – to dopiero początek budowania jednolitego, zwartego systemu ostrzegawczo-analitycznego, którego zadaniem jest dozorowanie przestrzeni publicznych i alarmowanie właściwych służb interwencyjnych w razie pojawienia się zagrożenia czy też wykrycia anomalii w zachowaniu się ludzi. Celem nadrzędnym jest osiągnięcie jak najwyższego stopnia budowania świadomości sytuacyjnej w procesie zarządzania kryzysowego.

Atak na park wodny Atlantis – pilotaż 3

Po raz pierwszy zespoły pracujące przy tworzeniu odpowiednich narzędzi i technologii w ramach projektu APPRAISE spotkały się na potrzeby przeprowadzenia pilotaży 11 maja 2023 r. w Słowenii. W parku wodnym Atlantis znajdującym się na terenie kompleksu handlowego BTC City Ljubljana

³ *Project in a Nutshell*, <https://safe-cities.eu/> [dostęp: 10 XI 2023].

⁴ *LAGO: Lessen Data Access and Governance Obstacles*, <https://lago-europe.eu/> [dostęp: 10 XI 2023].

⁵ *Smart Spaces Safety and Security for All Cities*, <https://www.s4allcities.eu/> [dostęp: 10 XI 2023].

⁶ *STARLIGHT. Enhancing the EU's strategic autonomy in the field of artificial intelligence (AI) for law enforcement agencies (LEAs)*, <https://www.starlight-h2020.eu/> [dostęp: 10 XI 2023].

⁷ *AIDA project. Research project to develop a Big Data Analysis and Analytics framework*, <https://www.project-aida.eu/> [dostęp: 10 XI 2023].

odbył się pilotaż 3. Połączono go z corocznymi ćwiczeniami słoweńskiej policji, w których uczestniczyli lokalni partnerzy, wraz z krajowym zespołem SWAT, interesariuszami i partnerami APPRAISE. Funkcję lidera pełnił Instytut za korporativne varnostne študije (Instytut Studiów nad Bezpieczeństwem Korporacyjnym), który przygotował to przedsięwzięcie we współpracy ze słoweńskim Ministerstwem Spraw Wewnętrznych oraz kompleksem handlowym BTC City i jego agencją ochrony⁸. Początkowy etap scenariusza pilotażu obejmował analizę treści zamieszczanych w mediach społecznościowych oraz Darknetcie. Na tej podstawie zostały wykryte posty z groźbami kierowanymi do zarządców kompleksu Atlantis. Programy komputerowe APPRAISE pomogły również w wykryciu próby ataku cybernetycznego na systemy bezpieczeństwa parku wodnego, aby zwiększyć ilość chloru w wodzie, a także ataku na system monitoringu obiektu, aby zakłócić przesyłanie jego nagrań. Scenariusz obejmował ponadto atak z użyciem broni palnej na osoby przebywające w parku wodnym. W pierwszej fazie ataku sprawca oddał kilkanaście strzałów na terenie basenu zewnętrznego. Spowodowało to uruchomienie technologii APPRAISE, dzięki której rozpoznano podejrzane dźwięki i zlokalizowano miejsce ataku. Analiza monitoringu wykryła panikę, która wybuchła wśród osób znajdujących się w okolicy basenu, oraz osoby ranne leżące na ziemi. W następnej fazie scenariusza strzelec przemieścił się do wnętrza kompleksu basenowego, gdzie oddał kolejne strzały. Ponownie zastosowane technologie do rozpoznawania dźwięku, identyfikacji przedmiotów z nagrań audiowizualnych (w tym wypadku pistoletu) oraz analizy zachowań zgromadzonych ludzi zadziałały poprawnie i zaalarmowały o zagrożeniu. Przyjęty scenariusz obejmował również wzięcie zakładnika, z którym sprawca zamknął się w piwnicy, a także policyjne negocjacje i neutralizację terrorysty⁹. Relacja z tego ćwiczenia jest dostępna w serwisie YouTube¹⁰.

W realizację pilotażu było zaangażowanych wiele publicznych i prywatnych podmiotów bezpieczeństwa oraz wolontariusze. Narzędzia powstałe na potrzeby APPRAISE zaprezentowano 20 słoweńskim i zagranicznym interesariuszom, m.in. przedstawicielom policji, poczty i firmy Plus Orbita, zajmującej się systemami i usługami z zakresu bezpieczeństwa. Ćwiczenie

⁸ *Pilot 3: Ljubljana*, <https://appraise-h2020.eu/node/103> [dostęp: 29 XI 2023].

⁹ N. Czyżewska, J. Przyjemczak, *Wsparcie technologiczne nowoczesnych systemów bezpieczeństwa...*

¹⁰ *APPRAISE First Pilot: BTC City – Ljubljana*, YouTube, 12 IX 2023 r., <https://www.youtube.com/watch?v=zWAJj2qHVbs>.

potwierdziło przydatność rozwiązań systemowych i technologicznych zastosowanych w narzędziach opracowanych na potrzeby projektu APPRAISE i stanowiło dobrą podstawę do ich dalszego rozwoju i testowania podczas kolejnych pilotaży. Zaangażowanie w to przedsięwzięcie słoweńskiej policji umożliwiło przetestowanie jej sprzętu, organizacji, taktyki i skuteczności w radzeniu sobie z takimi lub podobnymi zdarzeniami związanymi z bezpieczeństwem. Dodatkowo dzięki narzędziom APPRAISE sprawdzono współpracę pomiędzy publicznymi i prywatnymi podmiotami bezpieczeństwa oraz oceniono nowe możliwości wymiany informacji pomiędzy nimi.

Międzynarodowy wyścig kolarski Itzulia Basque Country – pilotaż 1

Kolejna wizyta studyjna odbyła się 20 lipca 2023 r. w Iurrecie w Hiszpanii, w ośrodku szkoleniowym baskijskiej policji. Scenariusz tego wydarzenia bazował na wyścigu kolarskim, który został zainscenizowany na terenie wspomnianego ośrodka (względy organizacyjne nie pozwoliły na udział technologii APPRAISE w realnym wydarzeniu). Założenia obejmowały przeprowadzenie wyścigu kolarskiego Itzulia Basque Country rozpoczynającego się w San Sebastian w Hiszpanii, a kończącego się w Bayonne we Francji. Pilotaż został zorganizowany przez Ertzaintze – autonomiczną policję Kraju Basków, firmę Oceta – organizatora wyścigu, firmę ochroniarską Alse oraz RAID – oddział specjalny francuskiej Policji Krajowej. Scenariusz zakładał skoordynowany atak przeprowadzony po obu stronach granicy oraz współpracę hiszpańskich i francuskich służb. W pierwszej fazie planowanych działań, jeszcze przed rozpoczęciem wyścigu, narzędzia APPRAISE do analizy treści internetowych wykryły posty z groźbami wymierzonymi w jednego ze sponsorów wyścigu. W kolejnej fazie ćwiczeń, w dniu wydarzenia, został zidentyfikowany post, który zawierał bezpośrednie groźby ataku na organizatora wydarzenia. W tym czasie w miejscach startu i mety zgromadziła się publiczność. Zgodnie z przyjętymi założeniami znaczna część tych terenów była strefą o ograniczonym dostępie, obejmującym zakaz ruchu pojazdów i pozwalającym na wejście jedynie pieszym oraz upoważnionym pracownikom. Scenariusz przewidywał zaistnienie na starcie wyścigu gwałtownego protestu podjętego w celu zablokowania rozpoczęcia zawodów. W trakcie tych zajęć osoba z podejrzanym pakunkiem (plecakiem) przedostała się do strefy ograniczonego ruchu. Gdy to przewinienie zostało wykryte przez narzędzia APPRAISE, połączone

z kamerami monitoringu obiektowego oraz prowadzonego przy użyciu drona, podejrzany został zatrzymany przez pracownika ochrony. Po przeanalizowaniu materiału wideo okazało się, że kilka minut po rozpoczęciu wyścigu ta osoba była widziana na parkingu w towarzystwie dwojga ludzi. Ochronie nie udało się zatrzymać pozostałych podejrzanych, dlatego powiadomiono francuską policję o potencjalnym zagrożeniu atakiem. Po stronie francuskiej, na mecie wyścigu, był prowadzony nadzór z użyciem dronów, które współpracowały z narzędziami APPRAISE. Systemy te wykryły bójkę przy linii mety i przesłały raporty do organizatorów z wykorzystaniem aplikacji crowdsensingowej¹¹. Dodatkowo scenariusz zakładał naruszenie strefy powietrznej nad linią mety wyścigu przez niezidentyfikowany dron oraz jego neutralizację przez policję za pomocą systemu antydronowego APPRAISE. Podczas realizacji tego pilotażu zarówno interwencja francuskiej policji, jak i inne jej działania zostały zasymulowane, gdyż w tym czasie jednostka RAID wykonywała ważne zadania we Francji (związane z zamieszkami w Paryżu i dużym zagrożeniem terrorystycznym). Czynności przeprowadzone przez francuską policję wyglądałyby następująco: po wskazaniu adresu pilota drona udaje się tam policja, ale podejrzany nie otwiera drzwi i grozi, że zaatakuje zgromadzonych ludzi. Na miejsce zostaje wezwany oddział specjalny RAID. Podczas dojazdu dokładnie analizuje on treści internetowe, aby pozyskać jak największą liczbę informacji o domniemanym terrorystyce. Policjanci z RAID dokonują szturm, wchodzi do mieszkania zamachowca i neutralizują go¹².

Również tym razem wszystkie narzędzia APPRAISE wykorzystane podczas pilotażu zostały zademonstrowane przedstawicielom publicznych i prywatnych służb bezpieczeństwa. W czasie otwartej sesji demonstracyjnej mieli oni możliwość bezpośredniego kontaktu z partnerami technologicznymi projektu i zadawania pytań dotyczących użytych technologii. Pilotaż 1 umożliwił przetestowanie narzędzi powstałych w ramach projektu APPRAISE przeznaczonych do szybkiej wymiany informacji pomiędzy siłami policyjnymi dwóch różnych krajów europejskich oraz organizatorami wyścigu.

¹¹ *Crowdsensing* – program na bazie aplikacji stworzony do komunikacji pomiędzy zbiorowiskiem ludzi a administratorem systemu, którego zadaniem jest zbieranie informacji od osób znajdujących się w niebezpieczeństwie i przesyłanie ich odpowiednim służbom.

¹² N. Czyżewska, J. Przyjemczak, *Wsparcie technologiczne nowoczesnych systemów bezpieczeństwa...*

Atak z użyciem noża na terenie Międzynarodowych Targów Gdańskich – pilotaż 4

W dniu 21 września 2023 r. konsorcjum APPRAISE przeprowadziło czwarty pilotaż, w ramach którego po raz kolejny przetestowano technologie wypracowane przez partnerów projektu. Ćwiczenia odbyły się na terenie Międzynarodowych Targów Gdańskich (MTG) – AMBEREXPO podczas 15. Międzynarodowych Targów Kolejowych TRAKO 2023. W zorganizowanie tych ćwiczeń były zaangażowane: Polska Platforma Bezpieczeństwa Wewnętrznego (lider pilotażu), Międzynarodowe Targi Gdańskie i Komenda Wojewódzka Policji w Gdańsku. Wzięli w nich udział również pracownicy biura ochrony TAURUS oraz studenci Akademii Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni, którzy wcielili się w role uczestników targów¹³.

Scenariusz tego pilotażu bazował na ataku nożownika na uczestników targów. Faza pierwsza obejmowała stałą obserwację mediów społecznościowych i treści zamieszczanych w Darknecie. W ten sposób zostały wykryte wzmożona aktywność związana z targami oraz post zawierający groźby skierowane do organizatorów. Za pomocą narzędzi przeznaczonych do analizy treści internetowych oraz wykrywania zagrożeń w sieci zebrano informacje o podejrzanych osobach mogących kierować te groźby. Ponadto policja uzyskała informacje, że w przeddzień rozpoczęcia targów jeden z podejrzanych zakupił nóż w pobliskim centrum handlowym. W dniu otwierającym imprezę dokonano ataku cybernetycznego na stronę internetową TRAKO, który wykryto za pomocą narzędzi APPRAISE. Tego samego dnia podejrzany wszedł na teren MTG, gdzie rozpoznał go jeden z ochroniarzy. Uruchomiony system monitoringu śledził tę osobę za pomocą narzędzia, w którym zastosowano technologię wykorzystującą tzw. cechy niebiometryczne. Początkowo obserwowany zachowywał się normalnie, spokojnie chodził po części wystawowej. W pewnym momencie system monitoringu zauważył podejznanego z plecakiem, którego wcześniej nie miał. Narzędzia APPRAISE przeznaczone do analizy wideo pozwalają bowiem na wyszukanie przedmiotów na nagraniach monitoringu. Dzięki temu zidentyfikowano także pomocnika osoby podejrzanej, który podrzucił plecak. Aby ułatwić jego odnalezienie, wyposażono jednego z ochroniarzy w okulary HoloLens z wyświetlonym na nich wizerunkiem pomocnika. W tym czasie podejrzany przedostał się do strefy o ograniczonym dostępie. Przy wejściu

¹³ *Update and video for Pilot 4 in Gdansk*, <https://appraise-h2020.eu/node/107> [dostęp: 10 XI 2023].

do sali konferencyjnej zranił nożem ochroniarza, po czym wszedł do niej i kontynuował atak. W wyniku tych zająć kilku uczestników targów odniosło rany. Następnie zamachowiec wziął poszkodowanych jako zakładników i zamknął się z nimi w sali konferencyjnej. Narzędzia APPRAISE nadzorujące to zdarzenie uruchomiły alerty o ataku, które zostały wysłane zarówno do ochrony MTG, jak i policji. Narzędzia do analizy dźwięku wykryły krzyki i panikę, a narzędzia analizujące wideo – biegnące tłumy, osoby rane leżące na ziemi oraz nóż. Przeciwdziałanie skutkom paniki wymagało skutecznego kierowania zbiorowiskiem ludzi i ewakuacją, aby uniknąć dodatkowych ofiar. Za pomocą aplikacji crowdsensingowej do osób przebywających na targach zostały wysłane instrukcje dotyczące ewakuacji. Na teren imprezy wezwano dodatkowe siły policyjne, w tym Samodzielny Pododdział Kontrterrorystyczny Policji i negocjatorów, którym udało się zneutralizować terrorystę oraz uwolnić zakładników. Rozmowy negocjatorów były nagrywane i zostały poddane transkrypcji za pomocą narzędzi przekształcających mowę na tekst. Pilotaż obejmował także obserwację obszaru za pomocą dronów. Pozwoliło to na wykrycie pojazdu przemieszczającego się po terenie MTG w podejrzany sposób (jazda zygzakiem). W tym scenariuszu wprowadzono również elementy komunikacji za pośrednictwem aplikacji crowdsensingowej umożliwiającej uczestnikom zdarzenia informowanie pracowników ochrony o potencjalnym niebezpieczeństwie oraz wysyłanie informacji na temat tego, gdzie znajdują się ranni bądź osoby, które ukryły się po ataku¹⁴. Relację z tego wydarzenia można obejrzeć w serwisie YouTube¹⁵.

Narzędzia wykorzystane w pilotażu zostały zademonstrowane ponad 20 interesariuszom, wśród których byli przedstawiciele Policji, Sił Zbrojnych, agend rządowych, Straży Pożarnej, operatorów obiektów sportowych, przedstawiciele portów morskich oraz środowisk akademickich. Tak jak podczas wcześniejszych spotkań istniała możliwość bezpośredniego kontaktu z partnerami technologicznymi i zadawania pytań dotyczących narzędzi wytworzonych na potrzeby projektu.

Scenariusz pilotażu 4 był najbardziej kompleksowy ze wszystkich przygotowanych. Jako pierwszy i jedyny został zrealizowany podczas trwającego rzeczywiście wydarzenia – dużej imprezy, jaką były targi TRAKO 2023.

¹⁴ N. Czyżewska, J. Przyjemczak, *Wsparcie technologiczne nowoczesnych systemów bezpieczeństwa...*

¹⁵ *APPRAISE Pilot in Gdańsk*, YouTube, 17 XI 2023 r., <https://www.youtube.com/watch?v8-7inzQ1grE>.

Wykorzystano w nim ponadto największą liczbę narzędzi powstałych w ramach projektu APPRAISE. Wiązało się to z wieloma – czasami nieprzewidywanymi – wyzwaniami dotyczącymi przygotowania i organizacji pilotażu, ale jednocześnie stworzyło konsorcjum wyjątkową możliwość przetestowania nowych rozwiązań w realnym otoczeniu. Pilotaż 4 udowodnił, że są one skuteczne. Ćwiczenie to było również okazją do wypracowania lepszej współpracy pomiędzy publicznymi i prywatnymi podmiotami zajmującymi się zapewnianiem bezpieczeństwa w przestrzeniach publicznych w przypadku ataków.

Kappa FuturFestival – pilotaż 2

Ostatnie sprawdzenie technologii opracowanych w ramach projektu APPRAISE odbyło się 30 listopada 2023 r. w Turynie we Włoszech. Pierwotnie plan zakładał, że testy odbędą się w dniach 13–17 listopada 2023 r. podczas rozgrywek turnieju tenisowego ATP Finals 2023. Niestety konieczna była zmiana terminu i miejsca. Ostatecznie pilotaż przeprowadzono w ramach Kappa FuturFestival – jednego z najbardziej lubianych we Włoszech festiwali miejskiej muzyki elektronicznej. W trakcie tego pilotażu organizatorzy chcieli sprawdzić takie elementy, jak: śledzenie i kontrola treści w internecie, analiza wideo w czasie rzeczywistym, nadzór nad terenami i obiektami za pomocą dronów i kamer, elementy komunikacji z uczestnikami.

Przebieg tego ćwiczenia wyglądał następująco. Podobnie jak w poprzednich pilotażach przed rozpoczęciem wydarzenia w sieci pojawiły się nienawistne tweety pod adresem Kappa FuturFestival, w związku z czym w dniu imprezy przygotowano dodatkowe siły w postaci ochrony publicznej i prywatnej oraz zespoły ratownicze. W pewnym momencie niezidentyfikowany samochód minął barierę dostępu, wjechał do strefy dla pieszych i z pełną prędkością zmierzał w kierunku osób stojących w kolejce i czekających na wejście na festiwal. Pojazd poruszał się w taki sposób, aby zranić jak najwięcej ludzi. Część z nich zdołała uciec, inni zostali ranni. Zamachowiec wysiadł z samochodu i próbował wejść na zadaszony teren parku Parco Dora. Przebywający tam widzowie zostali powiadomieni za pośrednictwem aplikacji APPRAISE, że w pobliżu doszło do ataku i powinni się ukryć. Część z nich to zrobiła, ale niektórzy wpadli w panikę. W trakcie ucieczki przewrócili się i doznali obrażeń. Informacje o zabitych i rannych podało przez radio, portale społecznościowe i aplikację służącą do wykrywania

zbiorowiska ludzi. Policja wysłała do pomieszczeń drona, aby sprawdzić, do jakich szkód doszło w wyniku tych zdarzeń, oraz czy obszar jest bezpieczny dla ratowników mających udzielić rannym pierwszej pomocy. Monitorowano pojawiające się w internecie treści związane ze zdarzeniem, aby poznać motywy działania sprawcy. Specjalne narzędzie przeszukiwało strony wyszukiwarek internetowych, mediów społecznościowych, analizowało teksty, a także oceniało ryzyko i szacowało powstałe zagrożenia. Biorąc pod uwagę duży przepływ ludzi po ataku, niezmiernie istotne było stałe monitorowanie sytuacji. Ważne było również zbieranie materiału dowodowego, który organy ścigania będą mogły wykorzystać podczas procesu wykrywczego. System monitoringu został wzbogacony o narzędzie analizujące zgromadzone dane (np. sytuacje paniki, pobic itp.). Podczas realizacji scenariusza poszczególne służby były na bieżąco informowane o kolejnych krokach i zadaniach.

Ćwiczenie to po raz kolejny udowodniło przydatność narzędzi i technologii powstałych w ramach projektu APPRAISE. Podobnie jak wcześniej po zakończeniu pilotażu zorganizowano spotkanie z interesariuszami, podczas którego dyskutowano o możliwościach tych narzędzi i wymieniano się uwagami.

Podsumowanie

Projekt Komisji Europejskiej APPRAISE dotyczący perspektywy H2020 SU-FCT03-2018-2019-2020: Zarządzanie przepływem informacji i danych w celu zwalczania cyberprzestępczości i terroryzmu jest inicjatywą, która wskazała odpowiedni kierunek rozwoju w zakresie sprawowania nadzoru nad bezpieczeństwem oraz monitoringu ogólnodostępnych przestrzeni publicznych. W trakcie tego przedsięwzięcia przetestowano funkcjonowanie narzędzi i technologii w wymagających, trudnych i problemowych sytuacjach po to, aby skutecznie przeciwstawiać się zagrożeniom, unikać ich i właściwie działać w momencie, gdy się pojawiają. Stopień zaawansowania opracowanych i wytworzonych technologii pozwala stwierdzić, że narzędzia, które z nich korzystają, będą sprawnie współdziałać z tymi już istniejącymi oraz przyczynią się do szybszej i skuteczniejszej reakcji służb na zaistniałe zagrożenia. Dzięki wysiłkom osób zaangażowanych w projekt APPRAISE podejmowane w nim działania na rzecz poprawy bezpieczeństwa będą kontynuowane i rozwijane w ramach różnych inicjatyw.

Dr Jarosław Przyjemczak

Doktor nauk społecznych w dyscyplinie nauki o bezpieczeństwie, adiunkt na Wydziale Prawa i Administracji Wyższej Szkoły Administracji i Biznesu im. E. Kwiatkowskiego w Gdyni. Podinspektor Policji w stanie spoczynku, przez wiele lat pełnił służbę w Samodzielnym Pododdziale Kontrterrorystycznym Policji w Gdańsku. Uczestnik licznych krajowych i zagranicznych kursów i szkoleń związanych z walką z terroryzmem. Ukończył m.in. strategiczny kurs kontrterrorystyczny i zagrożeń terrorystycznych w Bramshill w Wielkiej Brytanii, organizowany przez Kolegium Policyjne CEPOL w ramach Europolu. Członek Polskiego Towarzystwa Bezpieczeństwa Narodowego, ekspert ds. bezpieczeństwa Polskiej Platformy Bezpieczeństwa Wewnętrznego. Redaktor naukowy cyklicznej publikacji *Zadanie specjalne – człowiek, technologia, instytucja*.

Kontakt: jarek.przyjemczak@wp.pl

Nina Czyżewska

Menedżer ds. realizacji projektów w Polskiej Platformie Bezpieczeństwa Wewnętrznego (PPBW). Uzyskała tytuł magistra z zakresu nauk politycznych ze specjalizacją organizacje międzynarodowe w Leiden University w Holandii oraz tytuł licencjata ze stosunków międzynarodowych na Uniwersytecie Jagiellońskim. W PPBW jest odpowiedzialna za wdrażanie i realizację projektów w zakresie bezpieczeństwa przestrzeni publicznej i przeciwdziałania radykalizacji finansowanych z programów Unii Europejskiej.

Wierzę, że poradzimy sobie z nowymi zagrożeniami!

Wywiad z płk. rez. Christopherem P. Costą, byłym doradcą prezydenta USA do spraw walki z terroryzmem, dyrektorem Międzynarodowego Muzeum Szpiegostwa w Waszyngtonie

Świat zmienia się w szybkim tempie. Zmienia się również charakter współczesnych zagrożeń. Niestabilna sytuacja geopolityczna, dynamiczny rozwój nowych technologii, pojawienie się kryptowalut i sztucznej inteligencji powodują, że służby odpowiedzialne za zapewnienie bezpieczeństwa muszą się mierzyć z nowymi wyzwaniami. W jaki sposób mogą się do nich przygotować, aby skuteczniej przeciwdziałać pojawiającym się zagrożeniom? Pułkownik rez. **CHRISTOPHER P. COSTA**, wieloletni oficer amerykańskiego wywiadu, odpowiada na to pytanie, odwołując się nie tylko do własnego bogatego doświadczenia, lecz także do historii światowego szpiegostwa i terroryzmu. Wskazuje zarówno na potrzebę krytycznej analizy wniosków płynących z przeszłości, jak i na umiejętność wykorzystywania przez służby nowych możliwości technologicznych. Podkreśla wagę wymiany informacji i rozwijania współpracy na poziomie międzynarodowym oraz akcentuje rolę, jaką w działaniach prewencyjnych odgrywa edukacja społeczeństwa. Propagowanie wiedzy postrzega jako misję Międzynarodowego Muzeum Szpiegostwa w Waszyngtonie, którym kieruje. Wywiad został przeprowadzony podczas wizyty dyrektora Christophera Costy w Polsce, a rozmowie towarzyszą refleksje związane z aktualną sytuacją w Europie Środkowo-Wschodniej.

Damian Szlachter: Wywiad ukaze się w 20. rocznicę zamachów na system transportu miejskiego w Madrycie, które diametralnie zmieniły europejskie podejście do walki z terroryzmem. Rozmowę chciałbym jednak rozpocząć od nawiązania do innego wydarzenia, symbolu końca XX wieku. Proszę powiedzieć, gdzie był Pan 11 września 2001 r. W jakim miejscu zastała Pana informacja o atakach na World Trade Center i Pentagon oraz jakie konsekwencje te wydarzenia miały bezpośrednio dla Pana?

Christopher Costa: Na krótko przed zamachami z 11 września przeprowadziłem się do Albany – miasta w stanie Nowy Jork, położonego niedaleko od Nowego Jorku, w górę rzeki Hudson. W tym czasie objąłem dowództwo nad batalionem rekrutacyjnym, co wiązało się z nadzorowaniem zaciągania do armii młodych ludzi. Wcześniej byłem oficerem wywiadu działającym w strefach bezpośrednich walk. Wojsko zdecydowało jednak o przydzieleniu mnie do tego batalionu. Nie było to miejsce, w którym chciałem być, gdy doszło do ataków terrorystycznych. Początkowo czułem się w nim źle, ponieważ nie mogłem towarzyszyć kolegom walczącym w Afganistanie. Następne dwa lata musiałem poświęcić poznawaniu armii i jej misji. Postanowiłem, że ten czas potraktuję jako okazję do gruntownego poznania zjawiska terroryzmu. Wieczorami prowadziłem zajęcia poświęcone terroryzmowi, a jednocześnie pełniłem inne obowiązki. Tak spędziłem półtora roku. Mocno się zaangażowałem, chcąc jak najlepiej zrozumieć to zagrożenie.

Chociaż nie byłem za granicą, wciąż czekałem na wezwanie do wojska i wyjazd na wojnę. Chciałem wykorzystać swoje umiejętności i wiedzę i pomóc w walce z terroryzmem. W końcu, jeszcze przed zmianą dowództwa, zadzwonił do mnie przełożony w randze generała i poprosił o wsparcie w pracy wywiadowczej w Afganistanie. Przyjąłem tę propozycję chętnie i bez wahania.

Kiedy doszło do ataków z 11 września, przebywałem w stanie Nowy Jork i tak jak większość ludzi na świecie byłem przerażony tym, co się wydarzyło. To był czas, kiedy trochę się nad sobą użalałem, ponieważ nie mogłem wykorzystać swoich umiejętności i wykszolenia na rzecz wojsk stacjonujących w strefie działań militarnych. Patrząc z perspektywy czasu, dostrzegam jednak, że to doświadczenie miało pozytywny wpływ na mój rozwój osobisty. Mogłem poświęcić się nauce i merytorycznemu przygotowaniu się do walki z terroryzmem.

Pracował Pan w każdym obszarze amerykańskiego systemu antyterrorystycznego, od pracy operacyjnej, przez poziom taktyczny, aż po poziom strategiczny, na czele którego stoi prezydent Stanów Zjednoczonych. W każdym z nich niezwykle istotna jest koordynacja wielu podmiotów uczestniczących w działaniach antyterrorystycznych. Proszę powiedzieć, w jaki sposób można utrzymać wysoki stopień koordynacji na każdym z tych trzech poziomów. Jakie są Pana doświadczenia z tym związane?

Ch. C.: Sposób, w jaki koordynuje się wszystkie te podmioty na poziomie operacyjnym, taktycznym i strategicznym, jest bardziej sztuką niż nauką. To ważne pytanie. Przyznam się, że chociaż przez wiele lat działałem na poziomach: operacyjnym i taktycznym, byłem na wielu misjach, to przed 11 września nie służyłem na poziomie strategicznym. Na pewno prowadziłem operacje, o których wiedziałem, że będzie miał do nich wgląd np. przewodniczący Kolegium Połączonych Szefów Sztabów, aby w razie potrzeby poinformować o tym prezydenta USA. Nie widziałem jednak pełnego cyklu strategiczno-operacyjno-taktycznego, dopóki nie podjąłem służby w Białym Domu. Pozwolę sobie na krótką dygresję z tym związaną. Zgłębianie problematyki terroryzmu i przekazywanie po 11 września wiedzy o tym zagrożeniu pomogło mi zrozumieć problemy, jakie pojawiły się w systemie bezpieczeństwa narodowego w obszarze reagowania. Byłem zafascynowany tym, jak przedstawiciele rządu podejmują decyzje oraz jak robią to dowódcy na polu bitwy. Podczas pobytu w Białym Domu i służby w Radzie Bezpieczeństwa Narodowego obserwowałem współpracę z zagranicznymi partnerami i tworzenie wspólnoty antyterrorystycznej, mającej skupić się na globalnej walce z terroryzmem, miałem okazję zintegrować i wykorzystać swoje doświadczenia. To właśnie wtedy byłem organem zwołującym agencje, co oznaczało, że w naszym systemie byłem mniej więcej trzygwiazdkowym odpowiednikiem oficera generalnego, asystenta sekretarza. Tam udało mi się zebrać ludzi ze wspólnoty antyterrorystycznej, aby skupić się na strategicznym wymiarze walki z terroryzmem. Sekretem mojego sukcesu, jeśli w ogóle go odniosłem, była pokora. Zdawałem sobie sprawę, że nie znam wszystkich odpowiedzi. Miałem na tyle dystansu do siebie i doświadczenia, aby wiedzieć, czyje interesy strategiczne reprezentuję, a przy tym pozwolić innym wyrazić swoje krytyczne opinie. Byłem świadomy, że nie powinienem bezrefleksyjnie podchodzić do swoich zaleceń dotyczących polityki i kierunków działań,

o których miał decydować prezydent. Tego wszystkiego nauczyłem się na polu bitwy. Te doświadczenia pomogły mi służyć w Białym Domu. To było ogromne przeżycie.

Filarem amerykańskiego systemu antyterrorystycznego jest Narodowa Strategia Antyterrorystyczna z 2018 r. W tym czasie w Polsce funkcjonował Narodowy Program Antyterrorystyczny, który pełnił podobną funkcję. Jak skutecznie nadzorować realizację takiej strategii przez organy państwowe? Innymi słowy, jak ocenić terminowość i jakość realizacji zadań strategicznych przez liderów obszarów i instytucje, które ich wspierają? Jak rozwiązać ten problem w USA?

Ch. C.: Narodową Strategię Antyterrorystyczną z 2018 r. zaczęliśmy opracowywać w dniu, w którym podjąłem służbę w Białym Domu. Pierwszym etapem była operacjonalizacja idei antyterrorystycznych. Prawdę mówiąc, nasze wysiłki w większości polegały na ściganiu, w sensie fizycznym, terrorystów w miejscach takich jak Afganistan oraz w Syrii i Iraku. Wdrażając nasze podejście, określaliśmy również, jak będzie wyglądała nasza strategia. Był taki czas, kiedy uważałem, że powinna się skupić niemal wyłącznie na zagrożeniu ze strony dżihadystów, ponieważ tak mocno skoncentrowaliśmy się na islamskim terroryzmie. Ale potem mój zespół doszedł do wniosku, że istnieją również inne zagrożenia, w tym ze strony skrajnej prawicy oraz innych ruchów ekstremistycznych, które należy uwzględnić w strategii z 2018 r. Występują w niej określenia „naziści” czy „organizacja nazistowska”, ponieważ uznaliśmy, że nie możemy ograniczać się do zagrożeń o charakterze dżihadystycznym. W strategii połączyliśmy zatem korzyści płynące ze współpracy międzyagencyjnej i sprzężenia zwrotnego, to znaczy wzięliśmy pod uwagę głos wszystkich instytucji odpowiedzialnych za walkę z terroryzmem. Przyjeliśmy, że strategia musi objąć brutalny ekstremizm krajowy, przeciwdziałanie radykalizacji, skrajnej prawicy i wszelkiego rodzaju ekstremizmom mogącym prowadzić do przemocy politycznej. Tak więc po raz pierwszy w historii kraju Stany Zjednoczone mówiły na szczeblu politycznym o terroryzmie wewnętrznym. Pamiętajmy, że w 1995 r. doszło u nas do zamachu w Oklahoma City, ale w latach 2017–2018 byliśmy świadomi zmieniającego się charakteru terroryzmu. Pomimo skupienia się na ISIS, Al-Kaidzie, Afganistanie, Iraku i Syrii wiedzieliśmy,

że musimy poświęcić uwagę również terroryzmowi krajowemu. Aktualnie mamy rok 2023 (wywiad został przeprowadzony w sierpniu 2023 r. – dop. D. Sz.) i nastąpiła zmiana myślenia o zagrożeniach terrorystycznych. Administracja Bidena zrobiła to, co uważam za słuszne. Zogniskowała strategię na krajowym brutalnym ekstremizmie i udostępniła ją wkrótce po przejęciu władzy.

Rzeczywiście, charakter zagrożeń ewoluuje. Nie spodziewałem się, że strategia z 2018 r. będzie aktualna wiecznie, ale naprawdę cieszę się, że przetrwała do tego roku, ponieważ jest to solidna strategia, która pomogła zarówno poprzedniej administracji, jak i tej obecnej. Dodam jeszcze jedną uwagę na temat tego, w jaki sposób ocenia się wdrożenie. To jest, jak mówi przysłowie, robienie kiełbasy (ang. *making sausage* – nie chcesz wiedzieć wszystkiego, co dzieje się za kulisami – dop. D. Sz.). Agencja o charakterze międzyresortowym jest odpowiedzialna za ustalenie konkretnych wskaźników skuteczności i wydajności. Następnie zwraca się do Rady Bezpieczeństwa Narodowego i sprawdza, ile ataków udaremnilo i ile umów wywiadowczych z partnerami na całym świecie zostało naruszonych. Wspomniana agencja przekształca nieco górnolotne sformułowania użyte w strategii w rzeczowe instrukcje dotyczące sposobu wdrażania wytycznych. Napisanie odgórnej strategii jest łatwe. Wyzwanie stanowi jej zaimplementowanie oraz ocena skuteczności.

Obecnie na wschodniej flance NATO mamy bezprecedensową sytuację związaną z bezpieczeństwem wewnętrznym państw graniczących z Federacją Rosyjską i Białorusią. Zdaniem polskich i unijnych ekspertów w najbliższych trzech latach należy spodziewać się wykorzystywania metod terrorystycznych do działań hybrydowych realizowanych przy wsparciu podmiotów państwowych. Działania te będą skoncentrowane na atakach zakłócających ciągłość funkcjonowania infrastruktury krytycznej (np. transportowej, energetycznej, telekomunikacyjnej). W jaki sposób zwiększać odporność obiektów szczególnie ważnych dla bezpieczeństwa państwa?

Ch. C.: Zgadzam się, sytuacja na wschodniej flance NATO związana z bezpieczeństwem wewnętrznym państw graniczących z Rosją i Białorusią jest bezprecedensowa. Zdaniem unijnych ekspertów w najbliższych latach należy się spodziewać podjęcia działań przez podmioty

prywatne i przy wsparciu wymienionych państw. Działania te oczywiście skoncentrują się na atakach, których celem będzie zakłócenie ciągłości funkcjonowania infrastruktury krytycznej (poziom operacyjny państwa). Jak zwiększyć odporność obiektów infrastruktury krytycznej? Tu moim zdaniem dochodzimy do sedna problemu. Myślę, że Putin będzie coraz bardziej niezadowolony z poziomu swojej zdolności do prowadzenia wojny konwencjonalnej. Dlatego powróci do dokonywania bardziej przemyślanych ataków na tę infrastrukturę. W związku z tym twoje pytanie jest naprawdę istotne. Wiemy, że Rosja w przeszłości korzystała, jak zauważył to ktoś z Agencji Bezpieczeństwa Wewnętrznego, z maskirowki. Nie tylko z możliwości destabilizowania, lecz także z dezinformacji, aktywności wywrotowej, ukrytych działań i zabójstw, czyli z wszystkich tych rzeczy, o których mówimy w Międzynarodowym Muzeum Szpiegostwa w kontekście historycznym. Te działania zaczną być prowadzone poza Ukrainą po to, aby wywierać coraz większą presję na NATO i inne sojusze. Tak więc infrastruktura krytyczna, nie tylko ta cyfrowa, lecz także fizyczna, ma kluczowe znaczenie, ponieważ jest podatna na sabotaż. Widzieliśmy tamy, które zostały przerwane. Widzieliśmy mosty, które zawaliły się w Ukrainie, zagrożone były linie kolejowe i inne obiekty. Wróćmy jednak do operacji specjalnych. Wiadomo, że historia jest świetną nauczycielką. Pokazuje, w jaki sposób narody radziły sobie z tymi operacjami i działalnością wywrotową. W związku z tym uważam, że działalność Agencji Bezpieczeństwa Wewnętrznego ma ogromne znaczenie, że ważne są wyciągane przez was wnioski i dzielenie się doświadczeniami. Mówiłem w innym miejscu o tym, że ta wiedza nie jest przeznaczona tylko dla was. Moim przyjaciółm z FBI i generałom z Dowództwa Operacji Specjalnych powtarzam, że jak to mówią „monetą królestwa” (czyli czymś, co ma dużą wartość lub wpływ w danej sferze – dop. D. Sz.) będzie w przyszłości kontrwywiad. Zagrożenia będą miały charakter hybrydowy, a to oznacza, że służby wywiadowcze będą zachowywać się w coraz większym stopniu jak terroryści. Widzimy to na przykładzie Iranu, który korzysta z usług podmiotów pozapaństwowych. Podobnie czyni Rosja. Będą one skłaniane do robienia coraz bardziej niebezpiecznych rzeczy, niosących śmierć. Myślę więc, że pańskie pytanie jest ważne. Jednocześnie wierzę w polskie służby bezpieczeństwa. Poznają historię Polski i jestem pod ogromnym wrażeniem. Zawsze podziwiałem polskie wojsko i możliwości zapewnienia bezpieczeństwa. Z historii wiemy

niestety, że sowiecko-niemiecka dezinformacja przez lata próbowała rozpowszechniać kłamliwą narrację o waszym wspaniałym narodzie. Na przestrzeni dziejów Polska była potęgą militarną, ale wy też po części padliście ofiarą położenia geograficznego waszego kraju.



Zdjęcie: Christopher P. Costa, dyrektor Międzynarodowego Muzeum Szpiegostwa w Waszyngtonie (z lewej), i Damian Szlachter, redaktor naczelny czasopisma „Terroryzm – studia, analizy, prewencja”, podczas spotkania w Centralnym Ośrodku Szkolenia i Edukacji ABW w Emowie.

Źródło: materiały własne.

Jakie wyzwania stoją przed zachodnimi służbami specjalnymi i organami ścigania realizującymi zadania związane z walką z terroryzmem w tej dekadzie XXI wieku? W jaki sposób można usprawnić swoje struktury, zwiększyć potencjał osobowy czy zasoby techniczne w walce z terrorystami za pomocą systemów bezzałogowych, druku 3D, płatności kryptowalutami, profesjonalnie szyfrowanych komunikatorów internetowych czy ukrytych forów na platformach gamingowych?

Ch. C.: Służby wywiadowcze muszą przede wszystkim dogłębnie przeanalizować wyciągnięte już wnioski. Potrzebna jest introspektywność, skłanianie do refleksji, zachęcanie ludzi do pisania i dzielenia się swoimi punktami widzenia i spostrzeżeniami, nawet jeśli ich przemyślenia nigdy nie miałyby ujrzeć światła dziennego. Pierwszy krok to uznanie, że świat się zmienia, a służby wywiadowcze muszą zdecydowanie zwiększyć swoje zdolności adaptacyjne. Podam przykład. W Stanach Zjednoczonych, ku wielkiemu rozczarowaniu i złości niektórych moich byłych kolegów, na potrzeby wojny w Ukrainie

dokonano fundamentalnej zmiany w zakresie wymiany informacji wywiadowczych. W ramach amerykańskiej wspólnoty wywiadowczej zdecydowano się odtajnić wiele wrażliwych danych zbieranych przez służby specjalne. Ja akurat uważam, że to genialne i inspirujące. Myślę, że ta zmiana w zakresie wymiany informacji i wykorzystania mediów społecznościowych jest ważna, bo pozwala uprzedzić działania naszych przeciwników. Na przykład według doniesień medialnych Stany Zjednoczone zdawały się wiedzieć, że Rosja zamierza zrobić coś, co mogłoby być pretekstem do zasugerowania, że Ukraińcy użyli broni chemicznej. Zdaniem mediów Stany Zjednoczone miały świadomość, że Rosja może skorzystać z podstępów. Podzieliły się więc tymi danymi wywiadowczymi. Gdyby więc Federacja Rosyjska tak rzeczywiście postąpiła, to wszyscy wiedzieliby, że mamy do czynienia z rosyjską operacją dezinformacyjną. To jest właśnie wyprzedzanie pod względem szybkości informacji. A to tylko jeden z przykładów. Jak można wykorzystać media społecznościowe? Stany Zjednoczone, jak również Wielka Brytania, niestety nie śledzą polskich mediów, mówią otwarcie: hej, jeśli nie jesteś zadowolony z Putina, skontaktuj się z CIA, a oto numer i sposób, w jaki możesz to bezpiecznie zrobić. Wiemy, że niezadowolonych Rosjan jest wielu. Jak to wykorzystać? Jeśli można posługiwać się kontem w serwisie X (dawniej Twitter) w złych czy szkodliwych zamiarach, można również korzystać z mediów społecznościowych w dobrym celu lub na rzecz poprawy bezpieczeństwa.

Specjaliści ds. bezpieczeństwa muszą pogodzić wiedzę o wszystkim – druku 3D, kryptowalutach i wszystkich tych osiągnięciach nowego wieku – aby szybko połączyć siły i lepiej zrozumieć zagrożenia. Kolejnym zbliżającym się problemem jest sztuczna inteligencja. Stany Zjednoczone muszą się nim zająć we współpracy ze społecznością światową. I nie może to być rozwiązanie przeznaczone wyłącznie dla USA, zwłaszcza gdy mówimy o tym, jak być o krok przed AI. Właśnie uczestniczyłem w krótkiej konferencji, podczas której usłyszałem od byłych senatorów o wyzwaniach związanych z jej rozwojem. Nie ma uniwersalnej polityki dotyczącej sztucznej inteligencji, ale musimy współpracować ze społecznością międzynarodową w sposób, w jaki nigdy wcześniej tego nie robiliśmy. Stany Zjednoczone tak postąpiły w przypadku firmy Huawei. Nie wiem, jak korzystano z Huawei w Polsce, ale wiem o doniesieniach mediów na temat tego, że Stany Zjednoczone dostrzegły groźne konsekwencje dysponowania przez

Chiny tzw. tylnymi drzwiami (ang. *backdoor* – luka w zabezpieczeniach systemu komputerowego pozwalająca uzyskać nieautoryzowany dostęp do komputera lub sieci – dop. D. Sz.) do zbierania danych. Nie było to wystarczająco szybkie posunięcie, ale Stany Zjednoczone podzieliły się swoimi obawami z partnerami i wielu z nich zauważyło zagrożenia związane z ochroną prywatności. To samo trzeba zrobić w przypadku sztucznej inteligencji. Musimy zrozumieć, jakie niesie ze sobą zagrożenia i szanse oraz jakie są nasze słabe punkty. Chciałbym dodać, że Stany Zjednoczone zbierają dane wywiadowcze na temat różnych rodzajów zagrożeń obserwowanych w świecie i udostępniają je opinii publicznej. Dyrektor Wywiadu Narodowego publikuje ogólnosiątkową ocenę zagrożeń. Te zagrożenia związane z niewłaściwym wykorzystaniem sztucznej inteligencji, z globalnymi pandemiemi, być może bardziej niebezpiecznymi niż COVID-19, z niezadowolonymi grupami, wynikające nie tylko ze skrajnie prawicowych, ekstremistycznych lub populistycznych poglądów, lecz także z tych, którymi manipulują służby wywiadowcze, sprawiają, że więcej krajów będzie podatnych na działania podejmowane przeciwko nim. Innymi słowy, coraz wyraźniej rośnie tendencja do podatności rządów na zagrożenia. Na przykład ludzie mogą uważać, że rząd nie może ich ochronić przed COVID czy przed utratą oszczędności życia w wyniku włamań. Ze względu na istnienie tych wszystkich rzeczy i technologii, jak również ludzi, którzy nie są w stanie nadążyć za tymi zmianami technologicznymi i sztuczną inteligencją, narody stały się bardziej bezbronne niż kiedykolwiek. Tak więc to służby wywiadowcze oraz służby odpowiedzialne za bezpieczeństwo są pierwszą linią obrony. Cieszę się, że kiedy pracowałem za granicą, miałem do czynienia ze „starą szkołą”. Rosjanie posługiwali się tym samym „rzemiosłem” co ja. Było uniwersalne. W Polsce również. Życie było prostsze.

Pod wpływem technologii świat bardzo się zmienił. To niezwykle trudne. Ale wierzę, że damy radę. Tak było dziś, gdy patrzyłem na ludzi zgromadzonych w audytorium Centralnego Ośrodka Szkolenia i Edukacji ABW (spotkanie z uczestnikami kursów szkoleniowych, funkcjonariuszami oraz pracownikami Centrum Antyterrorystycznego ABW – dop. D. Sz.) i słyszałem ich pytania. Nie inaczej jest, gdy rozmawiam z FBI i innymi agencjami. Krótko mówiąc, jestem przekonany, że to pokolenie to dźwignie.

Na zakończenie chciałbym zapytać Pana jako dyrektora słynnego Międzynarodowego Muzeum Szpiegostwa w Waszyngtonie o to, czy znajdują się tam eksponaty bezpośrednio związane z historią działań operacyjnych prowadzonych w ramach wojny z terroryzmem?

Ch. C.: Cóż, niestety, uświadamiamy społeczeństwu, jakie mogą być konsekwencje zaskoczenia, zwłaszcza w kontekście wydarzeń z 11 września. Zmieniły one nastawienie Stanów Zjednoczonych do walki z terroryzmem. Zmusiło to agencję międzyresortową do komunikowania się w sposób, jakim nigdy wcześniej się nie posługiwała. Nie chcemy czekać, aż kryzys spowoduje konieczne zmiany, a niestety z reguły tak się dzieje. W Muzeum Szpiegostwa nie tylko mówimy o 11 września, lecz także porównujemy tę „strategiczną niespodziankę” do Pearl Harbor, jak również demonstrujemy interaktywne rozwiązania dotyczące luk w zabezpieczeniach cyfrowych. Przedstawiamy proces wydania dyspozycji dotyczących bezpieczeństwa narodowego na przykładzie decyzji o ataku na Bin Ladena. Pokazujemy pokrótce, jak przebiegała ta operacja. To ważne, ale dla edukowania społeczeństwa większe znaczenie ma to, w jaki sposób zapadła decyzja o rozpoczęciu nalotu. Jak czerwony zespół (ang. *red team* – grupa, która udaje wroga i na polecenie organizacji próbuje dokonać fizycznego lub cyfrowego włamania do niej po to, aby mogła ona poprawić poziom swojej ochrony – dop. D. Sz.) kwestionował własne dane wywiadowcze? Kim byli ci bezimienni analitycy? Jak wykonywali swoją pracę na długo przed przeprowadzeniem operacji?

Muzeum Szpiegostwa opowiada te historie. Gdy wejdzie się w nim na czwarte piętro, które jest poświęcone odpowiedzi na pytanie, dlaczego narody szpiegują, zaprezentowane tam historie zawierają ważne ostrzeżenia. Skupiamy się nie tylko na dżihadystach i terroryzmie po 11 września, lecz także na anarchistach w Stanach Zjednoczonych i zagrożeniach ze strony organizacji paramilitarnych (np. tzw. straży wspólnotowej – dop. D. Sz.). Mówimy np. o czerwonej panice (ang. *red scare* – termin odnoszący się do okresów silnego antykomunizmu w historii Stanów Zjednoczonych, pierwszy dotyczył lat 1919–1920, drugi był związany z zimną wojną – dop. D. Sz.) i lęku przed rosnącym w siłę anarchizmem w 1919 r. FBI powstało w czasie, gdy J. Edgar Hoover prowadził śledztwo w sprawie anarchistów, prawda? Zajmujemy się również atakiem w Oklahoma City. Międzynarodowe Muzeum Szpiegostwa prezentuje szeroki wachlarz

historii. Jedna z moich ulubionych i bardzo osobistych dotyczy wydarzeń w Monachium w 1972 r. Miałem dziesięć lat, kiedy doszło do tego zamachu. Oglądałem to na żywo, podobnie jak 900 mln innych ludzi na świecie. Zwróciło to moją uwagę. Zamach w Monachium zapoczątkował nową erę w historii terroryzmu. Powoli przekształcił się w falę, z którą wciąż mamy do czynienia, czyli w terroryzm inspirowany dżihadem. Muzeum opowiada te wszystkie historie z szerokiej perspektywy. Mamy eksponaty, za pomocą których akcentujemy te ważne okresy w historii terroryzmu. Pokazujemy również tematy niewygodne, jak historia tzw. wzmocnionych technik przesłuchań. Nie mam nic przeciwko temu, by mierzyć się z kontrowersjami, jakie wywołuje ten temat. Nie będę się tutaj dłużej rozwodził, bo chcę, aby czytelnicy czasopisma przyszli i sami ocenili, jak poradziliśmy sobie w Muzeum z tym zagadnieniem.

Czy mogę zrobić dygresję? Chcę powiedzieć, że będąc w Warszawie, poszedłem do Muzeum Powstania Warszawskiego. Historia polskiego ruchu oporu w czasie II wojny światowej, historia wykorzystywanych wtedy metod i technik, to przykład niezwykle odważnej. Każdemu, kto chce słuchać, opowiadam o tym. Nadal ważne jest, aby zrozumieć rolę niekonwencjonalnych działań wojskowych. Nie rozmawialiśmy dziś o tym zbyt wiele, ale większość mojej pracy zawodowej dotyczyła poznawania, czym jest ruch oporu i czym są takie działania, jak również pracy z ludźmi, którzy się tym zajmowali. Jestem przekonany, że Polska jest niezwykle ciekawym polem do badań poświęconych tym zagadnieniom. W obliczu destrukcyjnych działań Rosji te lekcje historii nie tracą na aktualności i warto się nad nimi zastanowić.

W ramach opowieści dotyczących wywiadu osobowego prezentujemy w Muzeum historię człowieka pochodzącego z Danii, który zgłosił się na ochotnika do służby i został zwerbowany jako szpieg. Nazywa się Morten Storm. Znał on Anwara al-Awlakiego – propagandzistę Al-Kaidy. To jedna z pierwszych historii, które opowiadamy na temat walki z terroryzmem w kontekście wywiadu osobowego. W tej samej galerii przedstawiamy też historię izraelskiego oficera służącego w Szin Bet i zarazem Palestyńczyka powiązanego z Hamasem (chodzi o Mosaba Hassana Yousefa – dop. D. Sz.), odkrywając, na czym polega zakonspirowana relacja między źródłem osobowym a agentem prowadzącym. Jako ktoś, kto zajmował się źródłami,

doceniam sposób, w jaki Muzeum ukazuje tę historię. Poświęcono jej też książkę *Zielony książę* (ang. *The Green Prince*).

Kolejna prezentowana historia o walce z terroryzmem dotyczy analizy danych. Zarówno przed, jak i po 11 września Bin Ladena śledziły głównie analityczki z CIA i innych instytucji wywiadowczych USA. I te kobiety opowiadają o niektórych wykorzystywanych przez nie narzędziach analitycznych. Jest też kilka świetnych ekspozycji interaktywnych. Można również zapoznać się z ćwiczeniami tzw. czerwonego zespołu, które pokazują skomplikowanie kryjówki Bin Ladena i jej zdobycie przez jednostkę specjalną. Prezentujemy również przykłady sposobów podejmowania decyzji dotyczących bezpieczeństwa narodowego. Wspominałem już o moich doświadczeniach w Białym Domu i pracy związanej z terroryzmem. W sprawie obławy na Bin Ladena to nie do mnie należała ostateczna decyzja. Podejmował ją prezydent Stanów Zjednoczonych.

W Muzeum przyrównujemy również, jak już powiedziałem, przebieg wydarzeń z 11 września do tych w Pearl Harbor. A jest on niemalże analogiczny. Wszystko się zgadza – od lustrzanego odbicia po techniki komunikacji i transmisji pozyskanych informacji lub uzyskanych wytycznych. Wydarzenia z 11 września są zatem ukazane przez pryzmat historii. Wpisują się w nią również anarchiści i ich działania w 1919 r. w miejscach takich jak Waszyngton oraz ekspozyty związane z atakiem na budynek federalny w Oklahoma City. Na koniec opowiadamy historię wydarzeń w Monachium w 1972 r., z którymi wiąże się moje osobiste wspomnienia.

Stała wystawa Muzeum jest poświęcona historii szpiegostwa oraz technikom i metodom wykorzystywanym w czasie zimnej wojny. Uświadamiamy, jak podobne są niektóre strategie działania, aby stworzyć ważny kontekst dla tego, co dziś obserwujemy w Ukrainie. Rozmawialiśmy o idei ruchu oporu oraz o działaniach niekonwencjonalnych i hybrydowych. W Muzeum można obejrzeć ekspozyty związane z działaniami konspiracyjnymi prowadzonymi w czasie II wojny światowej, które to działania Polska tak dobrze zna. Zwracam uwagę, że jesteśmy świadkami tego, jak Ukraina stosuje przeciwko Rosji kilka doskonałych niekonwencjonalnych działań wojskowych. Te lekcje z przeszłości powinniśmy uznać za pouczające i warte rozważenia, ponieważ Zachód musi przeciwstawić się wywrotowej aktywności Rosji.

Międzynarodowe Muzeum Szpiegostwa nie zajmuje stanowiska. Nie mówimy ludziom, co mają myśleć. To oni decydują. Uważam, że to istotne. To były naprawdę ważne pytania. Dziękuję za nie.

Rozmawiał: Damian Szlachter

Płk Christopher P. Costa

Emerytowany oficer wywiadu. Przez 34 lata służył w Departamencie Obrony, z czego 25 lat jako oficer wywiadu w siłach specjalnych (Special Operations Forces). Za swoją pracę wywiadowczą w Afganistanie został odznaczony dwiema Brązowymi Gwiazdami (Bronze Stars). Po przejściu na emeryturę kontynuował służbę w Grupie Rozwojowej Wojsk Specjalnych Marynarki Wojennej Stanów Zjednoczonych (Naval Special Warfare Development Group) jako cywil. Za swoją służbę na rzecz amerykańskich operacji specjalnych został uhonorowany odznaczeniem Dowództwa Operacji Specjalnych Stanów Zjednoczonych (United States Special Operations Command Hall of Honor). Pułkownik Costa pełnił w Białym Domu funkcję doradcy prezydenta oraz dyrektora ds. przeciwdziałania terroryzmowi. Obecnie zajmuje stanowisko dyrektora w Międzynarodowym Muzeum Szpiegostwa (International Spy Museum).

TERRORISM

studies
analyses
prevention

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

Editorial team Damian Szlachter, PhD (editor-in-chief)
Agnieszka Dębska (editorial secretary, layout editor)

Translation Sylwia Kłobuszewska

Cover design Aleksandra Bednarczyk

© Copyright by Agencja Bezpieczeństwa Wewnętrznego 2024

ISSN 2720-4383
e-ISSN 2720-6351

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

Articles express the views of the authors

Declaration of the original version:

The printed version of the journal is the original version

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

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

Articles for the journal should be submitted through the editorial panel available at: <https://ojs.ejournals.eu/Terroryzm/about/submissions>

Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota”
ul. Nadwiślańczyków 2, 05-462 Wiązowna, Poland

Contact

phone (+48) 22 58 58 671
e-mail: wydawnictwo@abw.gov.pl
www.abw.gov.pl/wyd/



Printed in March 2024.

Print

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

Academic Editor Board

Sebastian Wojciechowski, Professor
Adam Mickiewicz University,
Institute for Western Affairs in Poznań

Waldemar Zubrzycki, Professor
Police Academy in Szczytno

Aleksandra Gasztold, Associate Professor
(PhD with habilitation)
University of Warsaw

Ryszard Machnikowski, Associate Professor
(PhD with habilitation)
University of Łódź

Agata Tyburska, Associate Professor
(PhD with habilitation)
Police Academy in Szczytno

Barbara Wiśniewska-Paź, Associate Professor
(PhD with habilitation)
University of Wrocław

Piotr Burczaniuk, PhD
Internal Security Agency

Jarosław Jabłoński, PhD
Armed Forces of the Republic of Poland

Anna Matczak, PhD
The Hague University of Applied Sciences

Paulina Piasecka, PhD
Collegium Civitas in Warsaw

Reviewers issue 5

Magdalena Adamczuk, PhD

Tomasz Białek, PhD

Daniel Boćkowski, PhD

Wojciech Grabowski, PhD

Marek Jeznach, PhD

Adam Krawczyk, PhD

Katarzyna Maniszewska, PhD

Anna Polak, PhD

Karolina Wojtasik, PhD

Jakub Zięty, PhD

TABLE OF CONTENTS

227 Foreword by Editor-in-Chief

ARTICLES

233 **Krzysztof Izak**
Twenty years since the Madrid attacks. Spain's anti-terrorist security issues

273 **Aleksander Olech**
The Wagner Group in Africa.
The sham battle of Russian mercenaries against terrorism

311 **Mariusz Cichomski**
Between armed conflict and state terrorism – specific individual restrictive measures adopted in Poland in the context of the war in Ukraine and the situation in Belarus. Legal perspective

351 **Julia Puczyńska, Marcin Podhajski, Karolina Wojtasik, Tomasz P. Michalak**
Large Language Models in jihadist terrorism and crimes

REVIEW ARTICLES / REVIEWS

383 **Jędrzej Łukasiewicz**
Book review: Rafał Miętkiewicz, Autonomous Systems in Maritime Operations

VARIA

391

Adam Tatarowski

Building resilience of critical infrastructure in the light of asymmetric threats and terrorism.

Legislative trends in the Polish implementation of the CER Directive with particular reference to aspects of standardisation and certification of organisational and technical solutions

411

Jarosław Przyjemczak, Nina Czyżewska

APPRAISE project. Building a security system for public spaces

423

I believe we can handle the new threats!

Interview with Col. (Ret.) Christopher P. Costa,
former counterterrorism advisor to the US president
and director of the International Spy Museum in Washington, DC

Ladies and Gentlemen!

The fifth issue of the journal “Terrorism – Studies, Analyses, Prevention” (T-SAP) is published on the twentieth anniversary of the terrorist attacks on Madrid’s urban transport system. The tragic events of 11 March 2004 remain the largest attack on European Union territory in terms of fatalities and injuries. Their emergence contributed to the development of the EU counter-terrorism policy framework. Among other things, the post of a EU Counter-Terrorism Coordinator was created at the time and the first EU counter-terrorism action plan was adopted. Several months after the attacks, the Counter-Terrorism Department – a separate counter-terrorism division – was created within the Internal Security Agency. Every year, 11 March is a reminder of the need to continue to take action against extremism and terrorism and the need to raise public awareness of these threats. To commemorate the victims of the Madrid attack, four of whom were Poles, 11 March is the European Day of Remembrance for Victims of Terrorism. We begin the next issue of T-SAP with a reminder of these events. In the article entitled *Twenty years after the Madrid attacks. Spain’s anti-terrorist security issues*, you will find a description of the course of the attack and an analysis of its political and social impact.

This issue also discusses the Wagner Group’s activities in Africa and its impact on the fight against terrorism on that continent, given that the presence of Russian mercenaries there has increased significantly in recent years. We hope that this study will reignite the discussion on the legitimacy of including such entities on the EU list of terrorist organisations.

The following article, which we would like to invite you to read, is the first scientific analysis of specific individual restrictive measures adopted in Poland in the context of the war in Ukraine and the situation in Belarus. The text discusses the relationship between national and EU restrictive measures and the rationale for including entities supporting Russian actions in Ukraine on Poland's sanctions list.

Recent months have seen the most rapid development of artificial intelligence technologies. In an article on large language models such as ChatGPT, the authors describe the new possibilities provided by such modern technologies and how they can be used in jihadist terrorism and crime.

We also encourage you to read the review of the monograph entitled *Autonomous Systems in Maritime Operations*. This is the first study in Polish to discuss so comprehensively the challenges of protecting seaports and maritime strategic infrastructure from the hostile use of autonomous floating vehicles for sabotage and terrorist activity.

By creating a space within T-SAP to talk about how to prevent, counter and combat terrorist threats, the journal's pages serve to initiate interesting discussions among security experts. Read the text on the need for a new approach to risk assessment of critical infrastructure in the light of asymmetric threats and terrorism. Standardisation and certification of organisational and technical solutions under the CER Directive, including technical measures to ensure physical security, will play a particular role in this effort.

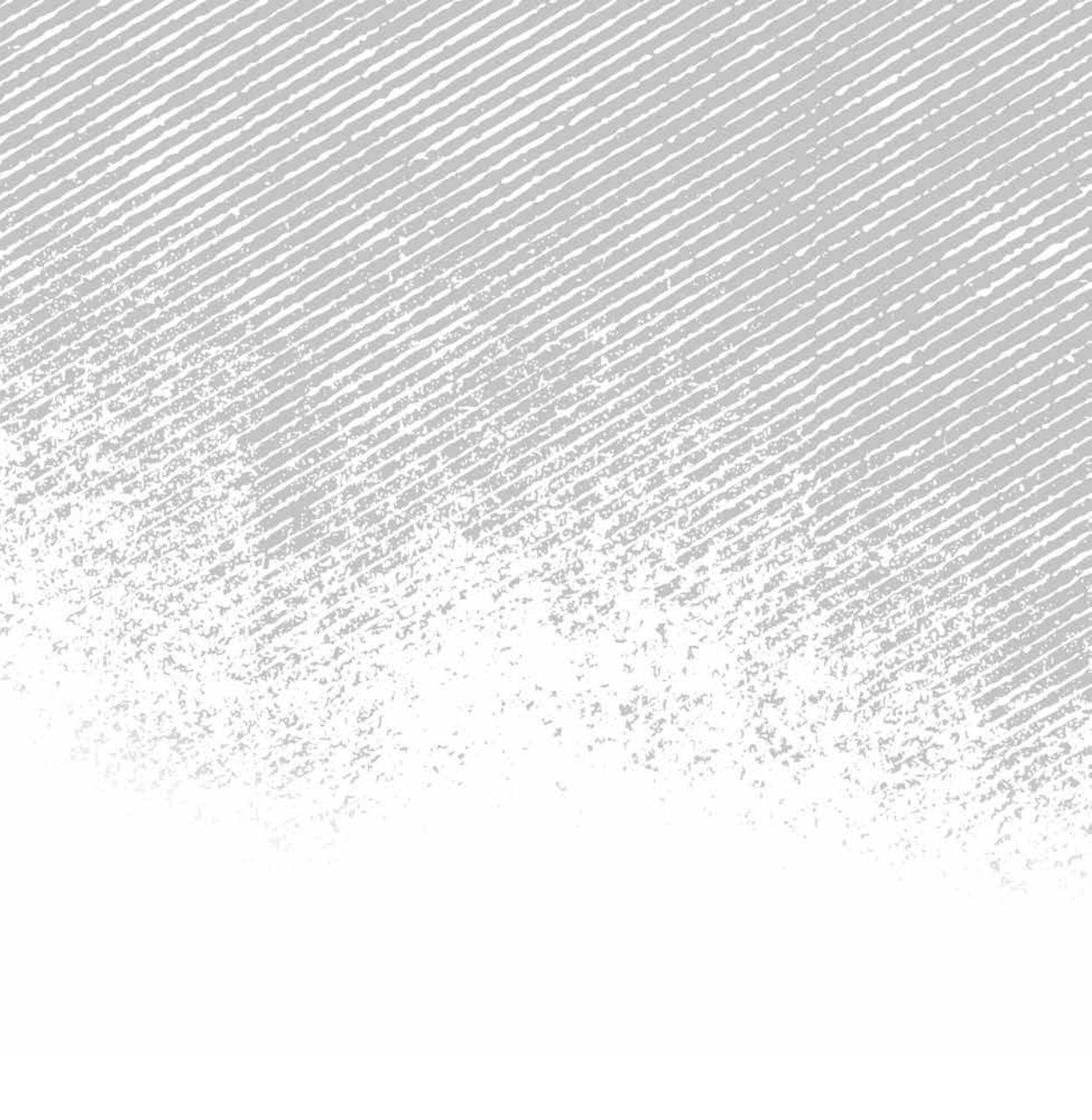
Polish state institutions, research centres or think tanks take part in many counter-terrorism initiatives funded by the EU or NATO. We would like the results of these projects to be presented also in T-SAP. One of them is the APPRAISE project, which is an element of building a security system for public spaces.

In the last section of the magazine, we publish an interview with a former Special Assistant to the President and Senior Director for Counterterrorism at the White House, who talked about the changes in counter-terrorism in the United States

introduced after the 11 September 2001 attack and shared more than three decades of experience he had gained while serving.

Inviting you to read the fifth issue of T-SAP, I hope that the materials presented in it will influence the discussion on Polish counter-terrorism priorities to be adopted for implementation during the next Polish Presidency of the EU Council in the first half of 2025. The previous Polish chairmanship of the counter-terrorism working groups was recognised by experts in the field of internal security from EU countries as one of the best in the period 2010-2020.

Editor-in-Chief
Damian Szlachter, PhD



ARTICLES

Terrorism – Studies, Analyses, Prevention, 2024, no. 5: 233–272

 CC BY-NC-SA 4.0

<https://doi.org/10.4467/27204383TER.24.009.19397>

Articles

Twenty years since the Madrid attacks. Spain's anti-terrorist security issues

KRZYSZTOF IZAK

Independent author

 <https://orcid.org/0000-0001-9815-6035>

Abstract

The aim of the article is to present the causes, chronological course and effects of the attack carried out on 11 March 2004 in Madrid, taking into account differences and contradictions in reports about these events. The author analyses the actions taken by the Spanish authorities to ensure anti-terrorist security in the country, including the creation of structures to fight Islamic terrorism and Muslim extremism. He also discusses the problems and challenges faced by Spanish services fighting political violence and illegal migration of people from high-risk countries, which affect the state of state security.

Keywords

Al-Qaeda, Muslim extremism, ETA, immigrants, secret services, terrorism, attacks

Spain is among the countries that have been fighting terrorism the longest. Separatist terrorist group Basque Homeland and Liberty (Euskadi Ta Askatasuna, ETA) has carried out terrorist attacks continuously for more than 50 years. In 2011, Basque nationalists announced an end to armed activity. Two years later, there was the self-dissolution of Batasuna, the political wing of ETA, and in 2018, of ETA itself. Since the beginning of the organisation in 1960, between 830 and 857 people have been killed, according to various press publications and books, including military personnel, officers of the Civil Guard (Guardia Civil), police officers, politicians, judges and random people. In addition, ETA carried out 84 kidnappings.

In the first decade of the 21st century Spain struggled with two different faces of terrorism: nationalist-separatist and Islamist. After the attacks of 11 September 2001 Spain took part in the operation against the Taliban in Afghanistan. Spain was also an initiator and signatory of the so-called the Letter of the Eight signed on 30 January 2003 by the Prime Ministers of Spain, Poland, Portugal, Italy, the United Kingdom, Hungary, Denmark and the President of the Czech Republic. The letter was an expression of solidarity with the United States in the common fight to defend democracy against the regime of Saddam Hussein. This letter demonstrated the division that had arisen in Europe on the issue of the Iraqi question. The Spanish government has consistently supported the intervention in Iraq. This was because Hussein's regime was not complying with UN resolutions and did not show the slightest willingness to cooperate with the inspectors of the International Atomic Energy Agency, who were supposed to check that arms stocks had been dismantled and work on weapons of mass destruction had stopped¹.

The state of the terrorist threat in Spain in the run-up to the attack

Prior to the Madrid attack, Spanish authorities had been monitoring the local Al-Qaeda network and terrorist cells connected with extremist organisations in Algeria and Morocco. Their creation in Spain in the 1990s was helped by the construction of a network of mosques financed by Saudi

¹ Later, the USA and other countries reported that no weapons of mass destruction had been found in Iraq and that reports of Iraq possessing them were false, propagated to create a casus belli.

Arabia and charitable organisations under its influence. Mosques were often staffed by imams and preachers adhering to the most radical Salafi doctrine of Islam, prohibiting the integration of Muslims into Western society and promoting the concept of jihad as armed struggle against ‘infidels’.

In the 1990s, Syrian Imad Eddin Barakat alias Abu Dahdah, one of the founders of Al-Qaeda in the country and its alleged leader, was active in Spain. From the Adolfo Suárez Madrid-Barajas airport, he sent jihadi volunteers to fight in Bosnia, Chechnya and Afghanistan. He provided wounded fighters with treatment in Spanish hospitals. In the first half of the 1990s, another Syrian – considered one of Osama bin Laden’s closest associates – Mustafa Setmariam Nasar, aka Abu Musab al-Suri, also lived in Spain. After marrying a Spanish woman who had converted to Islam, he was granted citizenship of that country².

The network of the Moroccan Islamic Combatant Group (Al-Jama’a al-Islamiyya al-Mukatila fi al-Maghrib) and the Algerian Armed Islamic Group (Al-Jama’a al-Islamiyya al-Musallah) were also active in Spain. It is worth knowing that five of the terrorists who directed aircraft to targets in the USA on 11 September 2001 were in Spain, working out the details of the attack with Al-Qaeda liaison officer Ramzi bin ash-Shibah.

In October 2001, Bin Laden on Al-Jazeera television spoke of Spain as the Arab Andalusia: *Let the whole world know that we shall never accept that the tragedy of Andalusia would be repeated*³. During Operation “Dactyl” (‘Dátíl’) conducted in November 2001 and in April and July 2002, the police smashed the Spanish Al-Qaeda network, in which the so-called Syrian group played a significant role. Abu Dahdah and ten members of the group, mostly Syrians, were detained at the time. Dozens of people were also arrested at the time, 25 of whom stood trial in Madrid in 2003⁴. At the same

² Abu Musab al-Suri is regarded as the most eloquent ideologue of the modern jihad and a sophisticated strategist. His work entitled *Dawa al-mukawama al-islamiyya al-alamijja* (Eng. A call for Islamic global resistance) published in cyberspace in 2004 and, running to 1,604 pages, was the most quoted on Islamist websites. In 2005, Al-Suri was arrested in Pakistan and handed over to Syria, where he was wanted for extremist activities in the 1980s. His current whereabouts are unknown. See: S. Grześkowiak, *Poczet islamskich ideologów i ekstremistów* (Eng. Islamic ideologues and extremists), Warszawa 2023, pp. 307–318.

³ *What’s Osama Talking About?*, Slate, 8 X 2001, <https://slate.com/news-and-politics/2001/10/what-s-osama-talking-about.html> [accessed: 8 X 2001].

⁴ R. Gunaratna, *Spain: An Al Qaeda Hub?*, “UNISCI Discussion Papers” 2004, no. 5, <https://www.redalyc.org/pdf/767/76712467002.pdf>, pp. 1–8 [accessed: 22 II 2014]; Fernando

time, both Spanish citizens and facilities belonging to Spain were targeted in terrorist attacks in Iraq, Algeria and Morocco.

In May 2003, the United States Army Forces Command entrusted Poland with the organisation and subsequent command of the Multinational Division Central-South - MND C-S in Iraq. The MND C-S officially began operations on 3 September 2003. In its first phase⁵, it consisted of three multinational brigades: a Polish brigade of 2,400 soldiers in the provinces of Babylon and Karbala; a Ukrainian brigade of 1,800 soldiers responsible for the province of Wasit; and a Spanish brigade of 1,300 soldiers assigned to the provinces of Al-Qadisiyah and An-Najaf for security control⁶. José María Aznar of the right-wing People's Party (Partido Popular, PP) saw the intervention in Iraq as part of the war on terrorism and considered it the greatest threat in the modern world. He claimed that it was NATO's task to develop appropriate political and military instruments to combat it. This position reflected his personal attitude to terrorism, also expressed many times before in the context of the ETA threats⁷.

The majority of the population and the opposition Spanish Socialist Workers' Party (Partido Socialista Obrero Español, PSOE) led by José Luis Rodríguez Zapatero were opposed to sending Spanish forces to Iraq. In 2003, mass protests were organised against the departure of soldiers to Iraq. In October of the same year, Bin Laden accused the U.S. of pursuing imperial interests. He also threatened Italy, Turkey, the United Kingdom, Japan, Australia, the Netherlands, Poland and Spain that if they did not withdraw their troops from Iraq, appropriate retaliatory measures would be taken against them⁸.

At the end of November 2003, seven members of the task force of the Spanish National Intelligence Centre (Centro Nacional de

Reinares, *experto en terrorismo internacional, advierte: "Al Qaeda está hoy más extendida de lo que ha estado nunca"*, Universidad Internacional Menéndez Pelayo, <https://www.uimp.es/actualidad-uimp/fernando-reinare-experto-terrorismo-internacional.html> [accessed: 21 VI 2021].

⁵ More about MND C-S later in the article – editor's note.

⁶ M. Brylew, *Irak 2006–2012. Stabilizacja czy konflikt?* (Eng. Iraq 2006–2012. Stabilisation or conflict?), Toruń 2013, p. 50.

⁷ P. Domejko-Kozera, *Polityka bezpieczeństwa w Hiszpanii w latach 1992–2004* (Eng. Security policy in Spain 1992–2004), Warszawa 2006, p. 46.

⁸ A. Wejkszner, *Ewolucja terroryzmu motywowanego ideologią religijną na przykładzie salafickiego ruchu globalnego dżihadu* (Eng. The evolution of terrorism motivated by religious ideology as exemplified by the Salafist global jihad movement), Poznań 2010, p. 338.

Inteligencia, CNI) were killed in an ambush and one was wounded. The incident occurred on a busy highway, 30 km south of Baghdad⁹. In early December 2003, the Institute of the Islamic Centre for Jihad Media (Markaz al-Islam al-Jihadi Media Institute) controlled by the Al-Qaeda Organisation in the Arabian Peninsula (Tanzim Al-Qaeda fi Jazirat al-Arab) published a four-page *Message to the Spanish People* and a forty-seven-page analysis of the situation in Iraq and the role of the Mujahidin fighting in the name of Islam¹⁰. The document devotes one chapter to a detailed discussion of the political, economic and social realities of the UK, Poland and Spain, which supported the U.S. in the Iraq war. Leaving aside the extensive threads relating to Iraq and the U.S., the section on Spain, to which six pages are devoted, can be considered particularly interesting. The author or authors put forward the thesis that the authorities of this country could be forced to withdraw troops from Iraq by carrying out several painful attacks. Such an action would have an impact on the elections. Indeed, it could be predicted that the government would not hold out following two or three strikes, and under public pressure would withdraw some forces. It was projected that a certain victory would then be won by the Socialist party, which opposed sending troops to Iraq, and that it would be this party which would lead to the Spanish contingent leaving there. Such a decision by Madrid, coupled with a similar one by Rome, would create social and political pressure in the UK. As a result, Prime Minister Tony Blair would have lost power. There is no doubt that the author or authors of the documents were well aware of the political situation in Europe, including Poland as a loyal ally of the United States¹¹.

On 24 December 2003, a bomb attack was foiled at the Chamartin train station in the north of Madrid. On the Intercity train from Irún in the Basque Country to Madrid, ETA terrorists intended to place two suitcases containing explosives weighing a total of around 50 kg. The police prevented a tragedy - one bomb was managed to be intercepted as the terrorist Garikoitz Arruarte Santacruz, who was carrying a suitcase with 25 kg of explosives, was arrested

⁹ *Siedmiu hiszpańskich agentów zginęło w Iraku* (Eng. Seven Spanish agents killed in Iraq), Wirtualna Polska, 29 XI 2003, <https://wiadomosci.wp.pl/siedmiu-hiszpańskich-agentow-zginelo-w-iraku-6036492925121665a> [accessed: 30 XI 2003].

¹⁰ H.A. Fernández, *Does al-Qaeda have a global strategy?*, Elcano Royal Institute, 4 V 2004, <https://www.realinstitutoelcano.org/en/analyses/does-al-qaeda-have-a-global-strategy/> [accessed: 6 V 2004].

¹¹ *Ibid.*

in San Sebastián. The second bomb was found in the luggage compartment of a train, stopped at Burgos train station, and - after the passengers had been evacuated - detonated. It was placed on the train in San Sebastián by Gorka Loran, who was subsequently arrested. The bombs were thought to have exploded in Chamartin during the afternoon rush hour. According to experts, the times set on the detonators suggested that ETA did not so much want to carry out a massacre as to cause panic and chaos. All passengers and railway workers would have managed to evacuate, as ETA had a habit of warning of bombings. A recording of such a warning was found by the police in the hideout of the arrested terrorists¹². On 26 December 2003, a bomb was found on the tracks of the Zaragoza-Caspe-Barcelona line, which was due to explode on 31 December 2003.

On 29 February 2004, Civil Guard officers arrested young ETA terrorists Gorka Vidal Álvaro and Irkus Badillo Borde, who were carrying 536 kg of explosives in a van. Also in the van was a map of Madrid, with a marked district including the NII Shopping Park, the airport and a section of Alcalá de Henares. The target of the next attack was to be the Avenida de América metro station in Madrid. One of the terrorists admitted that ETA was planning to carry out an assassination attempt on the King during the Christmas break¹³. The secret services also expected a major attack in Madrid before the 14 March elections, as a show of strength from the Basque separatists at a time of crisis within the organisation. In order to prevent terrorists from carrying out their plans, all state security services have been put on alert¹⁴.

Preparations for a terrorist attack in Madrid

According to Spanish police, the initiator of the attack was Rabei Osman Ahmed aka Muhammad Al-Masri (Muhammad the Egyptian), a former Egyptian army officer and explosives specialist. In the 1990s

¹² *ETA pretendía volar la estación de Chamartín con un "tren bomba" y provocar una masacre*, ABC España, 26 XII 2003, https://www.abc.es/espana/abci-pretendia-volar-estacion-chamartin-tren-bomba-y-provocar-masacre-200312260300-228547_noticia.html [accessed: 26 XII 2003].

¹³ *Actividad Terrorista de ETA 2004*, Ministerio del Interior, <https://www.statewatch.org/media/documents/news/2005/jan/mirbal2004acteta.pdf> [accessed: 12 III 2005].

¹⁴ *Ibid.*

he was in Afghanistan, where he made contact with Al-Qaeda. In 1999, he reached Germany illegally. He was then arrested on a train while travelling to France because he was travelling without documents. In doing so, he gave a false identity - he asserted that he was Palestinian. After his stay in prison, he was sent to the Lebach refugee camp, where he was granted a one-year residence permit. During this time he became an active preacher, preaching hatred of Jews. Just before the attacks of 11 September 2001, he appeared in Spain. In Madrid, he was contacted by a Tunisian national, Serhan Abdelmajid Fakheth (Sirhan bin Abdelmadjid Fakhith) aka El Tunecino (the Tunisian), who had come to Spain in 1996 as part of a scholarship programme. He undertook doctoral studies in economics, but did not complete them. Instead, he preached increasingly radical views until he became a religious fanatic. He became radicalised under the influence of Imam Munir Mahmoud Al-Masari of the M-30 mosque in Madrid. It was to the credit of the Tunisian that the Al-Qaeda cell was rebuilt in the Spanish capital. It was mainly made up of Moroccans, who had hitherto posed no threat and remained at large after Operation "Dactyl". The Syrian, Algerian and Tunisian nationals arrested at the time were experienced fighters with a war past in Bosnia, Chechnya and Afghanistan. Fakheth befriended Algerian Ahmed Brahim, the alleged treasurer of Al-Qaeda in Spain, and after his arrest - in connection with the attacks on the U.S. embassies in Kenya and Tanzania on 7 August 1998 - with Brahim's family. The Tunisian is believed to have maintained contacts with other extremist groups operating in Spain, not directly connected to his cell, but operating within international jihadist structures¹⁵. His acquaintance with Al-Masri, who frequently changed identities and documents in Spain, contributed to Fakheth becoming the organiser and coordinator of the Madrid train attack. Even before this event, Al-Masri had left Spain. He went to Italy, where he was employed as a bricklayer and was planning a major attack in Europe and recruiting Islamic volunteers to fight against NATO forces in Iraq. After Al-Masri fled Spain, Fakheth took over his logistical base and contacts. He turned to Amer Azizi aka Osman al-Andalusi, considered to be Abu Dahdah's right-hand man, for help in carrying out the attack. After his arrest, Azizi took over the leadership of Al-Qaeda's Spanish cell. In 2001 after the attack in the U.S., he hid from Madrid police for a week.

¹⁵ F. Reinares, *Al-Qaeda's Revenge. The 2004 Madrid Train Bombings*, New York 2016, pp. 56–59.

Upon his return to the Spanish capital, he quickly sold his car and fled the country. In November 2001, during the dismantling of a Spanish Al-Qaeda cell, police found documents in Azizi's home indicating his contacts with the organisation, his recruitment of young Muslims for training in Afghanistan and his links to some of the 11 September 2001 attackers, to whom he and Abu Dahdah had organised a meeting in Tarragona. He also maintained contacts with the organisers of the attacks in Casablanca on the night of 16-17 May 2003¹⁶. Azizi was also the liaison between Al-Qaeda and the Moroccan Islamic Combatant Group and this circumstance the Tunisian tried to exploit. A meeting between the two extremists took place in Turkey in late 2002 and early 2003. Fakhret asked Azizi to assign him fighters willing to die as martyrs to carry out a terrorist operation. Azizi refused because such people had been arrested. Instead, he allowed him to act on behalf of Al-Qaeda. He also recommended a Moroccan, Jamal Zougam, who could help organise a functioning terrorist group¹⁷.

According to the conception of Fernando Reinares, a Spanish terrorism expert, Azizi was the instigator of the Madrid attack. His name appears in 149 of the 271 volumes of court files relating to the events of 11 March 2004¹⁸. The decision to attack Spain was reportedly made in Karachi, in southern Pakistan. The plan was approved in February 2002 at an Al-Qaeda meeting in Turkey, which Azizi also attended. In 2005, he was killed in a U.S. air strike in North Waziristan within West Pakistan¹⁹. Reinares primarily challenged the thesis promoted by left-wing circles

¹⁶ In May 2003, a group of 14 terrorists belonging to the Salafi Jihad organisation (As-Salafijja al-Jihadijja) attacked two restaurants in Casablanca, Farah hotel, Belgian consulate, Jewish centre and cemetery. Thirty-one people were killed and around 100 injured. See: K. Izak, *Leksykon organizacji i ruchów islamistycznych* (Eng. Lexicon of Islamist organisations and movements), Warszawa 2014, p. 117.

¹⁷ F. Reinares, *Al-Qaeda's Revenge...*, pp. 118–120; Z. Jakubowska, *Madryt 11 marca* (Eng. Madrid 11 March), Warszawa 2005, pp. 116–117.

¹⁸ *Madrid bombings "probably al Qaeda"*, Stuff, 21 I 2010, <https://www.stuff.co.nz/vl-push/world/3226277/Madrid-bombings-probably-al-Qaeda> [accessed: 21 I 2010].

¹⁹ A. Hernández, *11M: quién fue el autor intelectual y otras claves que plantea el documental de Netflix sobre el mayor atentado yihadista en Europa*, BBC, 11 III 2022, <https://www.bbc.com/mundo/noticias-60693476> [accessed: 11 III 2022]; W. Maclean, *New evidence of Qaeda tie to Madrid blast: expert*, Reuters, 13 I 2010, <https://www.reuters.com/article/cnews-us-security-spain-qaeda-idCATRE60B52020100112> [accessed: 13 I 2010]; A. Martín Plaza, *Los atentados del 11M que sacudieron España*, RTVE, 11 III 2014, <https://www.rtve.es/noticias/20140311/atentados-del-11m-sacudieron-espana/893543.shtml> [accessed: 11 III 2014].

linking the Madrid attack to the war in Iraq. According to his conception, the Madrid attack was supposed to be Al-Qaeda's revenge for the police's dismantling of its Spanish network in 2001-2002. The attack, however, had nothing to do with the presence of Spanish soldiers in Iraq, as they had started their mission in 2003. Their presence only then became the perfect pretext for carrying out the attack²⁰. Al-Masri admitted to the early preparation of a series of attacks in Madrid in a telephone conversation with his "protégé" Palestinian²¹. It was overheard by Italian police in May 2004. In it, Al-Masri stated, among other things, that it had taken him two and a half years to prepare for the attack. Although he was not in Madrid at the crucial moment, he maintained contact with the attackers²². Also among the organisers of the attack was a Moroccan, Hasan al-Haski, believed to be the leader of a cell of the Moroccan Islamic Combatant Group in Spain, where he had appeared after an extended stay in Belgium²³.

Taking Azizi's advice, Fakhret made contact with Zougam. He was, along with compatriots Muhammad Chaoui and Muhammad Bekkali, co-owner of the Nuevo Siglo (New Century) mobile phone shop in Madrid's Lavapiés district. Zougam had been known to the police since 2001, when they were cracking down on the Al-Qaeda network in Spain. He was arrested and later released from prison - despite his known links with the Algerian Armed Islamic Group, with many of Abu Dahdah's men, with Azizi and Muhammad al-Fizazi, one of Morocco's most radical preachers. Another person helping Fakhret recruit volunteers for the terrorist cell and most likely funding the preparations for the attack was Moroccan Jamal Ahmidan, nicknamed 'Chinaman' or 'Mowgli' - a wealthy clothing shop owner and drug trafficker who became the Tunisian's deputy. Another figure in the group of assassins was Moroccan Rafa Zuhier, an associate of the 'Chinaman' in the drug trafficking. He also maintained contacts with individuals with access to explosives. He established these relationships while in prison, where he was serving a sentence for armed robbery. There he met the Spaniard Antonio Toro Castro, a drug and explosives

²⁰ F. Reinares, *The Evidence of Al-Qa`ida's Role in the 2004 Madrid Attack*, "CTC Sentinel" 2012, vol. 5, no. 3, <https://ctc.westpoint.edu/the-evidence-of-al-qaidas-role-in-the-2004-madrid-attack/> [accessed: 18 IV 2012].

²¹ Z. Jakubowska, *Madryt 11 marca...*, pp. 114-115.

²² *Llega a España "El Egipcio" para ser juzgado por el 11-M*, 20 minutos, 17 XI 2006, <https://www.20minutos.es/noticia/173755/0/egipcion/11-m/italia/> [accessed: 17 XI 2006].

²³ F. Reinares, *The Evidence of Al-Qa`ida's Role...*, pp. 51-52.

trafficker whose brother-in-law Jose Emilio Suárez Trashorras was a miner in Avilés (a town in Asturias in the north-west of Spain). After leaving prison, Zuhier continued to maintain his acquaintance with Castro and his associates. He put them in contact with Moroccan drug traffickers. Close relations between Muslims and Spaniards were such that the former were even invited to Trashorras' wedding to Castro's sister, which took place in February 2004. At that time, negotiations were already taking place for the purchase by the Moroccans of some 200 kg of the dynamite-based explosive goma-2 eco, used in the Spanish construction and mining industries. It was also, in addition to titadine produced in France, used by the ETA. The purchase of explosives by the Spaniards for 6,000 euros and 25 kg of hashish was justified by its use both in Morocco and to blow up safes during robberies in Madrid. The material came from the "Conchita" kaolin mine owned by Caolines de Merilles, where Trashorras had previously worked. The Goma-2 eco was taken out of the plant by Emilio Llano Álvarez, a supervisor at the "Conchita" mine²⁴.

The explosive was first sent in small quantities in the luggage compartment of airline coaches travelling between Asturias and Madrid. The goods were sent by a 16-year-old boy, who was called 'Gitano' ('Gypsy')²⁵. For the largest part of the goma, the Moroccans personally came to Avilés, where they collected it directly from Trashorras. He also prepared nails and bolts to reinforce the deadly power of the explosive. From Avilés to Madrid, the Moroccans returned in two cars: their own Volkswagen Golf, in the boot of which they carried the goma-2 eco, and a Toyota borrowed from the Spaniards. It was driven by a 'Chinaman' who drove first and was supposed to warn against police patrols. He had already been stopped and fined three times before for various offences. The explosive was brought safely to a rural house in Morata de Tajuña, near Chinchón, a suburb of Madrid. It was a low-traffic area and the building was completely enclosed by a covering fence. The property had previously served as a shelter for illegal immigrants who sympathised with Muslim extremists. It belonged to a Syrian man arrested in 2001 on suspicion of belonging to Al-Qaeda. The first tenant was a Moroccan arrested in 2003 in connection with the Casablanca attack, and the second was a 'Chinaman'. A month before the attack,

²⁴ Z. Jakubowska, *Madryt 11 marca...*, p. 126.

²⁵ Due to the boy's young age, his name was not made public.

the village house had begun a flurry of bomb-making activity based on explosives brought from Avilés. Aluminium detonators and mobile phones were used as igniters. The phones were delivered to the Nuevo Siglo shop by two Indians: Vinay Kohly and Suresh Kumar. Zougam then took mobile phones to a house in the village, where they were converted into timed detonators. This was probably done by the aforementioned Chaoui and Bekkali. The bombs were constructed by the Moroccan Abderrahman Zbakin known as 'The Chemist'. Zugam, 'Chinaman' and Trashorras were also frequent visitors. Osman al-Ghanut, a young Moroccan working as a bricklayer and helping to prepare the explosives, was in the house at all times. A total of 13 bombs were constructed and placed in backpacks and bags. The ready-made explosives were transported in a stolen Renault Kangoo van and a Škoda passenger car to a house in Madrid's Alcalá district, inhabited by North African immigrants, and to a flat in the Leganés neighbourhood, rented three days before the attack. It was located on the first floor of the building and had an area of almost 100 m². On 10 March, the terrorists involved in placing the bombs on the trains carried out a ritual cleansing at a hairdressing establishment owned by Moroccan Abdeluaid Berrak, a friend of Abu Dahdah. In total, more than 40 people were involved in the preparations for the attack²⁶.

Course of the attack

On the morning of Thursday 11 March 2004, seven terrorists - Tunisian Fakheth and Moroccans - Ahmidan, Abd an-Nabi Kundja, Allakema Lamari, Muhammad Ulad Akcha, his brother Rachid Oulad Akcha and Asri Rifat Anuar arrived in Renault Kangoo and Škoda cars in Alcalá de Henares, a town about 30 km east of Madrid, to land bombs in the carriages of the Cercanías light rail. There are ten main lines of these trains in and around Madrid itself. The trains, with the exception of one line, stop or terminate at Atocha station, the central hub railway station in the Spanish capital. There are three Cercanías lines in Alcalá de Henares. One runs

²⁶ F. Reinares, *Al-Qaeda's Revenge...*, pp. 71–74; Z. Jakubowska, *Madryt 11 marca...*, pp. 127–129.

from Guadalajara and the other two start here. During the morning rush hour, crowded trains towards Madrid leave here every five minutes²⁷.

The van was parked near the station. Luis Garrudo, a caretaker living nearby, noticed that three people had got out of it. They were filmed by surveillance cameras along with four others as they entered and exited trains standing on the platforms. The perpetrators had placed explosive devices on four trains. The trains full of passengers left Alcalá de Henares for Madrid between 7.01 a.m. and 7.14 a.m.²⁸

Atocha railway station, train no. 21431

The train stopped at platform 2. Many passengers left the train and people who wanted to travel towards Alcobendas, 13 km north of Madrid, started to board it. At 7.37 a.m. (according to other sources at 7.39 a.m.)²⁹ the first bomb exploded and two more exploded four seconds apart. The explosions occurred in carriages 4, 5 and 6³⁰, as a result of which 29 passengers were killed and 115 injured. The force of the explosion was somewhat reduced as a result of the open doors of the train, but the explosion of the bombs placed in the baskets on the right caused the shockwave to spread across the platform, where there were many passengers. Chaos reigned among them. Their goal was to get out of the wreckage of the train. People were bumping into each other trying to run to the escalators, which was not easy given that at that hour Atocha station resembled a Tokyo underground station. As the bombs exploded, a second train was approaching Atocha station³¹.

²⁷ Compiled on the basis of residual information. See: Z. Jakubowska, *Madryt 11 marca...*, pp. 56–57, 74, 129, 207–208, 212–214.

²⁸ A. Martín Plaza, *Los atentados del 11M que sacudieron España...; Atentados Terroristas del Día 11 del Marzo de 2004 de Madrid*, Juzgado Central de Instrucción Nº 6 Audiencia Nacional Madrid, <https://e00-elmundo.uecdn.es/documentos/2006/04/11/auto11m/01.pdf>, p. 1 [accessed: 11 IV 2006]; Z. Jakubowska, *Madryt 11 marca...*, pp. 55–56.

²⁹ Publications give different times for the explosion of the first bomb on the train at Atocha station, e.g. 7.37, 7.38 or 7.39 a.m. There are also discrepancies in the timing of the explosions on the other trains, all of which were supposed to have occurred between three and five minutes apart, and not as indicated in the graphics (Figure 1, Figure 2). See: *The Terror Attacks in Madrid...*, pp. 28–30 [accessed: 11 III 2008]; F. Reinares, *Al-Qaeda's Revenge...*, p. xxiii.

³⁰ F. Reinares, *Al-Qaeda's Revenge...*, p. xxiii.

³¹ *The Terror Attacks in Madrid...*, p. 27.

Atocha railway station, Téllez street, train no. 17305

The train that was due to travel from Atocha to Chamartin station was slightly late. The train slowed down to stop at the level of Téllez Street, which runs parallel to the track, about 800 m from Atocha³². Here it was to await the departure of train 17393. At 7.39 a.m. four bombs exploded in carriages: 1, 4, 5 and 6³³. The force of the explosion was so great that many of the 65 dead were thrown outside. Had it not been for the train delay, the casualties could have been many more. 165 people were injured. According to witnesses to the incident, the most surprising thing was the silence and calmness with which the injured passengers, some in very serious condition, disembarked from the destroyed railway cars, helping each other, still without the support of the medical services. The report of the explosion at Atocha station was received by the ambulance service immediately after the explosion. Eight minutes later, the first ambulance arrived. Most of them were sent to Atocha station³⁴.

El Pozo del Tío Raimundo station, train no. 21435

An overcrowded double-decker train from Guadalajara via Alcalá de Henares arrived at the station (Figure 1). It was disembarked by students and schoolchildren and boarded by workers, including many parents who had left their children at nearby kindergartens at that hour. At 7.38 a.m. (7.40 a.m.) the train set off for Alcobendas station, three stops away. It had not yet passed the platform when massive explosions occurred in two railway cars 4 and 5, killing 67 people and injuring 56 - mainly those on the platform. The attack at El Pozo station was the third in a row, which meant that it would take longer to mobilise and direct services. The first call was made at 7.47 a.m. and an ambulance arrived 15 minutes later. Within 1 hour and 10 minutes, all the injured were transported to hospitals³⁵.

³² See: *Atentados Terroristas del Día 11 del Marzo de 2004 de Madrid...*; F. Reinares, *Al-Qaeda's Revenge...*, p. xxiii; Z. Jakubowska, *Madryt 11 marca...*, p. 57, 205.

³³ See: F. Reinares, *Al-Qaeda's Revenge...*, p. xxiii.

³⁴ *The Terror Attacks in Madrid...*, p. 30.

³⁵ *Ibid.*, p. 29.

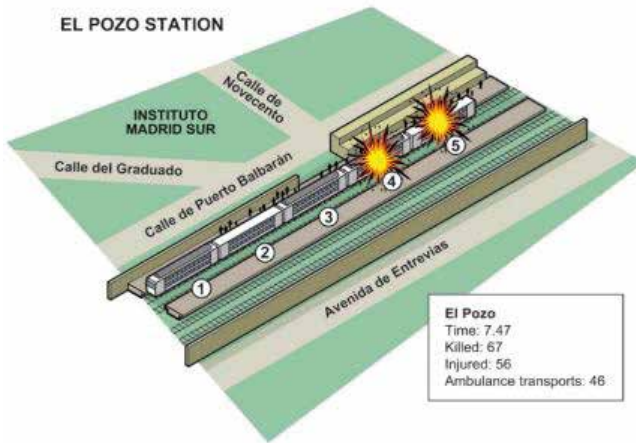


Figure 1. Train no. 21435 at El Pozo del Tío Raimundo station.

Source: *The Terror Attacks in Madrid, Spain, 2004, Kamedo-report 90*, Socialstyrelsen 2007, https://www.socialstyrelsen.se/globalassets/sharepoint-dokument/artikelkatalog/ovrigt/2007-12336_200712336.pdf, p. 30 [accessed: 11 III 2008].

Santa Eugenia station, train no. 21713

At 7.40 a.m. (7.42 a.m.), the last of a series of explosions occurred (Figure 2)³⁶. It happened just as the train was starting from the station. The explosion of material placed in a travel bag caused enormous havoc, as the result of which 17 people were killed and 52 injured. Human remains were scattered within a 50-metre radius. The station buildings were severely damaged³⁷.

³⁶ The explosion on the train at Santa Eugenia station is listed in *The Terror Attacks in Madrid, Spain, 2004, Kamedo-report 90* as second in order, while it occurred at the same time as explosion on the train at El Pozo station or as the last one.

³⁷ *Ibid.*, p. 28.

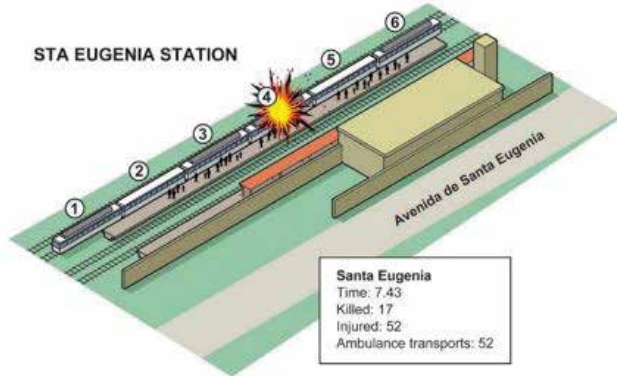


Figure 2. Train no. 21713 at Santa Eugenia station.

Source: *The Terror Attacks in Madrid, Spain, 2004, Kamedo-report 90*, Socialstyrelsen 2007, https://www.socialstyrelsen.se/globalassets/sharepoint-dokument/artikelkatalog/ovrigt/2007-12336_200712336.pdf, p. 29 [accessed: 11 III 2008].

Immediately after the Madrid attack, all forces were mobilised. Field hospitals were set up at the sites of the disaster, medical services appealed for blood donations as supplies were running out at a fast rate. Crowds of people lined up in front of mobile blood donation points. In parallel with the rescue operation, an investigation and anti-terrorist operation code-named 'Cage' ('Jaula') was launched to prevent terrorists from escaping the city. The capital was gripped by traffic paralysis. By 10 a.m. almost all the injured had been taken to around 20 hospitals. More than 300 people were taken to the Gregorio Marañón Hospital, which had never been so busy before. An emergency plan for major disasters had also never been practised, and the situation on the morning of 11 March 2004 even resembled war³⁸. Police delayed publishing the names of those killed. The tragic death toll has finally been made public. More than 6,000 people were travelling on the four trains. The attack left 192 people dead and more than 1,400 injured³⁹. Among the victims from 16 countries were four Poles: two women, a man and his seven-month-old daughter, who died in hospital

³⁸ Z. Jakubowska, *Madryt 11 marca...*, p. 64.

³⁹ The last injured person died in 2014 after being in a coma for ten years. The total number of fatalities was therefore 193 people. See: B. Cedeira, *La víctima que entró en coma el 11M hasta morir 10 años después*, *El Español*, 11 III 2017, https://www.elespanol.com/reportajes/20170310/199730525_0.html [accessed: 11 III 2017].

the day after the attack⁴⁰. The statistics of the wounded were then updated and the final number was 1858⁴¹. It was the second deadliest terrorist attack in Europe after the 21 December 1988 attack on a Pan American airliner over Lockerbie, Scotland, which killed 259 passengers and crew members and 11 residents of that town.

The police investigation discovered that there were more backpacks put on the trains. Of the thirteen, ten bombs exploded. One was found on a train at Atocha station and another in a train at El Pozo del Tío Raimundo station. Both were detonated by sappers from the Regional Operations and Reconnaissance Brigade (Técnico Especialista en Desactivación de Artefactos Explosivos, TEDAX). A third explosive charge was discovered among the luggage carried off the train in El Pozo when a mobile phone rang in one of the backpacks. Specialists defused this bomb. It consisted of a goma-2 eco explosive, screws and nails to increase the explosive force, two detonators and the aforementioned prepaid phone with an alarm programmed for the time when the explosion was supposed to take place. It did not happen because of a defect in the detonator. It was established that the card came from a shop owned by Zugam. The disclosed connections identified a number of terrorists⁴². On the day of the attack, residents of Alcalá de Henares informed the police about a suspicious van parked near the station. It was towed to a police car park. Officers found in it, among other things, seven detonators, remnants of explosive material and a cassette tape with a recorded recitation of a passage from the Koran, a blanket, a scarf and gloves, etc.⁴³

Moments after the attacks, politicians of the ruling party accused the Basque organisation ETA, which allegedly wanted to influence the elections, of carrying them out. Prime Minister Aznar said: *ETA is behind these attacks*⁴⁴. He was echoed by Interior Minister Ángel Acebes,

⁴⁰ *Zmarła czwórka Polaków rannych w Madrycie* (Eng. Four Poles injured in Madrid died), *Gazeta Wyborcza*, 12 III 2004, <https://web.archive.org/web/20091214225052/http://wyborcza.pl/1,75248,1961962.html> [accessed: 12 III 2004].

⁴¹ *Zamachy w Madrycie – odwet za Irak* (Eng. Madrid attacks - retaliation for Iraq), *Polskie Radio*, 11 III 2014, <https://www.polskieradio.pl/106/246/Artykul/1071933%2CZamachy-w-Madrycie---odwet-za-Irak> [accessed: 11 III 2014].

⁴² A. Martín Plaza, *Los atentados del 11M que sacudieron España...*

⁴³ *Atentados Terroristas del Día 11 del Marzo de 2004 de Madrid...*, pp. 147–149.

⁴⁴ M. Catalán, *Prensa, verdad y terrorismo: la lección política del 14-M*, “El Argonauta Español” 2005, no. 2. <https://doi.org/10.4000/argonauta.1191> [accessed: 26 VIII 2023].

who stated: *There is no doubt that ETA is responsible*. In a TV speech at 2.30 p.m., Aznar strongly accused ETA of carrying out the attack. He also announced the holding of a demonstration against Basque separatists the following day. Other PP politicians also pointed without any doubt to ETA as the perpetrator of the attack. The same signals initially came from the secret services, although ETA rejected these accusations⁴⁵. In the evening, the Abu Hafs al-Masri Brigade sent an email to the Arabic-language daily *Al-Quds al-Arabi* ('Arab Jerusalem'), published in London, in which it admitted to having carried out the attacks⁴⁶. At the same time, the police found a videotape at the location indicated by this brigade. It recorded Al-Qaeda's representative in Europe, Abu Dujan al-Afghani, confessing on behalf of the organisation to the attacks carried out exactly two and a half years after 9/11, in response to Spain's collaboration with the 'criminal Bush'. This was supposed to be retaliation for the evils perpetrated in the world by the West, especially in Iraq and Afghanistan⁴⁷.

On Saturday 13 March, the three co-owners of the Nuevo Siglo phone shop, from which the cellphones converted into incendiaries came, were arrested. Intelligence agents also managed to locate the terrorists' hideout in a rented flat in the Leganés district. This was helped by mobile phone cards and a pre-paid card found on 2 April in a bag of explosives placed on the tracks of the high-speed railway (Alta Velocidad Española, AVE). The following day, police officers and officers of the Special Operations Group (Grupo Especial de Operaciones, GEO) proceeded to lay siege to the building where the terrorists' headquarters were located. The start of the operation and the conflicting information about how it was going to be carried out caused much controversy. At around 6 p.m., one of the terrorists went outside to throw rubbish away. He saw the police officers, after which

⁴⁵ Ibid.

⁴⁶ The organisation is named after Muhammad Atef aka Abu Hafs al-Masri, one of Bin Laden's closest associates and an activist of the Egyptian Islamic Jihad (Al-Jihad al-Islami al-Misri). The brigade made itself known again on 17 March 2004, declaring a ceasefire in Spain if the new government fulfilled its promise and withdrew troops from Iraq. By the way, it called Aznar the 'tail of the United States', which had been 'consigned to the dustbin of history'. The same organisation took responsibility for the attacks in Istanbul in November 2003 and London in July 2005. It also published dozens of proclamations, statements and communiqués. However, it turned out that the brigade existed only in the virtual sphere. See: K. Izak, *Leksykon organizacji i ruchów islamistycznych...*, p. 413.

⁴⁷ Z. Jakubowska, *Madryt 11 marca...*, p. 82.

he warned his colleagues and fled⁴⁸. According to another version of events, he fled without warning his comrades, who themselves saw the policemen nearby⁴⁹. The terrorists then opened fire through the window, raising shouts in Spanish in praise of Allah. After the residents were evacuated, it was decided that a group of GEO officers would blast the door to the flat and throw tear gas inside. When the anti-terrorists were in the stairwell next to the flat, a naked man stood at the front door. At this point, a massive explosion occurred, killing one officer and injuring 15 others, several seriously. A large part of the building's facade was destroyed. The force of the explosion of the explosives stored in the flat was so great that it was impossible to count the number of massacred bodies of the terrorists who committed collective suicide. It was first reported that four of them had died. Only after three days was it established that there were seven⁵⁰. They were the same terrorists who had planted bombs on the trains at Alcalá de Henares station.

Political impact of the events of 11 March 2004

The Madrid attacks took place three days before the general elections. In the event that ETA had actually carried out the attack, the electorate would certainly have supported the party of Aznar, who pursued a policy of dealing tough with Basque terrorists and rejected any possibility of negotiating with them. With Aznar having already declared that he would not seek re-election as prime minister, the PP therefore chose Mariano Rajoy as its leader in the election campaign. However, if the attack in Madrid had been carried out by Islamic extremists, the situation could have changed dramatically, as 80% of the public was against sending Spanish soldiers to Iraq. Surely PSOE politicians would have used this fact to discredit

⁴⁸ Ibid., p. 130.

⁴⁹ *Los terroristas del 11-M se inmolan y matan a un geo al volar su «piso franco» en Leganés*, ABC España, 4 IV 2004, https://www.abc.es/espana/abci-terroristas-inmolan-y-matan-volar-piso-franco-leganes-200404040300-962802830594_noticia.html [accessed: 4 IV 2004].

⁵⁰ Z. Jakubowska, *Madryt 11 marca...*, p. 82; R. Becares, O. Cernuda, *Cuatro terroristas islámicos se inmolan en un piso de Leganés y matan a un agente de policía*, elmundo.es, 4 IV 2004, <https://www.elmundo.es/elmundo/2004/04/03/enespecial/1081016920.html> [accessed: 4 IV 2004]; *La policía eleva a siete los terroristas muertos en Leganés*, Cadenaser, 7 IV 2004, https://cadenaser.com/ser/2004/04/07/espana/1081295423_850215.html [accessed: 7 IV 2004].

the current government. For this reason, Aznar and Acebes kept accusing ETA of carrying out the attack, even though the facts revealed in the hours that followed contradicted this. The analysis of the material evidence examined by forensic experts forced at least restraint in the statements made by politicians from people's party. Meanwhile, on 11 March, at around 9.30 p.m., Zapatero telephoned the editor-in-chief of the daily 'El Mundo' and informed him that, in view of the new evidence, he was convinced of Al-Qaeda's guilt and, moreover, according to him, the government also had this knowledge. While the opposition disputed the words of members of the right-wing government the following day, ETA representatives spoke out. An anonymous caller telephoned the editorial board of the extreme nationalist daily 'Gara', declaring that the Basque organisation bore no responsibility for Thursday's attacks. A dozen minutes later, Acebes, on behalf of the government, announced that he did not believe in the authenticity of this information. On Friday evening, some 11 million Spaniards, including some 2.3 million in Madrid alone, took part in demonstrations against ETA's violence, and as an expression of remembrance for the victims and support for their families. This show of unity was disrupted when the police investigation began to focus on Al-Qaeda. On Saturday 13 March, when the first arrests of Islamic radicals connected to the attack took place, the government spokesman and interior minister continued to blame ETA. Faced with the contradiction of emerging new evidence with statements by government representatives, the opposition decided to act despite the electoral silence in force. The pre-election ban on agitation was broken by the shouts of the crowd that gathered at the PP headquarters in Madrid. Residents demanded to know the truth before taking part in the elections. Anti-government protests also erupted in Barcelona and other major Spanish cities. That same evening and night there was a battle of words between the PP and the PSOE, which accused the government of lying during an ongoing investigation⁵¹.

On 14 March, the Left won with 11 million votes, while the PP won 9.7 million. Participation in the general election was 77.26%, one

⁵¹ J. Cieszko, *Tragedia w Madrycie, 11-14 marca 2004 roku* (Eng. Tragedy in Madrid, 11-14 March 2004), in: *Hiszpania: Media masowe i wybory w obliczu terroryzmu* (Eng. Spain: Mass media and elections in the face of terrorism), B. Dobek-Ostrowska, M. Kuś (eds.), Wrocław 2007, pp. 51-54; J.L. Gonzalez Esteban, *Kronika 11 marca: terroryzm i polityczna zmiana w Hiszpanii* (Eng. Chronicle 11 March: terrorism and political change in Spain), in: *Hiszpania: Media masowe i wybory...*, pp. 67-70.

of the highest in Spain⁵². The following day, after announcing the Socialists' victory, Zapatero announced that he intended to invite the other political parties to a dialogue on the fight against terrorism. He also announced a return to an alliance with France and Germany, i.e. pursuing a pro-European policy instead of the pro-American policy of the previous government. He announced that his first step would be to withdraw troops from Iraq. He called the war against the Hussein regime a mistake because no weapons of mass destruction had been found in Iraq. In addition, it had emerged that secret service reports had been manipulated in the U.S. and Britain to lend credence to the need to intervene. Spain's new Prime Minister also said that his victory in the vote is a signal of change for other countries with elections coming up soon, including the United States, where President George W. Bush will face Massachusetts Senator John Kerry in November. If voters do not accept the war in Iraq and its occupation, they can protest at the polls and at the ballot box, thus changing the direction of policy. The final decision to withdraw the Spanish contingent was taken on 19 April 2004⁵³.

In May 2004, 1,300 Spanish soldiers left Iraq⁵⁴. Soldiers from the Dominican Republic and Honduras also returned to the country. In the summer of 2004, MND C-S of 9,000 soldiers commanded by Poles was reduced to about 7,000. Although their presence in Iraq did not have any significant military importance, the end of the mission was perceived as a gesture of a political nature, a consequence of the reorientation of Spain's position, in which the new government clearly distanced itself from the tactics of the war on terror preached by the USA⁵⁵. The international media reported at the time that the Spanish had failed. The Polish Ministry of Defence hoped that the Spaniards would take command in the zone. Poland's Prime Minister at the time, Leszek Miller, appealed to the Spanish for loyalty to the international anti-terrorist coalition, but to no avail⁵⁶.

⁵² J. Cieszko, *Tragedia w Madrycie...*, pp. 56–57.

⁵³ A. Martin Plaza, *Los atentados del 11M que sacudieron España...*; J. Cieszko, *Tragedia w Madrycie...*, pp. 54–55.

⁵⁴ M. Brylew, *Irak 2006–2012...*, p. 50.

⁵⁵ The Spanish contingent, on the other hand, remained in Afghanistan. Indeed, Zapatero expressed his belief that the two interventions were fundamentally different in their rationale and legality.

⁵⁶ *Po pięciu latach koniec polskiej misji w Iraku* (Eng. After five years, the end of the Polish mission in Iraq), money.pl, 29 X 2008, https://www.money.pl/archiwum/wiadomosci_agencyjne/pap/

The stance of the new Spanish government was severely criticised by Washington and other capitals. The Bush administration did not hide its anger at Zapatero, comparing the current situation with the signing of the Munich Agreement in 1938. At that time, to calm the situation, France and the United Kingdom agreed to annex part of Czechoslovakia's territory to Germany. Spain has now acted in a similar way, withdrawing its military contingent from Iraq in an attempt to 'calm' the terrorists. There were malicious comments in the Polish media that the elections in Spain had been won by Al-Qaida⁵⁷. The events of 11 March and their consequences have had an impact on both general international relations and bilateral relations between Spain and the United States. The change of government in Spain was not welcomed by the Bush administration. During a visit to EU countries, the then chairwoman of the U.S. National Security Council, Condoleezza Rice, ignored Madrid. She did not stay there, recognising that she would hear nothing in Madrid that she could not hear in Paris. The attacks in the Spanish capital were used by President Bush during the 2004 election campaign. He used them to justify the need to continue his military policy in Iraq and to maintain the restrictions on the civil liberties of the U.S. population. He further pointed out that terrorism was indeed the greatest threat to the world and that pursuing this policy was therefore a priority in his foreign policy⁵⁸. Another consequence of the Madrid events of international significance was the adoption of a declaration on combating terrorism by the European Council in March 2004. Two months later, the post of EU Counter-Terrorism Coordinator was created.

artykul/po;pieciu;latach;koniec;polskiej;misji;w;iraku,188,0,381372.html [accessed: 29 X 2008]. In autumn 2014, the Spanish Ministry of Defence decided to send 300 soldiers to Iraq. This time they supported the international coalition in the fight against the Islamic State. They trained the Iraqi military in carrying out special operations and in detecting and defusing mines. The Spaniards did not take an active part in the fighting, but had to resist attacks. See: *Hiszpański parlament zgodził się na wysłanie żołnierzy do Iraku* (Eng. Spanish parliament agrees to send troops to Iraq), Wirtualna Polska, 22 X 2014, <https://wiadomosci.wp.pl/hiszpanski-parlament-zgodzil-sie-na-wyslanie-zolnierzy-do-iraku-6027730872366209a> [accessed: 22 X 2014].

⁵⁷ B. Łódzki, *Reakcja polskich mediów masowych na atak terrorystyczny w Madrycie 11 marca 2004 r.* (Eng. Reaction of the Polish mass media to the terrorist attack in Madrid on 11 March 2004), in: *Hiszpania: Media masowe i wybory w obliczu terroryzmu* (Eng. Spain: Mass media and elections in the face of terrorism), B. Dobek-Ostrowska, M. Kuś (eds.), Wrocław 2007, p. 126.

⁵⁸ T. Płudowski, *Reakcje prasy amerykańskiej na madrycki atak terrorystyczny z 11 marca 2004* (Eng. U.S. press reactions to the Madrid terrorist attack of 11 March 2004), in: *Hiszpania: Media masowe i wybory w obliczu terroryzmu* (Eng. Spain: Mass media and elections in the face of terrorism), B. Dobek-Ostrowska, M. Kuś (eds.), Wrocław 2007, pp. 156–157.

Conviction of the perpetrators of the Madrid attack

On 14 March 2005 Al-Qaeda claimed responsibility for the Madrid attack. A speaker presenting himself as the spokesman for Al-Qaeda in Europe declared that the attacks were revenge for (...) *Spain's collaboration with the criminal Bush and his allies*⁵⁹. This information did not provoke much of a public reaction, as the investigation showed that Bin Laden's organisation was responsible for the attack anyway. The political and social debate surrounding the events in Madrid resurfaced in 2007 following the controversial sentences handed down to the organisers and helpers of the terrorist attack. There were 21 people, most of them Moroccans, directly involved in preparation and realisation of the attack. The trial lasted from 15 February to 2 July 2007. Fifteen Moroccans, nine Spaniards, two Syrians, an Algerian, a Lebanese and an Egyptian stood trial. The verdict was read out on 31 October 2007 - 21 of the 29 accused of involvement in the attacks, none of whom pleaded guilty, were sentenced to more than 40,000 years in prison. Eight were acquitted by the court. The same case also names 28 defendants, seven of whom were acquitted. Among them was Al-Masri, considered by some authors to be the instigator of the Madrid attacks. In 2004, he was detained in Milan after police overheard his conversation in which he admitted to planning the Madrid attack. Muhammad the Egyptian was also acquitted, which was twistedly explained by the fact that he was already serving a 10-year prison sentence (reduced to eight) in Italy for belonging to a terrorist organisation. Another organiser of the attack, Al-Haski, who was also the head of the Spanish cell of the Moroccan Islamic Combatant Group, was sentenced to 15 years in prison instead of the more than 40,000 the prosecutor had demanded. The heaviest sentences were handed down to Zugam and Al-Ghanut: 30 years for each of the 191 killed, 20 years for each of the 1,858 wounded (attempted murder) and 12 years for membership of a terrorist organisation. Also among those sentenced was Trashorras, who was charged with complicity in the events by selling explosives to Islamic terrorists. His sentence is 34,715 years in prison. However, under the Spanish legal system, none of the convicts will serve more than 40 years in prison. The remaining defendants received sentences ranging from 3 to 23 years

⁵⁹ A. Mroczek, *Zamach w Madrycie 11 III 2004 - minuta po minucie* (Eng. Madrid attack 11 III 2004 - minute by minute), *terroryzm.com*, 25 IX 2005, <http://www.terroryzm.com/zamach-w-madrycie-11-iii-2004-minuta-po-minucie/> [accessed: 25 IX 2005].

in prison. The public prosecutor's office and associations of the victims' relatives appealed the sentences to the Supreme Court, which upheld most of them in a ruling on 17 July 2008. The public, and above all the families of the victims of the attacks, received the verdicts, especially the lowest and acquittal ones, with incredulity, indignation and anger⁶⁰. Spaniards found it difficult to accept that the massacre was committed by Muslims who lived in Madrid, worked here and were often friends with the local community. Politicians of the ruling PSOE were unlikely to comment on the verdict. Instead, they continued to accuse the previous right-wing government of trying to hide the truth about the real perpetrators of the attack and blame it on ETA, lest Spaniards think that the attack was retaliation for sending Spanish troops to Iraq⁶¹.

Anti-terrorist security problems in Spain

With the results of the ongoing investigation, questions and doubts were raised not only about the perpetrators of the attack, but also about the state of anti-terrorist security in Spain. An attack motivated by jihadist ideology took place in a country that fought against Basque separatist terrorism between 1960 and 2011. On the one hand, praise was expressed for the efficiency and professionalism of the emergency medical services and experts in forensic science and medicine. On the other hand, the investigation revealed a number of errors and omissions related to the surveillance of the most radicalised individuals and the handling of informants by the police and the Civil Guard. As many as five informants of these services were among the group of people linked to the attack. The police rejected, for example, the information provided by one of them that it was not ETA that carried out the attack, because it went against

⁶⁰ M. Tryc-Ostrowska, *Kontrowersyjny wyrok za zamachy w Madrycie* (Eng. Controversial sentence for Madrid attacks), "Rzeczpospolita", 2 XI 2007.

⁶¹ C. Taracha, *Wybory w cieniu zamachu. Kilka uwag na temat wydarzeń z marca 2004 roku w Madrycie* (Eng. Elections in the shadow of an attack. Some comments on the events of March 2004 in Madrid), in: *Terroryzm wczoraj i dziś. Wybrane problemy* (Eng. Terrorism yesterday and today. Selected issues), P. de la Fuente, W. Gizicki, C. Taracha (eds.), Lublin 2015, p. 80; *El final del principio en la investigación del 11-M*, elmundo.es, 1 XI 2007, <https://www.elmundo.es/elmundo/2007/11/01/espana/1193885319.html> [accessed: 1 XI 2007]; M. Tryc-Ostrowska, *Kontrowersyjny wyrok...*

the political line⁶². Also, the trial left many questions and doubts about both the authorship of the attack as well as its perpetrators and originators. Not surprisingly, this hot topic became the subject of scholarly and journalistic consideration. Various interpretations and speculations about the events of 11 March 2004 have reached the public. The author of the official conception accepted by Spain's ruling political establishment and much of the public is Reinales. Also accepted was the opinion of Luis del Pino, who saw traces of the presence of the secret services in the attacks, without identifying them specifically⁶³.

In order to increase effectiveness in the fight against domestic and international terrorism, two months after the attacks, Spain's National Counter Terrorism Coordination Centre (Centro Nacional de Coordinación Antiterrorista, CNCA) was created. In Poland, its counterpart is the Counter-Terrorism Centre of the Internal Security Agency. It was made up of top officers from the National Police Corps (Cuerpo Nacional de Policía, CNP), the Citizen Guard, the CNI and prisons. The National Counter Terrorism Coordination Centre fell under the Secretary of State for Security at the Ministry of the Interior (MIA). The CNCA's departments dealing with Islamic terrorism and Muslim radicalism included many specialists. It was an institution of an analytical nature. The primary objective of the CNCA was to receive, process and evaluate available strategic information on all types of terrorism that posed a threat to Spain, without taking operational action, which was the responsibility of the State Security Forces and Bodies (Fuerzas y Cuerpos de Seguridad del Estado, FCSE). The FCSE comprised intelligence, the police, the Civil Guard and the Catalan police Mossos d'Esquadra. The new counter-terrorism institution constantly updated its assessment of the terrorist threat, sought to maintain the initiative in the fight against terrorists, choose the best scenarios for possible intervention and plan the response. Legislative changes were introduced. Modification and expansion of the terrorist prevention system was initiated, including the improvement of the rapid reaction force and the use of the military. EU intelligence cooperation with the U.S. and Muslim countries strengthened⁶⁴.

⁶² Z. Jakubowska, *Madryt 11 marca...*, pp. 173–175.

⁶³ C. Taracha, *Wybory w cieniu zamachu...*, pp. 81–85.

⁶⁴ *Centro Nacional de Coordinación Antiterrorista CNCA*, La Pagina de ASR, <https://intelpage.info/centro-nacional-de-coordinacion-antiterrorista.html> [accessed: 12 XII 2015].

The rise of the Al-Qaeda organisation in the Islamic Maghreb Countries (Tanzim Al-Qaida fi Bilad al-Maghrib al-Islami) in 2007 saw an increase in the terrorist threat in Spain. The organisation's online media organ 'Al-Andalus' proclaimed, among other things, that its aim was to recruit supporters under the banner of fighting for a caliphate in the Iberian Peninsula. Statements and propaganda material posted on the portal contributed to the radicalisation of Spanish Muslims. Bin Laden's deputy in Al-Qaeda, Ayman az-Zawahiri, called for (...) *the recapture of Al-Andalus, which is the duty of our people in general and of you* (the Maghreb countries – author's note) *in particular. This objective can only be achieved by ridding the Islamic Maghreb of the sons of France and Spain*⁶⁵. Spain also held a special place in the ideology of the Islamic State, by which it was seen as a natural part of the caliphate now occupied by the 'infidels'. To minimise the growing threat, the number of officers dealing with Muslim extremism was increased. More Arabic language translators have been employed at the CNCA. There were 11 of them in April 2004⁶⁶ and 86 in November 2007. There have been many operations during which local radicals and immigrants from North Africa and the Middle East have been arrested. They arrived in Spain and were prosecuted for terrorism in their home countries. In addition, a number of terrorist cells with international links were broken up, including the cell preparing the attack on the Supreme Court in Madrid (October 2004). There was a real threat emanating from the activity of radicals in prisons, who sought to recruit Muslims there to carry out terrorist activities after leaving prison. The police operation code-named 'NOVA' was intended to counter these tendencies. After the Madrid attacks, much Muslim extremist activity was concentrated in Catalonia. By 2009, 14 anti-terrorist operations had been carried out there, most of them in and around Barcelona, including 'Tiger' ('Tigris'), 'Jackal' ('Chacal') or 'Chameleon' ('Camaleon')⁶⁷. In its 10 years of activity, the CNCA carried out more than 50 operations in Spain against international terrorist structures and loose cells without wider organisational links. During this time, more than 500 people were arrested, but only 14% of them were convicted,

⁶⁵ K. Izak, *Leksykon organizacji i ruchów islamistycznych...*, p. 469.

⁶⁶ S. Kosmyńska, *Święta wojna w Al-Andalus. Przeobrażenia aktywności dżihadystycznych komórek terrorystycznych w Hiszpanii w latach 1995–2012* (Eng. *The Holy War in Al-Andalus. The transformation of jihadist terrorist cell activity in Spain between 1995 and 2012*), Łódź 2015, p. 304.

⁶⁷ *Ibid.*, p. 259, 262.

the rest were released for lack of evidence⁶⁸. The authorities did, however, allow Islamic radicals to hold meetings attended by several thousand people each. At least 10 Salafist congresses were held in Spain in 2010, attended by between 2,000 and 3,000 people. Two years earlier, only one such congress had been held⁶⁹. The policy of multiculturalism, tolerating and even supporting the activities of religious minorities, promoted by the authorities, who downplayed the funding of organisations, mosques and Muslim centres from abroad, clashed with the actions of the secret services, which had increasing problems with the surveillance of radical circles.

Following ETA's announcement in 2011 that it had ceased its armed activities, the special services focused on countering Islamic terrorism and countering Muslim extremism, which correlated in time with the creation of a new jihadist battle front in Iraq and Syria. As the threat from terrorists linked to the Islamic State increased in mid-October 2014 the CNCA was merged with the Intelligence Centre against Organised Crime (Centro de Inteligencia contra el Crimen Organizado, CICO) to form the Intelligence Centre against Terrorism and Organised Crime (Centro de Inteligencia contra el Terrorismo y el Crimen Organizad, CITCO). The aim of the merger was to optimise efforts and make better use of the economic resources of both agencies in the face of growing threats and links between extremists, terrorist organisations and organised crime. In addition to the already mentioned activities carried out by the CNCA, CITCO's tasks include providing the FCSE with relevant information and forecasts, coordinating their activities, drawing up annual reports on organised crime, terrorism and radicalism in Spain and periodically assessing the threat in these areas. It is the responsibility of the CITCO to compile and distribute statistics related to the above matters, as well as to liaise with the relevant institutions in Brussels and similar bodies in EU member states. A special team has been created to monitor online activities. It was on the web that 80% of jihadists were recruited to take part in the fighting in Iraq and Syria. It has also embarked on a programme of deradicalisation of communities of young Muslims⁷⁰.

⁶⁸ Ibid., p. 310.

⁶⁹ J. Loredo, *Marzenie o Al Andalus* (Eng. The dream of Al-Andalus), "Nasz Dziennik", 19 XI 2011.

⁷⁰ *Interior cesa al jefe del CITCO y nombra a un comisario al frente del Gabinete de Estudios y Coordinación*, elDiario.es, 7 VII 2018, https://www.eldiario.es/politica/interior-citco-gabinete-estudios-coordinacion_1_2035094.html [accessed: 7 VII 2018].

The aim of the Spanish services was to intervene at the earliest possible stage to prevent attacks. In the case of Islamist terrorists, this was successful for 13 years (with varying degrees of success in the case of ETA, which last carried out an attack in 2009). A 2016 report by the Spanish Interior Ministry noted that the number of messages sent by jihadists calling on so-called ‘lone wolves’ to carry out attacks on Spain and to ‘liberate’ cities such as Toledo, Córdoba and Seville had doubled compared to previous years⁷¹. It became obvious that the jihadists would seek to carry out further attacks. Catalonia was a realistic target. As early as October 2007, the CIA handed over a report to the authorities in Madrid, which showed that the autonomous region of Catalonia had turned into an operational and recruitment base for terrorists. There were even alarming claims that Catalonia had become the new centre of global jihad⁷². It should not be forgotten that the Islamic State’s call for all terrorist activities in Europe found fertile ground in Spain, where the influx of illegal immigrants from Africa had increased and local Muslims were becoming heavily radicalised. When in 2016 the EU concluded an agreement with Turkey on the return of illegal migrants, migrant routes from Libya and Tunisia to Italy and from Morocco through the Strait of Gibraltar to Spain became important. Nevertheless, the Spanish service has been recognised as one of the most effective in Europe when it comes to detecting terrorists, and Spanish counter-terrorism experts have become known as the best in the world. In recognition of their merits, a meeting of the UN Counter-Terrorism Committee was held in Madrid in July 2015⁷³. This image was not spoiled by the attack in Barcelona two years later.

On 17 and 18 August 2017 Catalonia became the target of attacks by jihadists from Ripoll. At the time, 16 people were killed and 128 injured⁷⁴.

⁷¹ J. Badcock, *The Long Shadow of al-Andalus. Spain is on the periphery of Europe, but central to modern jihad*, Foreign Policy, 21 VIII 2017, <https://foreignpolicy.com/2017/08/21/the-long-shadow-of-al-andalus-spain-islamic-state-terrorism-al-qaeda/> [accessed: 21 VIII 2017].

⁷² K. Haahr, *The Growth of Militant Islamist Micro-Diaspora Communities*, “CTC Sentinel” 2008, vol. 1, no. 4, <https://ctc.westpoint.edu/wp-content/uploads/2010/06/Vol1Iss4-Art6.pdf> [accessed: 18 IV 2008].

⁷³ *Madryt: posiedzenie Komitetu Antyterrorystycznego ONZ* (Eng. Madrid: meeting of the UN Counter-Terrorism Committee), Dziennik Gazeta Prawna, 27 VII 2015, <https://www.gazetaprawna.pl/wiadomosci/artykuly/885271,madryt-posiedzenie-komitetu-antyterrorystycznego-onz.html> [accessed: 27 VII 2015].

⁷⁴ *Hiszpania: Rozpoczął się proces dżihadysty zatrzymanego w Warszawie* (Eng. Spain: Trial of jihadist detained in Warsaw begins), Dziennik Gazeta Prawna, 11 VI 2018,

In addition, seven terrorists were killed by the police during or shortly after the attacks and three were brought to justice. The terrorists attacked in Barcelona and Cambrils using cars and knives. They intended the attack to take a very different course. The change of plans was prompted by an explosion at the terrorists' base in Alcanar, which killed the radical imam Abdelbaki (Abdel Baki) As-Satty, the initiator of the attack, and the terrorist preparing the explosive⁷⁵. One of the terrorists was wounded. The investigation revealed that the original plan of the bombers was to place 200 kg of an explosive made from triacetone triperoxide (TATP), also known as the mother of Satan, in the van, laden with gas cylinders to increase the force of the explosion. The target was probably the Sagrada Familia. Many opinions expressed the thesis that the attack could have been thwarted if it had not been for the arrogance of the Catalan authorities, who disregarded warnings and sabotaged cooperation with the state's security forces by refusing to provide Madrid with vital information about the jihadists⁷⁶. They have also refused to erect concrete barriers at the entrance to the La Rambla promenade to prevent cars from entering it. This is where the speeding car killed the most people. The safety of Barcelona's residents and tourists has been subordinated to local politicians, who have committed numerous omissions in the name of Catalonia's policy of independence from Spain, one element of which

<https://www.gazetaprawna.pl/wiadomosci/artykuly/1132741,proces-dzihadysty-zatrzymanego-w-warszawie.html> [accessed: 11 VI 2018].

⁷⁵ Abdelbaki As-Satty was a Moroccan national. In 2014, a court ordered his expulsion from Spain, shortly after he had finished serving his sentence for drug trafficking. Despite this decision, As-Satty remained in Spain; moreover, in 2015, a higher court ordered his expulsion to be revoked. He was therefore able to stay in Spain legally. He settled in the Catalan town of Ripoll, where he preached radical sermons, taught and recruited to fight on the side of the Islamic State in Iraq and Syria at a local mosque until June 2017. He himself was recruited while in prison, where he met Rashid Aglif, serving a sentence for complicity in the Madrid attacks of 11 March 2004. This shows the shortcomings of the preventive work of the penitentiary service, above all the insufficient control of the relationships that convicts established in prisons. The system was sealed in autumn 2018. See: J. Dziedzina, *Imam kazał zabijać* (Eng. Imam ordered to kill), *gość.pl*, 7 IX 2017, <https://www.gosc.pl/doc/4166327.Imam-kazal-zabijac> [accessed: 7 IX 2017].

⁷⁶ *Zamachy terrorystyczne w Hiszpanii. Można było im zapobiec* (Eng. Terrorist attacks in Spain. They could have been prevented), *Magazyn TVN24*, <https://archiwum.tvn24.pl/magazyn-tvn24/114/tvn24.pl/magazyn-tvn24/willa-na-uboczu-matka-szatana-i-plan-a-zamach-na-niespotykana-skale,114,2082.html> [accessed: 22 VIII 2017].

was to rally Muslim sympathies ahead of the secession referendum on 1 October 2017⁷⁷.

A week after the events in Catalonia, the Islamic State has claimed responsibility for the attack and warned of more attacks. In a publicised video, Muhammad Jasin Ahram Pérez, a Spanish citizen who travelled to Syria in 2014, threatened: *Spanish Christians, do not forget the Muslim blood that was shed and the Spanish Inquisition. We will avenge the massacres you have carried out and those you are carrying out now against the Islamic State. Al-Andalus will once again be what it was, the land of the caliphate*⁷⁸. Faced with new challenges, Spain's then Deputy Prime Minister Soraya Sáenz de Santamaria gave the CNI an additional €20 million for counter-terrorism activities and the hiring of 600 new agents. Legal reforms were introduced in the justice system that made it easier to bring suspects to justice. Until now, they could be detained, questioned and, if insufficient evidence was found of the suspects' guilt, they had to be released⁷⁹. Following the Barcelona terrorist attack, the Spanish services supported by the CNI conducted an eighteen-month covert operation codenamed 'Alexandra'. It culminated in the arrest of 17 people in January 2019. Among them were five Algerian, Libyan and Iraqi nationals. They were accused of belonging to the Islamic State. In addition, operations 'Minerva' and 'Neptune' were carried out to track the travel routes of terrorists returning from the combat zones in Iraq and Syria after the fall of the Islamic State. They usually arrived in Spain mixed in with groups of African migrants, crossing the Strait of Gibraltar in boats. It also emerged that the prisoner deradicalisation programme introduced in 2014 was ineffective. Two years after its introduction, the number of Muslim radicals in Spanish prisons was almost 100, double the number before the programme began. In October 2018, it was revealed that a total of 25 people in 17 prisons housing Islamic extremists were involved in the radicalisation process, including some convicted of the Madrid attack in March 2004, including

⁷⁷ K. Izak, *Sieć ekstremistów religijnych i politycznych. Sojusznicy i wrogowie* (Eng. A network of religious and political extremists. Allies and enemies), "The Internal Security Review" 2019, no. 21, p. 107; *Zamachy terrorystyczne w Hiszpanii...*

⁷⁸ J. Martin-Arroyo, *El Cordobés, the Spanish face of Islamic State*, El País, 25 VIII 2017, https://english.elpais.com/elpais/2017/08/25/inenglish/1503659430_853709.html [accessed: 25 VIII 2017].

⁷⁹ T. Skowronek, *Hiszpania walczy ze światowym terroryzmem* (Eng. Spain fights global terrorism), "Przegląd" 2019, no. 46, p. 29.

Al-Haski. Of this group, as many as 21 were in solitary confinement. Despite this, they carried out their propaganda activities by means of letters handed over to other prisoners on their way out, and with the participation of their family members. In February 2018, the Spanish government launched a new programme to counter the radicalisation of prisoners. As part of its implementation, all officers in prison were required to observe the behaviour of inmates who profess Islam on a daily basis, as well as those deemed susceptible to radicalisation. There were a total of 140 jihadists in 28 prisons in October 2018, some of whom are already at large⁸⁰.

The year 2018 was critical for Spanish services due to the unprecedented number of irregular migrants who arrived from Morocco, crossing the Strait of Gibraltar. More than 57,500 migrants out of a total of more than 64,000 arrived through this route at the time, more than a fourfold increase compared to 2017⁸¹. For the most part, they did not have any identity documents in order to hinder possible extradition. The phenomenon of illegal migration to Spain is accompanied by the trafficking of false documents and identity theft. Spain is at the forefront of EU countries in this practice⁸². This crime enables immigrants to legalise their stay with a false identity, which poses an additional challenge for the secret services. Among others, Abdel-Majed Abdel Bary, known as the Islamic State rapper, who has posted numerous threats against Western countries on social media, has reached Spain via this route⁸³.

Moroccan authorities are using the migratory pressure on Spain's borders for political and economic purposes, making further demands and demanding concessions from Madrid. On 22 May 2021, Rabat authorities

⁸⁰ A. Kłos, *Fikcja walki z radykalizmem* (Eng. The fiction of the fight against radicalism), "Gazeta Polska Codziennie", 13 X 2018; "El Mundo": *zamachowcy z Madrytu radykalizowali młodych muzułmanów w więzieniach* (Eng. 'El Mundo': Madrid bombers radicalised young Muslims in prison), TVN24, 11 X 2018, <https://tvn24.pl/swiat/zamachowcy-z-madrytu-radykalizowali-młodych-muzułmanow-w-wiezieniach-ra875396-2384538> [accessed: 11 X 2018].

⁸¹ K. Izak, *Hiszpania i Francja walczą z nielegalną imigracją i fałszerstwami dokumentów* (Eng. Spain and France fight illegal immigration and document forgery), "Człowiek i Dokumenty" 2021, no. 62, p. 68.

⁸² *Ibid.*, p. 69.

⁸³ K. Izak, *Oryginalne paszporty w rękach terrorystów i oszustów* (Eng. Original passports in the hands of terrorists and fraudsters), "Człowiek i Dokumenty" 2019, no. 54, p. 51; J. Wójcik, "Raper ISIS" wrócił do Europy po azyl (Eng. "ISIS rapper" returned to Europe for asylum), euroislam.pl, 20 V 2020, <https://euroislam.pl/rapper-isis-do-europy-powrocil-jako-szukajacy-azyłu/> [accessed: 20 V 2020].

called on Spain to launch an investigation into the arrival of seventy-three-year-old Brahim Ghali, leader of the Polisario Front, for medical treatment in the country. Madrid's decision to admit Ghali without informing Rabat strained relations between the two countries and caused Moroccan border guards to loosen their border protection. This has encouraged migrants camped at the border to cross it. Within 35 hours, more than 8,000 migrants, including more than 2,000 minors, had arrived in Ceuta, a Spanish enclave in Morocco⁸⁴.

Between 2020 and 2027, the EU will pay Rabat €3.5 billion to stop its own citizens from crossing Morocco's land and sea borders with Spain. It follows that the agreement does not cover migrants from other African countries who continue to push across the Spanish border⁸⁵. Their destination is also the Canary Islands. In 2020, 23,000 migrants arrived here, ten times more than the previous year. This direction is also being exploited by Rabat, loosening control of the coast. The aim is to get Spain to recognise Moroccan sovereignty over the Western Sahara and gain the greatest access to the underwater deposits of tellurite, a rare semi-metal ore found off the coast of the Canary Islands⁸⁶.

Another factor negatively affecting security in Spain is the situation in Catalonia, where separatist aspirations continue unabated. In October, violent demonstrations are held there to mark the anniversary of the 2017 independence referendum. In 2019, the anniversary demonstration in Barcelona turned into violent riots and a general strike in Catalonia, infringing the politics of the region and Spain as a whole as never before. It should be noted that the Catalan authorities, home to 1/4 of Spain's total Muslim population, have their own migration policy.

Between 2019 and 2023, Spanish services managed to foil several major attacks, including during a Catholic procession in Seville in April 2019. Several terrorist incidents were also reported, including in January 2023. A Moroccan man attacked people in two churches in Algeciras. One

⁸⁴ K. Izak, *Migranci jako element nacisku w stosunkach międzynarodowych. Dokumenty dowodem przestępczej działalności państw* (Eng. Migrants as an element of pressure in international relations. Documents evidence of criminal activities of states), "Człowiek i Dokumenty" 2021, no. 63, p. 59.

⁸⁵ Ibid.

⁸⁶ G. Lindenberg, *Czy Maroko gra z Hiszpanią imigrantami?* (Eng. Is Morocco playing migrants with Spain?), euroislam.pl, 14 II 2021, <https://euroislam.pl/czy-maroko-gra-z-hiszpania-imigrantami/> [accessed: 14 II 2021].

person was killed and four were injured. The perpetrator was arrested as he entered a third church. In contrast, 11 people were injured in Madrid in August 2023, following an attack by unidentified assailants armed with knives. Spain currently has a terrorist threat level four on a five-step scale. Madrid has not changed its threat level since 2015 after the terrorist attacks in Paris⁸⁷.

Summary

Twenty years after the terrorist attack in Madrid, Spain is struggling with illegal immigration of people from Africa, nationalist movements and Islamic extremism and terrorism. The author does not find a clear answer to the question of whether the country has become more secure since 2004. One might think so, given the closure of the terrorist activities of the Basque separatists of ETA and the self-dissolution of that organisation, as well as after the successes of the Spanish services in eliminating further terrorist cells and arresting extremists. Behind these achievements of the counter-terrorism services, however, there are large numbers of arrests, which cannot give cause for optimism, as they have remained high for years with periodic downward trends. This indicates that, despite efforts, the level of radicalisation of Muslims is not decreasing, which poses a threat to the country's security. The reason for this is illegal migration from Morocco and Algeria and other Muslim countries. For the Arabs, Spain is a unique country in Europe, as it represents in their minds a mythologised Al-Andalus, *dar of al-islam* (the land of Islam) of their ancestors. After the terrorist attack of 11 September 2001 in the USA, and in the face of exponentially increasing migration from Muslim countries, the topic of Islam in Spain became the subject of debate, press articles and academic studies. In 2001, there were 324 000 foreigners of the Islamic faith living in Spain⁸⁸. The statistics were complemented by a large group of converts to Islam, especially in Andalusia, estimated at 20,000-25,000 members, and illegal Muslim immigrants, who made the estimated number of followers

⁸⁷ *La Policía Nacional advierte: «estamos en nivel 4 de alerta terrorista»*. Estas son las claves, Hipertextual, 30 V 2023, <https://hipertextual.com/2023/05/la-policia-nacional-advierte-estamos-en-nivel-4-de-alerta-terrorista-estas-son-las-claves> [accessed: 30 V 2023].

⁸⁸ R. Stryjewski, *Muzułmanie w Hiszpanii* (Eng. Muslims in Spain), in: *Muzułmanie w Europie* (Eng. Muslims in Europe), A. Parzymies (ed.), Warszawa 2005, p. 466.

of Islam in Spain around 600,000⁸⁹. There are now 2,350,000 of them living there, including more than 640,000 in Catalonia, which is four times as many as 20 years earlier⁹⁰.

Young people arriving in Spain from Muslim countries bring their own ideas and values, and these in recent years have been oriented towards increased religiosity and a desire for more and more religious participation in political life⁹¹. From there it is only a step to claims and struggles for concessions and privileges. Depending on who is in power in Madrid - the Socialists or the right-wing Popular Party - the state's migration policy is tightening or loosening. The same applies to the attitude towards the separatist aspirations of Catalonia and Basque and the strengthening of the country's territorial unity. Between 2021 and 2023, the Madrid authorities have succeeded in quietening down the problems with Catalonia, which has translated into an easing of the political dispute and a reduction of interest in the region's authorities in Barcelona. This has not been the case for the secret services, which, unable to count on the cooperation of the Catalan police Mossos d'Esquadra, have had to engage their own forces and resources to the surveillance of the Muslim communities there, which enjoy a high degree of autonomy thanks to the Barcelona authorities.

Spanish secret services fighting religious terrorism and political extremism therefore have no easy task. In the near future, they will face even more serious challenges from the rapidly growing number of Muslims, including radicals and conservative Islamists closed to integration with the Christian majority. Indeed, this growing number translates into their social demands and political aspirations. In 2018, Muslims announced the formation of their own parties along the lines of Morocco's Justice and Development Party (Hizb al-Adala wa at-Tanmijja), Justice and Charity Movement (Al-Adl wa al-Ihsan) and Tunisia's Renaissance Party (Hizb an-Nahda), all derived from the Muslim Brotherhood movement

⁸⁹ Ibid.

⁹⁰ R. Fernández, *Número total de musulmanes por comunidad autónoma de España en 2022*, Statista, 11 IV 2023, <https://es.statista.com/estadisticas/552893/musulmanes-en-espana-por-comunidad-autonoma/> [accessed: 11 IV 2023].

⁹¹ J. Wójcik, *Czy polityczny islam wraca na Bliski Wschód?* (Eng. Is political Islam making a comeback in the Middle East?), euroislam.pl, 22 VIII 2023, <https://euroislam.pl/czy-polityczny-islam-wraca-na-bliski-wschod/> [accessed: 22 VIII 2023].

(Al-Ichwan al-Muslimin)⁹². It is to be hoped that an increase in the forces and resources devoted to the activities of the Spanish secret services and good cooperation with their counterparts in Morocco, regardless of the political turmoil between Madrid and Rabat, will make it possible to effectively counter threats to Spain's anti-terrorist security.

Bibliography

Brylew M., *Irak 2006–2012. Stabilizacja czy konflikt?* (Eng. Iraq 2006-2012. Stabilisation or conflict?), Toruń 2013.

Cieszko J., *Tragedia w Madrycie, 11–14 marca 2004 roku* (Eng. Tragedy in Madrid, 11-14 March 2004), in: *Hiszpania: Media masowe i wybory w obliczu terroryzmu* (Eng. Spain: Mass media and elections in the face of terrorism), B. Dobek-Ostrowska, M. Kuś (eds.), Wrocław 2007, pp. 39–60.

Domejko-Kozera P., *Polityka bezpieczeństwa w Hiszpanii w latach 1992–2004* (Eng. Security policy in Spain 1992-2004), Warszawa 2006.

Gonzalez Esteban J.L., *Kronika 11 marca: terroryzm i polityczna zmiana w Hiszpanii* (Eng. Chronicle 11 March: terrorism and political change in Spain), in: *Hiszpania: Media masowe i wybory w obliczu terroryzmu* (Eng. Spain: Mass media and elections in the face of terrorism), B. Dobek-Ostrowska, M. Kuś (eds.), Wrocław 2007, pp. 61–72.

Grzeškowiak S., *Poczet islamskich ideologów i ekstremistów* (Eng. Islamic ideologues and extremists), Warszawa 2023.

Izak K., *Hiszpania i Francja walczą z nielegalną imigracją i fałszerstwami dokumentów* (Eng. Spain and France fight illegal immigration and document forgery), "Człowiek i Dokumenty" 2021, no. 62, pp. 67–75.

Izak K., *Leksykon organizacji i ruchów islamistycznych* (Eng. Lexicon of Islamist organisations and movements), Warszawa 2014.

Izak K., *Migranci jako element nacisku w stosunkach międzynarodowych. Dokumenty dowodem przestępczej działalności państw* (Eng. Migrants as an element of pressure in international relations. Documents evidence of criminal activities of states), "Człowiek i Dokumenty" 2021, no. 63, pp. 56–65.

⁹² K. Izak, *Sieć ekstremistów...*, p. 108.

Izak K., *Oryginalne paszporty w rękach terrorystów i oszustów* (Eng. Original passports in the hands of terrorists and fraudsters), "Człowiek i Dokumenty" 2019, no. 54, pp. 44–55.

Izak K., *Sieć ekstremistów religijnych i politycznych. Sojusznicy i wrogowie* (Eng. A network of religious and political extremists. Allies and enemies), "Internal Security Review" 2019, no. 21, pp. 96–134.

Jakubowska Z., *Madryt 11 marca* (Eng. Madrid 11 March), Warszawa 2005.

Kłos A., *Fikcja walki z radykalizmem* (Eng. The fiction of the fight against radicalism), "Gazeta Polska Codziennie", 13 X 2018.

Kosmyńska S., *Święta wojna w Al-Andalus. Przeobrażenia aktywności dżihadystycznych komórek terrorystycznych w Hiszpanii w latach 1995–2012* (Eng. The Holy War in Al-Andalus. The transformation of jihadist terrorist cell activity in Spain between 1995 and 2012), Łódź 2015.

Loredo J., *Marzenie o Al Andalus* (Eng. The dream of Al-Andalus), "Nasz Dziennik", 19 XI 2011.

Łódzki B., *Reakcja polskich mediów masowych na atak terrorystyczny w Madrycie 11 marca 2004 r.* (Eng. Reaction of the Polish mass media to the terrorist attack in Madrid on 11 March 2004), in: *Hiszpania: Media masowe i wybory w obliczu terroryzmu* (Eng. Spain: Mass media and elections in the face of terrorism), B. Dobek-Ostrowska, M. Kuś (eds.), Wrocław 2007, pp. 123–137.

Pludowski T., *Reakcje prasy amerykańskiej na madrycki atak terrorystyczny z 11 marca 2004 r.* (Eng. U.S. press reactions to the Madrid terrorist attack of 11 March 2004), in: *Hiszpania: Media masowe i wybory w obliczu terroryzmu* (Eng. Spain: Mass media and elections in the face of terrorism), B. Dobek-Ostrowska, M. Kuś (eds.), Wrocław 2007, pp. 140–159.

Reinares F., *Al-Qaeda's Revenge. The 2004 Madrid Train Bombing*, New York 2016.

Skowronek T., *Hiszpania walczy ze światowym terroryzmem* (Eng. Spain fights global terrorism), "Przegląd" 2019, no. 46, pp. 28–30.

Stryjewski R., *Muzułmanie w Hiszpanii* (Eng. Muslims in Spain), in: *Muzułmanie w Europie* (Eng. Muslims in Europe), A. Parzymies (ed.), Warszawa 2005, pp. 453–493.

Taracha C., *Wybory w cieniu zamachu. Kilka uwag na temat wydarzeń z marca 2004 roku w Madrycie* (Eng. Elections in the shadow of an attack. Some comments on the events of March 2004 in Madrid), in: *Terroryzm wczoraj i dziś. Wybrane problemy* (Eng. Terrorism yesterday and today. Selected issues), P. de la Fuente, W. Gizicki, C. Taracha (eds.), Lublin 2015, pp. 77–85.

Tryc-Ostrowska M., *Kontrowersyjny wyrok za zamachy w Madrycie* (Eng. Controversial sentence for Madrid attacks), "Rzeczpospolita", 2 XI 2007.

Wejksznier A., *Ewolucja terroryzmu motywowanego ideologią religijną na przykładzie salafickiego ruchu globalnego dżihadu* (Eng. The evolution of terrorism motivated by religious ideology as exemplified by the Salafist global jihad movement), Poznań 2010.

Internet sources

Actividad Terrorista de ETA 2004, Ministerio del Interior, <https://www.statewatch.org/media/documents/news/2005/jan/mirbal2004acteta.pdf> [accessed: 12 III 2005].

Atentados Terroristas del Dia 11 del Marzo de 2004 de Madrid, Juzgado Central de Instruccion N° 6 Audiencia Nacional Madrid, <https://e00-elmundo.uecdn.es/documentos/2006/04/11/auto11m/01.pdf> [accessed: 11 IV 2006].

Badcock J., *The Long Shadow of al-Andalus. Spain is on the periphery of Europe, but central to modern jihad*, Foreign Policy, 21 VIII 2017, <https://foreignpolicy.com/2017/08/21/the-long-shadow-of-al-andalus-spain-islamic-state-terrorism-al-qaeda/> [accessed: 21 VIII 2017].

Becares R., Cernuda O., *Cuatro terroristas islámicos se inmolan en un piso de Leganés y matan a un agente de policía*, elmundo.es, 4 IV 2004, <https://www.elmundo.es/elmundo/2004/04/03/enespecial/1081016920.html> [accessed: 4 IV 2004].

Catalán M., *Prensa, verdad y terrorismo: la lección política del 14-M*, "El Argonauta Español" 2005, no. 2. <https://doi.org/10.4000/argonauta.1191> [accessed: 26 VIII 2023].

Cedeira B., *La víctima que entró en coma el 11M hasta morir 10 años después*, El Español, 11 III 2017, https://www.elespanol.com/reportajes/20170310/199730525_0.html [accessed: 11 III 2017].

Centro Nacional de Coordinación Antiterrorista CNCA, La Pagina de ASR, <https://intelpage.info/centro-nacional-de-coordinacion-antiterrorista.html> [accessed: 12 XII 2015].

Dziedzina J., *Imam kazał zabijać* (Eng. Imam ordered to kill), gość.pl, 7 IX 2017, <https://www.gosc.pl/doc/4166327.Imam-kazal-zabijac> [accessed: 7 IX 2017].

El final del principio en la investigación del 11-M, elmundo.es, 1 XI 2007, <https://www.elmundo.es/elmundo/2007/11/01/espana/1193885319.html> [accessed: 1 XI 2007].

„El Mundo”: *zamachowcy z Madrytu radykalizowali młodych muzułmanów w więzieniach* (Eng. ‘El Mundo’: Madrid bombers radicalised young Muslims in prison), TVN24, 11 X 2018, <https://tvn24.pl/swiat/zamachowcy-z-madrytu-radykalizowali-mlodych-musulmanow-w-wiezieniach-ra875396-2384538> [accessed: 11 X 2018].

ETA pretendía volar la estación de Chamartín con un „tren bomba” y provocar una masacre, ABC España, 26 XII 2003, https://www.abc.es/espana/abci-pretendia-volar-estacion-chamartin-tren-bomba-y-provocar-masacre-200312260300-228547_noticia.html [accessed: 26 XII 2003].

Fernández H.A., *Does al-Qaeda have a global strategy?*, Elcano Royal Institute, 4 V 2004, <https://www.realinstitutoelcano.org/en/analyses/does-al-qaeda-have-a-global-strategy/> [accessed: 6 V 2004].

Fernández R., *Número total de musulmanes por comunidad autónoma de España en 2022*, Statista, 11 IV 2023, <https://es.statista.com/estadisticas/552893/musulmanes-en-espana-por-comunidad-autonoma/> [accessed: 11 IV 2023].

Fernando Reinares, *experto en terrorismo internacional, advierte: “Al Qaeda está hoy más extendida de lo que ha estado nunca”*, Universidad Internacional Menéndez Pelayo, <https://www.uimp.es/actualidad-uimp/fernando-reinare-experto-terrorismo-internacional.html> [accessed: 21 VI 2021].

Gunaratna R., *Spain: An Al Qaeda Hub?*, “UNISCI Discussion Papers” 2004, no. 5, <https://www.redalyc.org/pdf/767/76712467002.pdf> [accessed: 22 II 2014].

Haahr K., *The Growth of Militant Islamist Micro-Diaspora Communities*, “CTC Sentinel” 2008, vol. 1, no. 4, <https://ctc.westpoint.edu/the-growth-of-militant-islamist-micro-diaspora-communities-observations-from-spain/> [accessed: 18 IV 2008].

Hernández A., *11M: quién fue el autor intelectual y otras claves que plantea el documental de Netflix sobre el mayor atentado yihadista en Europa*, BBC, 11 III 2022, <https://www.bbc.com/mundo/noticias-60693476> [accessed: 11 III 2022].

Hiszpania: Rozpoczął się proces dżihadysty zatrzymanego w Warszawie (Eng. Spain: Trial of jihadist detained in Warsaw begins), Dziennik Gazeta Prawna, 11 VI 2018, <https://www.gazetaprawna.pl/wiadomosci/artykuly/1132741,proces-dzihadysty-zatrzymanego-w-warszawie.html> [accessed: 11 VI 2018].

Hiszpański parlament zgodził się na wysłanie żołnierzy do Iraku (Eng. Spanish parliament agrees to send troops to Iraq), Wirtualna Polska, 22 X 2014, <https://wiadomosci.wp.pl/hiszpanski-parlament-zgodzil-sie-na-wyslanie-zolnierzy-do-iraku-6027730872366209a> [accessed: 22 X 2014].

Interior cesa al jefe del CITCO y nombra a un comisario al frente del Gabinete de Estudios y Coordinación, elDiario.es, 7 VII 2018, https://www.eldiario.es/politica/interior-citco-gabinete-estudios-coordinacion_1_2035094.html [accessed: 7 VII 2018].

La policía eleva a siete los terroristas muertos en Leganés, Cadenaser, 7 IV 2004, https://cadenaser.com/ser/2004/04/07/espana/1081295423_850215.html [accessed: 7 IV 2004].

La Policía Nacional advierte: «estamos en nivel 4 de alerta terrorista». Estas son las claves, Hipertextual, 30 V 2023, <https://hipertextual.com/2023/05/la-policia-nacional-advierte-estamos-en-nivel-4-de-alerta-terrorista-estas-son-las-claves> [accessed: 30 V 2023].

Lindenberg G., *Czy Maroko gra z Hiszpanią imigrantami?* (Eng. Is Morocco playing migrants with Spain?), euroislam.pl, 14 II 2021, <https://euroislam.pl/czy-maroko-gra-z-hiszpania-imigrantami/> [accessed: 14 II 2021].

Llega a España “El Egipto” para ser juzgado por el 11-M, 20 minutos, 17 XI 2006, <https://www.20minutos.es/noticia/173755/0/egipcion/11-m/italia/> [accessed: 17 XI 2006].

Los terroristas del 11-M se inmolan y matan a un geo al volar su «piso franco» en Leganés, ABC España, 4 IV 2004, https://www.abc.es/espana/abci-terroristas-inmolan-y-matan-volar-piso-franco-leganes-200404040300-962802830594_noticia.html [accessed: 4 IV 2004].

Maclean W., *New evidence of Qaeda tie to Madrid blast: expert*, Reuters, 13 I 2010, <https://www.reuters.com/article/cnews-us-security-spain-qaeda-id-CATRE60B52020100112> [accessed: 13 I 2010].

Madrid bombings ‘probably al Qaeda’, Stuff, 21 I 2010, <https://www.stuff.co.nz/vl-push/world/3226277/Madrid-bombingsprobably-al-Qaeda> [accessed: 21 I 2010].

Madryt: posiedzenie Komitetu Antyterrorystycznego ONZ (Eng. Madrid: meeting of the UN Counter-Terrorism Committee), Dziennik Gazeta Prawna, 27 VII 2015, <https://www.gazetaprawna.pl/wiadomosci/artykuly/885271,madryt-posiedzenie-komitetu-antyterrorystycznego-onz.html> [accessed: 27 VII 2015].

Martin-Arroyo J., *El Cordobés, the Spanish face of Islamic State*, El País, 25 VIII 2017, https://english.elpais.com/elpais/2017/08/25/inenglish/1503659430_853709.html [accessed: 25 VIII 2017].

Martin Plaza A., *Los atentados del 11M que sacudieron España*, RTVE, 11 III 2014, <https://www.rtve.es/noticias/20140311/atentados-del-11m-sacudieron-espana/893543.shtml> [accessed: 11 III 2014].

Mroczek A., *Zamach w Madrycie 11 III 2004 – minuta po minucie* (Eng. Madrid attack 11 III 2004 - minute by minute), terroryzm.com, 25 IX 2005, <http://www.terroryzm.com/zamach-w-madrycie-11-iii-2004-minuta-po-minucie/> [accessed: 25 IX 2005].

Po pięciu latach koniec polskiej misji w Iraku (Eng. After five years, the end of the Polish mission in Iraq), money.pl, 29 X 2008, https://www.money.pl/archiwum/wiadomosci_agencyjne/pap/artykul/po;pieciu;latach;koniec;polskiej;misji;w;iraku,188,0,381372.html [accessed: 29 X 2008].

Reinares F., *The Evidence of Al-Qa`ida's Role in the 2004 Madrid Attack*, "CTC Sentinel" 2012, vol. 5, no. 3, <https://ctc.westpoint.edu/the-evidence-of-al-qaidas-role-in-the-2004-madrid-attack/> [accessed: 18 IV 2012].

Siedmiu hiszpańskich agentów zginęło w Iraku (Eng. Seven Spanish agents killed in Iraq), Wirtualna Polska, 29 XI 2003, <https://wiadomosci.wp.pl/siedmiu-hiszpańskich-agentow-zginelo-w-iraku-6036492925121665a> [accessed: 30 XI 2003].

The Terror Attacks in Madrid, Spain, 2004, Kamedo-report 90, Socialstyrelsen 2007, https://www.socialstyrelsen.se/globalassets/sharepoint-dokument/artikelkatalog/ovrigt/2007-123-36_200712336.pdf [accessed: 11 III 2008].

What's Osama Talking About?, Slate, 8 X 2001, <https://slate.com/news-and-politics/2001/10/what-s-osama-talking-about.html> [accessed: 8 X 2001].

Wójcik J., *Czy polityczny islam wraca na Bliski Wschód?* (Eng. Is political Islam making a comeback in the Middle East?), euroislam.pl, 22 VIII 2023, <https://euroislam.pl/czy-polityczny-islam-wraca-na-bliski-wschod/> [accessed: 22 VIII 2023].

Wójcik J., *„Raper ISIS” wrócił do Europy po azyl* (Eng. “ISIS rapper” returned to Europe for asylum), euroislam.pl, 20 V 2020, <https://euroislam.pl/rapper-isis-do-euro-powrocil-jako-szukajacy-azylu/> [accessed: 20 V 2020].

Zamachy terrorystyczne w Hiszpanii. Można było im zapobiec (Eng. Terrorist attacks in Spain. They could have been prevented), Magazyn TVN24, <https://archiwum.tvn24.pl/magazyn-tvn24/114/tvn24.pl/magazyn-tvn24/willa-na-uboczu-matka-szatana-i-plan-a-zamach-na-niespotykana-skale%2C114%2C2082.html> [accessed: 22 VIII 2017].

Zamachy w Madrycie – odwet za Irak (Eng. Madrid attacks - retaliation for Iraq), Polskie Radio, 11 III 2014, <https://www.polskieradio.pl/106/246/Artykul/1071933%-2CZamachy-w-Madrycie---odwet-za-Irak> [accessed: 11 III 2014].

Zmarła czwórka Polaków rannych w Madrycie (Eng. Four Poles injured in Madrid died), Gazeta Wyborcza, 12 III 2004, <https://web.archive.org/web/20091214225052/http://wyborcza.pl/1,75248,1961962.html> [accessed: 12 III 2004].

Krzysztof Izak

Retired Internal Security Agency officer.

Contact: lizior3@wp.pl

The Wagner Group in Africa. The sham battle of Russian mercenaries against terrorism

ALEKSANDER OLECH

Defence24

 <https://orcid.org/0000-0002-3793-5913>

Abstract

In recent years, the Wagner Group has significantly increased its presence in several African countries. Russian mercenaries have become involved in many conflicts in an effort to expand their influence. One of their main tasks was to fight against terrorism. The analyses carried out, in which the author used qualitative methods and sources relating to the theoretical and practical dimensions of the issue at hand, indicate that the Wagnerists have been posing as their operations in order to maintain military presence on the African continent. Intensifying the Wagner Group's presence is a long-term strategy of the Kremlin, which pursues interests along two tracks – benefiting from cooperation at the state level and engaging mercenaries. Countries of the wider West (members of the North Atlantic Alliance and the European Union) are also seeking to develop cooperation with African partners. Terrorist organisations also intend to fight for influence on the continent. In this regard, it is necessary to constantly monitor Russia's proactive foreign policy aimed at the rivalry as it affects the presence of Poland and its allies in Africa.

Keywords

Wagner Group, Africa, Russia, terrorism, anti-terrorism, mercenaries

Introduction

The Wagner Group was founded¹, with the approval of the Chief of General Staff of the Armed Forces of the Russian Federation, around 2010 by Dmitry Utkin and financed by Yevgeny Prigozhin. The first mercenaries were sent on missions abroad in 2014 - to Crimea and the Donbass, and more of them in 2015 to Syria². The strategy of engaging mercenaries abroad had the support of Vladimir Putin, and in the following years became an important part of the foreign policy of the Russian Federation (RF). The Wagner Group (in the sense of a Private Military Company, PMC) should be seen as an organisation that is a tool used by Russia to carry out operations of a political, military and economic nature on a global scale.

Unlike Western European states, Russia has no negative experience of occupying, either politically or economically, African countries (it did, however, attempt to subjugate and impose dependency on Central and Eastern European countries and colonise Somaliland, among others). Moreover, it has gone down in the history of some African countries as supporting national liberation movements. Today, Russia's actions in Africa are multifaceted.

The Kremlin provides armaments, mercenaries and finances the extraction of natural resources. It also uses political lobbying, which translates into both the achievement of political objectives and concrete financial benefits, including by creating a market for Russian equipment.

Nearly 40 African partners are interested in strengthening cooperation with Moscow in such an important area as the military³. The Russian Federation is the leader in arms supplies to Africa, with a market share of 26% for purchases by sub-Saharan African countries. When Maghreb

¹ The studies give different information about the formation and organisation of the Wagner Group.

² For more on the formation of the Wagner Group, see: Ch. Faulkner, *Undermining Democracy and Exploiting Clients: the Wagner Group's Nefarious Activities in Africa*, "CTC Sentinel" 2022, vol. 15, no. 6, <https://ctc.westpoint.edu/wp-content/uploads/2022/06/CTC-SENTINEL-062022.pdf>, pp. 29–31 [accessed: 4 XII 2023].

³ A. Olech et al., *Militarne zaangażowanie Federacji Rosyjskiej w Afryce. Zawarte porozumienia i umowy* (Eng. The Russian Federation's military engagement in Africa. Agreements and arrangements concluded), Instytut Nowej Europy, 23 V 2023, <https://ine.org.pl/militarne-zaangazowanie-federacji-rosyjskiej-w-afryce-zawarte-porozumienia-i-umowy/> [accessed: 23 V 2023].

countries are included, this percentage rises to as much as 40%⁴. Russia mainly supplies rocket and artillery weapons, small arms and armoured vehicles. The most important customers from the sub-Saharan African region are: Angola, Mali, Nigeria and Sudan.

Between 2019 and 2023, the Wagner Group has become an important instrument in Russian foreign policy, particularly in Africa, where Moscow seeks to expand its influence and compete with the West. To achieve this goal, the Wagnerists have established relationships with the governments of a number of African countries, offering military and security services in exchange for mining concessions and expanded political influence. However, the group is not interested in genuine defence capacity building or fighting terrorism. It seeks primarily to capitalise on profits and reap the benefits from prolonged chaos in order to maintain its presence on the continent.

The mercenaries can be used to maintain the security situation, as the Wagner Group has military experience in Africa, particularly in the protection of people and facilities, and is able to move efficiently and carry out ad hoc operations. Importantly, when cooperating with a Russian entity, there are no strictures in terms of meeting certain conditions (e.g. the existence of a democratic government, respect for human rights), as required by international organisations and Western countries. Furthermore, the Wagnerists support governments or juntas leaders after coups. The prospect of changing power and receiving support from Russian mercenaries may tempt some people in unstable African countries.

Research problem

The Wagner Group can be classified as a para-private actor because of its close ties to Russia's political elite and the ways in which the Kremlin uses the organisation in direct foreign policy. The group is not a registered organisation nor does it function as a state actor, making it difficult to determine what kind of threat to combat. It has been deliberately woven into a complex web of business entities and shell companies (part of Prigozhin's

⁴ M. Douet, *Russia overtakes China as leading arms seller in sub-Saharan Africa*, Le Monde, 28 III 2023, https://www.lemonde.fr/en/le-monde-africa/article/2023/03/28/russia-overtakes-china-as-leading-arms-seller-in-sub-saharan-africa_6021018_124.html [accessed: 10 XII 2023].

commercial empire at the time and individuals with links to the Russian government), as well as an equally complex web of government entities. The Wagnerists not only carry out strictly military operations, but also, among other things: information operations, training, arms and financial transfers, cyber operations, they also provide logistical support, company protection and surveillance.

In the course of research queries, the author of the article found that there are very few publications, both in Polish and English, that treat in detail the presence and activities of the Wagner Group in each of the African countries, as well as outlining how the issues of terrorism and counter-terrorism intersect, as the Kremlin uses different definitions of these phenomena in favour of its own interests, including in the Russian Federation⁵. The author gathered data from several hundred Polish and foreign articles, reports, books, media reports, as well as numerous materials obtained from his own searches.

The article does not cover the issue of the Wagner Group's presence in Syria and Ukraine, but the author is aware that these are important corps of Wagnerists operating around the world. Nor is a detailed description of the terrorist organisations (groups, cells, battalions) provided, i.e. the history of their formation, the views currently held, the religion represented, plans for expansion and the relationship between the various organisations and the states in which they operate⁶.

Globally, the Wagner Group may have been active, to a greater or lesser extent, in some 30 countries, including Eastern Europe (e.g. Ukraine), the Middle East (e.g. Syria) and South America (e.g. Venezuela), but its presence on the African continent is most visible. This involvement, which has an impact on the internal situation of countries and on their foreign policy, is mainly in Mali, Burkina Faso, Libya, the Central African Republic (CAR) and Sudan (Figure 1). Influence of the Wagnerists on the continent, however, extends much wider, as this analysis will discuss⁷.

⁵ A. Olech, *Ataki terrorystyczne w Federacji Rosyjskiej w XXI wieku* (Eng. Terrorist attacks in the Russian Federation in the 21st century), "Nowa Polityka Wschodnia" 2019, no. 4 (23), pp. 109–127.

⁶ On this topic see: K. Izak, *Leksykon organizacji i ruchów islamistycznych* (Eng. Lexicon of Islamist organisations and movements), Warszawa 2014.

⁷ The research conducted for this article was completed on 31 December 2023.



Figure 1. Countries in Africa where the Wagner Group is or was active.

Source: own elaboration.

Mali

Bamako has turned to Russian private military companies (mainly the Wagner Group) to increase security, due to repeated attacks by terrorist groups⁸, and also to limit the influence of the French Republic in Mali. Representatives of the Wagner Group were already lobbying the Malian interim authorities after they signed a defence agreement with Moscow in 2019. Cooperation intensified after the military putsch in May 2021, when Colonel Assimi Goita came to full power.

The situation in Mali is difficult due to the involvement of several actors vying for influence. Currently, three parties can be distinguished:

⁸ J. Wójcik, *Ekspansja dżihadu w Afryce: z Sahelu ku południu* (Eng. The expansion of jihad in Africa: from the Sahel towards the south), "Układ Sił" 2020, no. 20.

- 1) the Malian armed forces (Forces Armées Maliennes, FAMA) supported by Niger and Burkina Faso within the framework of the Alliance of Sahel States⁹, the Wagner Group and some Tuareg groups;
- 2) Tuareg and Arab militias and armed groups operating within coalitions of Tuareg organisations fighting for an independent Azawad¹⁰[including members of the Permanent Strategic Framework (Cadre stratégique permanent) and the National Movement for the Liberation of Azawad (Coordination des mouvements de l'Azawad, CMA)];
- 3) Terrorist organisations active in, inter alia, Mali, Burkina Faso and Niger¹¹, i.e.: the Group for the Support of Islam and Muslims (Jama'at Nasr al-Islam wa al-Muslimin, JNIM) and the so-called Islamic State (Ad-Dawla al-Islamiyya; Islamic State of Iraq and Syria, ISIS)¹² and its cells, including the Islamic State Sahel Province (ISSP; Sahil Wilajet ad-Dawla al-Islamiyya) and the Islamic State West Africa Province (ISWAP)¹³.

The start of the Wagner Group's official and fully military involvement should be dated to December 2021, when the organisation began building

⁹ A regional collective security organisation (Alliance des États du Sahel), but with aspirations to also work together economically, as a sort of counterbalance to the Economic Community of West African States.

¹⁰ The situation in the north of Mali was supposed to calm down after the 2015 peace agreement in Algiers between the central authorities and separatist Tuareg and Arab groups. However, years later, these groupings have re-engaged in fighting over land and influence. At the same time, operations MINUSMA and Barkhane have been unable to stop the resurgence and expansion of terrorist groups linked to al-Qaeda and ISIS. See: J. Czerep, *Przyszłość misji ONZ w Afryce po wycofaniu MINUSMA z Mali* (Eng. The future of the UN mission in Africa after MINUSMA's withdrawal from Mali), PISM, 6 X 2023, <https://www.pism.pl/publikacje/przyszlosc-misji-onz-w-afryce-po-wycofaniu-minusma-z-mali> [accessed: 2 XI 2023].

¹¹ K. Chesnutt, K. Zimmerman, *The State of al Qaeda and ISIS Around the World*, Critical Threats, 8 IX 2022, <https://www.criticalthreats.org/analysis/the-state-of-al-qaeda-and-isis-around-the-world> [accessed: 5 XI 2023].

¹² J. Czerep, *Afryka Subsaharyjska w strategii tzw. Państwa Islamskiego* (Eng. Sub-Saharan Africa in the strategy of the so-called Islamic State), PISM, 1 VIII 2022, <https://www.pism.pl/publikacje/afryka-subsaharyjska-w-strategii-tzw-panstwa-islamskiego> [accessed: 2 XI 2023].

¹³ Al-Qaeda and ISIS are in conflict with each other. They repeatedly operate in the same territory and seek to recruit members from the same communities.

a camp next to Modibo Keita International Airport in Bamako, a short distance from Airbase 101, a military facility used by the Malian Air Force. In the early months of 2022, the Wagnerists undertook operations in central Mali, with Russian personnel also deploying to Timbuktu, where they occupied the former bases of the French Barkhane operation. The arrival of Russian mercenaries accelerated the withdrawal of French forces and those of other European countries.

For a \$10.8 million monthly fee and gold mining concessions, the Wagnerists provide security and training to the Malian junta and engage militarily to fight the jihadists. As of early 2024, there are around 2,000 Russian mercenaries operating in Mali. An accurate estimate of their number is difficult, as the Russians arrive in the country bypassing Bamako. Most of the Russian planes land in Gao and Timbuktu, while vagrants are also sent to the east of the country, to Menaka. Their main activity is to support the Malian army in its attempts to take control of the country's northern territories, for years dominated mainly by Tuareg separatists¹⁴. The armed skirmishes in which mercenaries supporting the Malian army are involved concern attempts to take over strategic towns (including Kidal) and military bases (where United Nations forces were previously stationed) in the north of the country¹⁵, and to a lesser extent battles with terrorist groups¹⁶.

As part of its financial capacity building, the Wagner Group uses its presence in Mali to control the transport, agricultural and mining sectors. It collects fees and duties to finance its mercenaries. As in other African countries, the Malian authorities and the national military either accept

¹⁴ Tuareg separatists also have conflicting interests within communities, tribes and clans. See: M. Shurkin (@MichaelShurkin), X, 22 XI 2023, <https://twitter.com/MichaelShurkin/status/1727337675806650866> [accessed: 22 XI 2023].

¹⁵ K. Gadera, *Mali: chaotyczny koniec MINUSMA, Azawad znów walczy o niepodległość* (Eng. Mali: chaotic end of MINUSMA, Azawad fights for independence again), *Konflikty.pl*, 9 XI 2023, <https://www.konflikty.pl/aktualnosci/wiadomosci/mali-azawad-niepodleglosc/> [accessed: 13 XI 2023].

¹⁶ At the end of October 2023, members of the UN mission leaving the country were not given permission to transport their soldiers by air from their base in Kidal. For this reason, the soldiers (from, among others, Chad, Guinea, Egypt, Nepal, Cambodia and Bangladesh) embarked on a 350-kilometre road journey to Gao. The convoy of almost 850 vehicles came under repeated attack. The MINUSMA force base at Kidal initially fell to the CMA and was then quickly taken over by Malian troops and the Wagnerists.

or deliberately overlook the crimes committed by the Wagnerists against civilians¹⁷.

It should be noted that more than two years after the arrival of Russian mercenaries in Mali, the security situation in the country has deteriorated. Despite the fighting between Al-Qaeda¹⁸ and the Islamic State troops in the Sahel, both terrorist groups are combining their capabilities and engaging smaller terrorist and rebel groups, allowing them to significantly expand their territory of operations. The conflict is spilling over into the entire Sahel region and poses a threat to the Gulf of Guinea states. At the same time, the JNIM, whose cells operate in Burkina Faso, Benin and Togo, remains strong in the region.

The Wagner Group has never operated in Mali on its own and is logistically completely dependent on its hosts, the Malian army. In contrast to the Wagnerists, France had many years of experience of activity in the region and had very good military equipment at its disposal. In doing so, it cooperated with a coalition of states in the Barkhane and Takuba Task Force. The capabilities of the Russian mercenaries compared to the Paris-led operations were modest. French troops were specialised in aerially-led operations involving the neutralisation of ships and air facilities belonging to terrorist organisations.

Any action by the Malian junta, backed by the Wagner Group, against movements for an independent Azawad is being watched closely by Algeria. There are fears from the administration of President Abdelmadjid Tebboune that renewed conflict will result in the influx of thousands of refugees across the 1,300-kilometre border. Moreover, Mali's commitment to fighting Tuareg and Arab militias and armed groups is causing the Malian junta to lose sight of the growing terrorist threat. It may soon be too late to neutralise them effectively¹⁹. Already by the end of 2023, it was reported that some arms for Tuaregs and Arabs were entering Mali from Algerian territory, further aggravating the situation. The next step in

¹⁷ Ch. Faulkner, *Undermining Democracy...*, p. 21; P. Wójcik (@SaladinAlDronni), X, 7 XI 2023, <https://twitter.com/SaladinAlDronni/status/1721821654660092201> [accessed: 28 XI 2023].

¹⁸ Al-Qaeda has already united other groups within JNIM in March 2017 and continues to develop its potential.

¹⁹ *Much ado about Kidal*, Africa Confidential, 30 XI 2023, https://www.africa-confidential.com/article/id/14715/Much_ado_about_Kidal [accessed: 30 XI 2023].

the cooling of relations is the cancellation of ambassadors by both sides and the tightening of Morocco's relations with Mali, Burkina Faso and Niger²⁰.

The Wagner's Group will not be able to support Mali's armed forces to fully counter terrorist organisations and Tuareg and Arab groups in the region. The Malian junta must act simultaneously on at least two fronts. It would be realistic to hold on to some of the territory, but greater successes would require large supplies of arms directly from Russia, as well as the deployment of at least several hundred troops to Mali. The Russian Federation, due to the conflict in Ukraine and its involvement in other regions of Africa and the Middle East, cannot afford this. Moscow will therefore be part of a smouldering conflict and, at the same time, will be draining Mali as much as possible financially in order to obtain funds to build up its military presence in the Sahel.

Burkina Faso and Niger

The Wagner's Group was identified on Burkina Faso territory in November 2023. The first transport (20 soldiers) arrived in the country's capital on an Il-76 aircraft belonging to the Russian Air Force. Since the attempted coup in September 2023, President Ibrahim Traoré feared the loss of his regime and therefore asked for support from Russia²¹. This confirms that one of the main tasks of the Wagnerists is to protect senior government officials, especially the president (as in the CAR).

In Burkina Faso, the source of the terrorist threat is the JNIM-affiliated jihadist group Ansar al-Islam. Its ranks are mainly made up of radicalised Fulani (living in the north and east of the country) opposed to the domination of the Mossi people (Burkina Faso's most numerous ethnic group).

The scenario that occurred in Mali was not realised (until early 2024) in Burkina Faso, although Russia had the intention to do so. The authorities in Ouagadougou are primarily interested in enhancing their own counter-

²⁰ F. Bobin, *Coup de froid dans les relations entre l'Algérie et le Mali*, Le Monde, 27 XII 2023, https://www.lemonde.fr/afrique/article/2023/12/27/coup-de-froid-dans-les-relations-entre-l-algerie-et-le-mali_6207961_3212.html?fbclid=IwAR0ZDMZbfg7Wz-a4v1ft4pVoLJzi1MmsUqe5LpaYFGYx85_966-Y9yrQ4Y [accessed: 27 XII 2023].

²¹ B. Roger, *Au Burkina Faso, des militaires russes pour protéger Ibrahim Traoré?*, jeuneafrique, 17 XI 2023, <https://www.jeuneafrique.com/1503219/politique/au-burkina-faso-des-militaires-russes-pour-protoger-ibrahim-traore/> [accessed: 10 XII 2023].

terrorism capabilities and developing counter-terrorism services. This means that joint Russian-Burkina Faso exercises, the purchase of foreign armaments and international action against terrorists (rebel groups) are all realistic. Burkina Faso, however, is reluctant to invite a large group of the Wagnerists. Russian mercenaries are expected to support the consolidation of power by the Burkinese junta.

The presence of the Wagner's Group in Niger is also under scrutiny, as General Abdourahamane Tchiani staged a coup d'état on 26 July 2023, ousting the pro-Western (working closely with France and the US) President Mohamed Bazoum from power. Niger had been a source of stability in the Sahel region for the past years, so the sudden turn towards Russia came as a surprise.

The change of power in Niger has resulted in a halt to all efforts to build resilience against attacks by rebel groups, as well as operations against terrorist groups. The counter-terrorism support maintained by the U.S. (around 1 100 troops) and France (around 1 500 troops)²² (e.g. using the air base in Agadez – crucial for drone operations or the intelligence centre in the capital Niamey), as well as the training of local troops, formed the foundation in the fight against terrorism in the Sahel. The main adversaries were – as in Mali and Burkina Faso – terrorists from JNIM, ISSP, ISWAP and partly Boko Haram. Eventually, all French soldiers left Niger and the French embassy ceased to function.

At the end of July 2023, a few days after the coup, representatives of the Wagner Group appeared in Niamey. The junta in Niger, however, decided that instead of strengthening relations with the Wagnerists, it would immediately move closer to the Russian Federation. On 4 December 2023, the two countries signed an agreement to strengthen military cooperation. Niger ultimately opted for Russia, but US troops remain there, leaving little hope for Western cooperation with the country.

In the context of the situation in the Sahel – after coups in Mali, Burkina Faso, Niger and Sudan, there are reports that the Wagner Group is working with rebels from Chad to overthrow the country's current president²³. This also threatens security, as some French soldiers from Niger have gone to Chad and EU countries are planning to support the authorities in N'Djamena, including Hungary sending a contingent of up to 400 soldiers.

²² Belgium, Canada, Germany, Italy and Australia were also involved in Niger.

²³ W. Rampe, *What Is Russia's Wagner Group Doing in Africa?*, Council on Foreign Relations, 23 V 2023, <https://www.cfr.org/in-brief/what-russias-wagner-group-doing-africa> [accessed: 21 XII 2023].

Although the activity of the Wagnerists in Burkina Faso was small at the beginning, their appearance proved to be a prelude to the development of cooperation. In 2024, their numbers were increased by sending another 100 mercenaries. If the Russian Federation decides that it wants to build its capacity in the region, its presence in Burkina Faso could turn into a bridgehead for Russian mercenaries.

Libya

Today, Libya is a divided country, lacking a single political apparatus to administer the country and conduct foreign policy coherently. Due to rival centres of power, the involvement of other states, and the activity of terrorist groups and mercenaries, including the Wagner Group, it is impossible to emerge with a united government (as the UN and the US are pushing hard to do) that would allow a way out of the crisis and stop the humanitarian catastrophe affecting Libyans and those migrating through the country.

Following contested parliamentary elections in 2014, the country split into two areas with competing centres of power – the High Council of State (HCS), based in Tripoli in western Libya, and the House of Representatives (HoR), based in Tobruk in the eastern part of the country. Thanks to political interventions under the aegis of the UN, a ceasefire was concluded in 2020, which is still partially respected today²⁴.

The House of Representatives from the eastern part of Libya has carved out and supports the Government of National Stability (GNS) and receives support from the Libyan National Army (LNA) led by General Khalifa Haftar (the Wagnerists came to Libya at his invitation). The political rivals of the GNS and HoR are the Government of National Unity (GNU) and the HCS, but relations between the latter two are not harmonious. These so-called Big Five are responsible for the situation in Libya, where an agreement to end the conflict is still far from being reached. In this chaotic environment, the Wagner Group is trying to make its mark.

The Wagnerists emerged in Libya in 2015 with Russian special forces, also supported by another Russian mercenary group, the Rossiskie System Bezopasnosti. Encouraged by General Haftar, the Wagner's Group stepped

²⁴ The October 2020 ceasefire significantly reduced the Wagner Group's involvement in Libya, therefore some personnel were redeployed to Mali and Ukraine.

up activity in late 2018 and by mid-2019 had become a fully committed combatant. Among other things, it supported the LNA's attack on Tripoli against Government of National Accord acknowledged by the UN²⁵.

There are currently up to 2,000 mercenaries working for the Wagner Group in Libya²⁶. They are equipped with, among other things, armoured vehicles, air defence systems, electronic warfare equipment, anti-tank guided missiles, combat aircraft and drones. In Libya, the continent's leading oil producer, Russian mercenaries' activities are focused on accessing both oil and gas deposits²⁷.

In mid-2023, General Haftar threatened military action if oil revenues were not shared fairly. In his view, the profits from this resource are for the most part given to the Government of National Accord, despite the fact that the oil is mainly extracted in fields located in the east of the country²⁸. Russia is doing much to gain influence with the support of the Wagner Group and is using its own energy agreements and the involvement of Russian companies to do so²⁹.

The fight against terrorism has at no time been the purpose of the Wagner Group's presence in Libya, unlike its activities in Syria, Mali or Mozambique. This is because the Islamic State (among others the Islamic-State - Libya Province) had its strongest presence in Libya between 2014 and 2016, and lost large territories in 2018³⁰ (even before the Wagnerists arrived in the country³¹).

It should be pointed out that the methods used during the military operations carried out by the Wagner Group also in Libya fits the definition

²⁵ Ch. Faulkner, *Undermining Democracy...*, p. 30.

²⁶ At the peak of their presence, at least 2,500 mercenaries affiliated to the Wagner Group were carrying out tasks on Libyan territory.

²⁷ Libya's economy is heavily dependent, at around 85%, on hydrocarbon production.

²⁸ P. Wintour, *Fears for Libyan oil production amid military threats*, The Guardian, 4 VII 2023, <https://www.theguardian.com/world/2023/jul/04/fears-for-libyan-oil-production-amid-military-action-threats> [accessed: 13 XII 2023].

²⁹ G. Kuczyński, *Russia's Tatneft Discovers New Oil Field in Libya*, Warsaw Institute, 25 V 2023, <https://warsawinstitute.org/russias-tatneft-discovers-new-oil-field-in-libya/> [accessed: 21 XII 2023].

³⁰ Center for Preventive Action, *Civil Conflict in Libya?*, Council on Foreign Relations, 19 IX 2023, <https://www.cfr.org/global-conflict-tracker/conflict/civil-war-libya> [accessed: 23 XI 2023].

³¹ It is true that some of the Wagner Group's mercenaries were previously active in Syria, where they fought against the Islamic State, but in Libya they had other tasks.

of terrorism. It is an external actor that attempts to destabilise order in the country, engages in armed activities and carries out terrorist attacks. The Wagner Group soldiers who fought alongside the LNA during the 2019 attacks on Tripoli have been accused of carrying out unjustified killings and planting landmines in areas populated by civilians³².

The Russian Federation is currently taking steps to strengthen its military presence in Libya. Following the visit of Russian Deputy Defence Minister Yunus-Bek Yevkurov to Benghazi in August 2023, which took place at the initiative of General Haftar, a plan for the creation of a Russian Army Corps in Afrin was announced. According to it, the soldiers would carry out military operations across the African continent in support of cooperation between Russia and selected states (regimes/governments)³³. At the same time, Moscow is in contact with the government in Tripoli to keep alive the chance of cooperation if there would be a significant weakening of the Wagner Group and General Haftar's forces.

Mozambique

The Wagner's Group emerged in Mozambique due to the increasing activity since 2017 of terrorist groups linked to the Islamic State, operating in the Cabo Delgado region bordering Tanzania. The main reason for the deteriorating security situation in the country was the radicalisation of the economically marginalised population (more than 60 per cent of Cabo Delgado's population is Muslim, while in Mozambique the majority is Christian) and the involvement of extremists from, among others, the group ISIS-Mozambique³⁴, also known as Ansar al-Sunna³⁵ (as well as Ahl-al-Sunna) and locally as Al-Shabaab in Mozambique³⁶. The extremists

³² W. Rampe, *What Is Russia's Wagner Group Doing in Africa?...*

³³ *Russia works with Libya on the creation of a military corps in Africa*, Agenzia Nova, 17 XI 2023, <https://www.agenzianova.com/en/news/la-russia-lavora-con-la-libia-alla-creazione-di-un-corpo-militare-in-africa/> [accessed: 23 XI 2023].

³⁴ *ISIS-Mozambique*, Counter Terrorism Guide, November 2022, https://www.dni.gov/nctc/ftos/isis_mozambique_fto.html [accessed: 12 XII 2023].

³⁵ Also operating with Madinat at-Tawhid wa al-Muwahidin from the Democratic Republic of Congo.

³⁶ *State Department Terrorist Designations of ISIS Affiliates and Leaders in the Democratic Republic of the Congo and Mozambique*, U.S. Department of State, 10 III 2023, <https://www.state.gov/>

wanted the separation of the region from the country, control of drug routes and profits from discovered resource deposits. Growing tensions in the region led to an uprising³⁷. The Mozambican army and services could not cope with the extremist groups and needed the support of foreign forces³⁸.

Two hundred Russian mercenaries arrived in Mozambique with assault helicopters, drones and ground combat equipment in September 2019. The Wagner's Group was tasked with training and commanding the local armed forces. However, the group's members were not able to find their way in the densely forested terrain, cooperation with Mozambican soldiers did not go well, their equipment proved to be of little use against terrorists focusing on ambushes and irregular attacks, and enemy reconnaissance failed. In the first few weeks, more than a dozen Wagnerists were killed.

By early 2020, the situation in Cabo Delgado was bad - the terrorist groups had gained a significant advantage. The loss of a large part of the territory and subsequent unsuccessful operations led to the abandonment of cooperation with the Wagnerists. In March 2020, they left Mozambique, just six months after arriving. They were replaced by other mercenaries from the private military company Dyck Advisory Group. Thus, the Wagner Group's activities in Mozambique were short-lived and can be considered a failure. This is another example confirming that Russian mercenaries will leave any country where they perceive the opponent to be too demanding and where their presence is neither politically nor financially viable. The Russian Federation ignored the flight of the Wagnerists and took no action to improve and strengthen bilateral relations with Mozambique.

state-department-terrorist-designations-of-isis-affiliates-and-leaders-in-the-democratic-republic-of-the-congo-and-mozambique/ [accessed: 12 XII 2023].

³⁷ J. Penney, *Rwanda Helped Oust Jihadists in Mozambique. Can This Model Work in West Africa?*, PassBlue, 16 VIII 2023, <https://www.passblue.com/2023/08/16/rwanda-helped-oust-jihadists-in-mozambique-can-it-work-as-a-counterinsurgency-model-in-west-africa> [accessed: 14 XII 2023].

³⁸ J. Czerep, *Nowy front dżihadu w Mozambiku* (Eng. New jihadist front in Mozambique), PISM, 22 IX 2020, https://pism.pl/publikacje/Nowy_front_dzihadu_w_Mozambiku [accessed: 21 XI 2023].

Sudan

The Wagner's Group has been present in Sudan since 2017 and, amid an escalating power struggle in the country, has been working directly in support of Russia's interests³⁹. Cooperation between the two countries had been intensifying since 2015. A key moment was a meeting in 2017 between then President Omar Al-Bashir and Vladimir Putin, during which Sudan's ruler explicitly asked for support. The Russian Federation was interested in energy and transport cooperation using the Bab al-Mandab Strait⁴⁰. Agreements were signed at the time and talks were held, including on the establishment of a Russian naval base at Port Sudan in the Red Sea. In addition to those mentioned, gold mining concession agreements were signed in 2017.

In April 2023, another coup d'état took place in Sudan. Both Prigozhin and the Wagner Group would have been reluctant to support General Abdel Fattah al-Burhan and the Sudanese Armed Forces (SAF), but kept up operations in support of General Mohamed Hamdan Dagalo (alias "Hemetti", "Hemedti") and the Rapid Support Forces (RSF)⁴¹, with whom they already maintained training cooperation, as well as donating equipment (including ammunition, drones and missiles)⁴².

At present, the RF (as a state and with the support of leading Kremlin politicians) wants to maintain links with al-Burhan and the SAF in case it falls to them to win the civil war. At the same time, the Russians may favour the RSF behind the scenes, using the Wagner Group to do so, because of the situation in Libya and the good relations between Haftar

³⁹ I. Sheludkova, *Why is Russia's Wagner Group in Sudan, and what does it have to do with the war in Ukraine?*, EuroNews, 27 IV 2023, <https://www.euronews.com/2023/04/27/why-is-russias-wagner-group-in-sudan-and-what-does-it-have-to-do-with-the-war-in-ukraine> [accessed: 16 XI 2023].

⁴⁰ *Sudan's President Bashir asks Putin for 'protection' from 'aggressive' US*, France24, 23 XI 2017, <https://www.france24.com/en/20171123-sudan-president-bashir-asks-putin-protection-aggressive-us> [accessed: 16 XI 2023].

⁴¹ At the beginning of a conflict, Prigozhin expressed his willingness to engage in peace mediation because of his good contacts with both sides in the conflict.

⁴² Even before the outbreak of the conflict, arms were being supplied to the RSF using Entebbe Airport in Uganda, which received supplies from the CAR via the Wagner Group.

and Hemetti⁴³, as well as the support⁴⁴ given to them both by the United Arab Emirates⁴⁵.

The Wagner Group's objective in Sudan (where 500-700 mercenaries are currently based) is to secure access to raw materials, which Russia will then use to finance the war in Ukraine and to participate in other theatres of operations. Obtaining gold from Sudan, which is the leading (top three⁴⁶) producer of this mineral in Africa, is not difficult due to the unstable situation in the country and the ease of controlling selected mines.

The continuing collapse of power in Sudan and prolonged fighting means that Moscow is finding it arduous to rebuild cooperation. There is a risk that siding with the RSF will not work and the Kremlin will not realise its expansion plans in East Africa. Taking sides means losses not only politically and militarily, but also economically. An exit from Sudan will not be beneficial for the Russian Federation, and maintaining a presence is essential if Russia wants to continue to fight for its position in the region. An analogy can be drawn with the situation in Libya, where Moscow assists General Haftar militarily, but also ensures correct relations with the government in Tripoli, as it is recognised internationally. The situation is the same with Sudan, where Al-Burhan is recognised. In the event of his victory, the Wagner Group would be pushed out because of its cooperation with the RSF.

The Ukrainian thread

It is worth mentioning that there is an increasing number of revealed attacks by Ukrainian special forces on the Wagner Group mercenary

⁴³ G. Aftandilian, *The Fate of the Wagner Group in Syria, Libya, and Sudan*, Arab Center Washington DC, 18 VII 2023, <https://arabcenterdc.org/resource/the-fate-of-the-wagner-group-in-syria-libya-and-sudan/> [accessed: 23 XI 2023].

⁴⁴ J. Czerep, *Perspektywy zakończenia wojny w Sudanie* (Eng. Prospects for ending the war in Sudan), PISM, 25 V 2023, <https://pism.pl/publikacje/perspektywy-zakonczenia-wojny-w-sudanie> [accessed: 23 XI 2023].

⁴⁵ In the context of the Emirates, it would also be good for the country to disassociate itself from the Wagnerists and to stop supplying arms to the RSF. The United Arab Emirates wants to emphasise its position on the international stage, for example by organising COP28, and with actions such as in Sudan it is undermining its authority.

⁴⁶ M. Goosen, *Biggest Gold Producing Countries in Africa*, Energy Capital Power, 5 IX 2022, <https://energycapitalpower.com/biggest-gold-producing-countries-in-africa/> [accessed: 25 XI 2023].

positions in Sudan. It remains a priority for Ukraine not only to open new diplomatic missions in Africa in the near future⁴⁷, but also to combat the Wagnerists across the African continent⁴⁸.

It is worth noting that in 2024 (when Kiev is expected to conduct a military counter-offensive in the country), the dissemination of Ukrainian involvement in Sudan in the world media has political objectives. President Volodymyr Zelensky's meeting with Al-Burhan on 23 September 2023 at Shannon Airport in Ireland was a signal of support for the Sudanese commander⁴⁹.

In addition, there are reports that Ukrainian soldiers are training and advising Tuareg rebels in Mali, who are waging hostilities against the pro-Russian government and the Wagner Group stationed there⁵⁰. Ukraine - at least in theory - would like to challenge the Russian Federation, whose political presence in Africa is significant. Even if some states would prefer to cooperate with Kiev, they fear the transfer of the Russian-Ukrainian rivalry to the African continent.

The Central African Republic

The Wagner's Group is particularly active in the CAR. There are approximately 1,000 mercenaries in the country⁵¹. It is worth pointing out that a large proportion of the group's members have left Africa, mainly the CAR, due to Russia's invasion of Ukraine, and others after the Prigozhin rebellion. Their numbers have decreased significantly compared to their

⁴⁷ *Ukraine Expands Diplomatic Presence in Africa: New Embassy Launches in Ghana*, The Kyiv Independent, 27 XII 2023, <https://www.kyivpost.com/post/26022/> [accessed: 29 XII 2023].

⁴⁸ T. Eydoux, L. Savoye, *Quand les forces spéciales ukrainiennes combattent des mercenaires russes de Wagner au Soudan*, Le Monde, 19 XI 2023, https://www.lemonde.fr/videos/video/2023/11/19/quand-les-forces-speciales-ukrainiennes-combattent-des-mercenaires-russes-de-wagner-au-soudan_6201120_1669088.html [accessed: 21 XI 2023].

⁴⁹ R. Black, *ZelenskymeetsSudaneseofficialduring 'technicalstopover' in Ireland*, The Independent, 23 IX 2023, <https://www.independent.co.uk/news/uk/volodymyr-zelensky-north-america-ireland-joe-biden-department-of-foreign-affairs-b2417251.html> [accessed: 10 XII 2023].

⁵⁰ S. Sadkiewicz (@StanSadkiewicz), X, 7 XI 2023, <https://twitter.com/StanSadkiewicz/status/1721882283916079351> [accessed: 7 XI 2023].

⁵¹ R. Chason, B. Debout, *In Wagner's largest African outpost, Russia looks to tighten its grip*, The Washington Post, 18 IX 2023, <https://www.washingtonpost.com/world/2023/09/18/wagner-central-african-republic-touadera> [accessed: 5 XI 2023].

peak, when there were more than 2,500 Wagnerists active in the CAR⁵². A priority, especially in the early days, was training for the Central African armed forces, primarily for special forces. The joint exercises were intended to improve the interoperability of the country's troops and allow them to carry out rapid strikes against enemy positions, as the CAR struggles with the presence of rebel groups.

Russian mercenaries are carrying out activities in the CAR that allow them to gain significant material benefits. They protect mines and have rights to extract or distribute specific raw materials in exchange for services rendered. Over the years, the Wagner Group has gained a strong foothold in the country. Mainly thanks to the support of President Faustin-Archange Touadéry, who invited the mercenaries in 2018 (talks were already underway in 2017, and the first contracts were signed with another Russian group, Sewa Security Group⁵³).

As in other African countries where the Wagnerists are building up their presence, troops from the French Republic were previously present in the CAR (since 2012). In 2013, they launched Operation Sangaris to combat rebels and terrorists⁵⁴. At its peak, France deployed around 2,500 troops in the CAR, supporting around 10,000 UN peacekeepers as part of the MINUSCA mission⁵⁵. In 2016, French forces finally withdrew from the country. Unlike in Mali, the UN mission in the CAR is being carried out in spite of the continued presence of the Wagner Group, whose mercenaries carry out atrocities against the civilian population and remain

⁵² L. Serwat, *Moving out of the shadows: Shifts in Wagner Group Operations Around the World*, ACLED, 2 VIII 2023, https://acleddata.com/acleddatanew/wp-content/uploads/2023/08/ACLED_Report_Shifts-in-Wagner-Group-Operations-Around-the-World_2023.pdf [accessed: 5 XI 2023].

⁵³ Sewa Security Group operated its Lobaye Invest SARLU company executing resource extraction contracts.

⁵⁴ Launched at the end of 2013, Operation Sangaris was the seventh French military intervention in the CAR since the country's independence in 1960, with France officially announcing its end on 30 October 2016.

⁵⁵ *France to end Central African Republic military mission in 2016*, France24, 30 III 2016, <https://www.france24.com/en/20160330-france-end-military-operations-central-african-republic> [accessed: 5 XI 2023].

unpunished⁵⁶. It is worth mentioning that in 2021 a monument was erected to the Wagnerists in Bangui⁵⁷.

In the current situation, French troops will not be returning to the CAR, mainly because of the presence of the Wagnerists. For Paris, however, the relationship with Bangui is not completely lost⁵⁸. The matter is seen in a similar way by Washington which remains in contact with the Touadéry administration and to which it offers security cooperation⁵⁹. Talks are also being held with Bancroft Global Development, an American private military company.

The role of Rwanda

In the context of the CAR, it is worth mentioning the military involvement of the Rwandans, who are a counterweight to the Wagner Group in the country. It is Kigali that has been able to improve the security level in several regions of the CAR, support the reform of security structures and provide training for anti-terrorist groups. Although the Russian mercenaries initially cooperated with Rwandan soldiers, with whom they jointly fought rebel groups, especially in 2021, since mid-2022 (when the Russians began to become more heavily involved in the CAR, Sudan and to support the Democratic Republic of Congo, which remains in conflict with Rwanda) there have been increasing tensions between the two.

The rivalry is mainly over control of resource deposits and activities in conflict areas. Kigali has good relations with Moscow, but does not want to be associated with the activities of the Wagner Group. Both groups - in theory - are fighting the rebels (terrorism), but at the same time they are competing. It is worth mentioning that it is currently Rwanda that has

⁵⁶ *Wagner Group Uses Mafia-Style Tactics to Dominate CAR's Diamond Sector*, ADF, 1 VIII 2023, <https://adf-magazine.com/2023/08/wagner-group-uses-mafia-style-tactics-to-dominate-cars-diamond-sector/> [accessed: 25 XI 2023].

⁵⁷ Between 2020 and 2023, the Wagner Group was involved in nearly 40 per cent of the attacks that occurred during the conflicts unfolding in the CAR.

⁵⁸ *Touadéra stirs the geopolitical cauldron*, Africa Confidential, 2 XI 2023, https://www.africa-confidential.com/article/id/14682/Touad%c3%a9ra_stirs_the_geopolitical_cauldron [accessed: 5 XI 2023].

⁵⁹ E. Peltier, *Battle for Influence Rages in Heart of Wagner's Operations in Africa*, The New York Times, 26 XI 2023, <https://www.nytimes.com/2023/11/26/world/africa/wagner-russia-central-african-republic.html> [accessed: 15 XII 2023].

the most numerous and important foreign contingent in the MINUSCA mission.

While the CAR-Rwanda partnership has had positive effects in the context of the fight against terrorism, it has also brought another external actor into the country. The Rwandans have become involved in the same areas in which the Wagner Group operates economically (including the mining sector). The cooperation of the Russian mercenaries with the administration of the CAR is very good and the Kremlin does not intend to make political changes in the country (as, for example, it did in Syria)⁶⁰. However, it recognises the growing role of Rwanda. For the moment, the Wagner Group and the Rwandan military accept their presence in the CAR as they see the benefits of this. However, relations are very tense and conflict could arise.

Democratic Republic of Congo and possible presence of Russian mercenaries

Further information is emerging about the involvement of the Wagner Group in the Democratic Republic of Congo (DRC)⁶¹. It is to conduct coordinated operations with the Congolese armed forces near the border with Uganda. The Wagnerists are also to be present in North Kivu as part of countering the March 23 Movement (supported by Kigali) and terrorist groups [including Madina at Tauheed Wau Mujahedeen (also known as ISIS-DRC)⁶² which originates from the Allied Democratic Forces (ADF) linked to the Islamic State⁶³].

The Wagner's Group is another organisation that could greatly support the Congolese army's operations. It is important to add that Russian

⁶⁰ 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: 16 XI 2023].

⁶¹ S. Schlindwein, *Are white mercenaries fighting in the DRC conflict?*, Deutsche Welle, 17 I 2023, <https://www.dw.com/en/are-white-mercenaries-fighting-in-the-drc-conflict/a-64407711> [accessed: 16 XII 2023].

⁶² *Country Reports on Terrorism 2020: Democratic Republic of the Congo*, U.S. Department of State, <https://www.state.gov/reports/country-reports-on-terrorism-2020/democratic-republic-of-the-congo/> [accessed: 16 XII 2023].

⁶³ *State Department Terrorist...*

mercenaries based in the DR Congo could benefit from the support of their permanent bases in the CAR. Congo is currently in need of arms supplies, and Russia has promised to help equip the Congolese army with new military equipment, especially armoured vehicles, tanks, helicopters and combat aircraft.

Madagascar

The Wagner Group's building of influence in Madagascar is a rather unique example, as it was involved there not militarily, but politically and economically. In mid-2018, a group of political experts from Russia arrived in the country. They provided financial support, protection and advice to those who the Kremlin thought should win the presidential elections⁶⁴. In addition to this, they organised disinformation campaigns on social media, supported protests and engaged some media outlets to create the impression that spontaneous election campaigns by politicians were taking place in Madagascar. Malagasy authorities tracked the threat and expelled those interfering in the elections from the country⁶⁵. However, a military cooperation agreement between Madagascar and the Russian Federation was signed in March 2022 and the Kremlin's influence on the island is discernible. This makes the risk of Russian mercenary involvement there still high.

Russian terrorism and counter-terrorism

The effectiveness of the Wagner Group in the fight against terrorism in Africa is highly debatable. Interventions by Russian mercenaries in Mali are not working and are leading to an increasing number of terrorist attacks. It is pointed out that the Wagnerists are not motivated to end the conflicts in which they participate, as they are driven by financial motivation. Even

⁶⁴ *Master and Chef. How Evgeny Prigozhin led the Russian offensive in Africa*, The Proekt team, 14 III 2023, <https://www.proekt.media/en/article-en/evgeny-prigozhin-africa/> [accessed: 5 XI 2023].

⁶⁵ A. Legucka, J. Czerep, *Wzrost zaangażowania Rosji w Afryce* (Eng. Increased Russian engagement in Africa), PISM, 20 XI 2019, https://pism.pl/publikacje/Wzrost_zaan_gazowania_Rosji_w_Afryce [accessed: 16 XII 2023].

when an operation ends or peace is achieved, military mercenaries are not like reservists who are only engaged when they are needed. Once an operation is over, mercenaries do not integrate and rebuild the state, but seek new employers and profit opportunities. The prolonged fight against terrorist threats is their way of earning⁶⁶.

Another important aspect is that the Russian Federation can carry out what are described as terrorist activities in Ukraine and Syria, among others. At the same time, the Wagner Group's activity in Africa, an extension of Russia's foreign policy, is maintained. The Kremlin, on the one hand, oversees private mercenary groups engaged to fight terrorism and, on the other, obliges Russian soldiers to undertake terrorist activities.

Reference should be made to the actual level of terrorist threat in countries where Russian mercenaries are present. Terrorist groups in the Sahel and the Horn of Africa are very adaptable⁶⁷. The survival of Al-Qaeda for more than 30 years, as well as the regular development of new organisations and groups (including the Islamic State and its cells) is evidence of the very high degree of resilience, proper planning and long-term strategy of these groups. The terrorists in Africa, intermingling with the rebels, are a very difficult opponent that no coalition (including those of Western countries) has been able to defeat. Most of the countries in which the Wagnerists operate are at very high risk of terrorism and its impact on state security⁶⁸.

The direction of counter-terrorism cooperation should be set by African countries, and their partners (the West in the broadest sense) should assist them in this. There is no 'one Africa', including in the dimension of counter-terrorism, because there are as many specificities as there are countries on the continent. One cannot compare the fight against terrorism in the Sahel with that in Mozambique. In countering terrorists and rebels, Russia is not in a position to provide effective support to African countries

⁶⁶ T. Mehra, M. Demuyneck, *Raising the stakes against the Wagner Group: From mercenaries to a designated terrorist group?*, ICCT, 17 I 2023, <https://www.icct.nl/publication/raising-stakes-against-wagner-group-mercenaries-designated-terrorist-group> [accessed: 16 XII 2023].

⁶⁷ J. Warner, *A View from the CT Foxhole: Idriss Mounir Lallali, Deputy Director, African Centre for the Study and Research on Terrorism (ACSRT)*, "CTC Sentinel" 2021, vol. 14, no. 5, <https://ctc.westpoint.edu/a-view-from-the-ct-foxhole-idriss-mounir-lallali-deputy-director-african-centre-for-the-study-and-research-on-terrorism-acsr/> [accessed: 16 XII 2023].

⁶⁸ *Global Terrorism Index 2023: Measuring the Impact of Terrorism*, Institute for Economics & Peace, Sydney, March 2023.

financially, militarily, technologically or, as described in the article, by delegating the Wagner Group.

Terrorism remains a huge problem in Africa. The presence on the continent of the Wagner Group, which makes good use of its imitated specialisation, i.e. counter-terrorism, to engage in a selected country, and which seeks to oppose Western countries, means that this threat will not disappear in the coming years. However, if the Wagnerists or other Russian mercenaries are perceived as incompetent or unreliable due to their lack of real impact on improving the security situation, African countries will abandon their services⁶⁹.

Ending and conclusions

The Kremlin will not give up building influence in Africa, as this would damage its growing position as a trusted partner to governments in need of support.

Currently, the Wagner Group is being absorbed by the Russian army and services⁷⁰. After Prigozhin's death, some of the Wagnerists dispersed to find employment in other mercenary groups, or set up their own businesses⁷¹. The important thing is, the group will not be disbanded – because of its position, which it has worked for several years. Some of the contracts, agreements and tasks will be transferred to other mercenary organisations influenced by the RF. Bullion mining in Africa allows, among other things, the financing of the war in Ukraine, and the Wagner Group's profits reach up to a billion dollars a year⁷².

⁶⁹ A. Kadlec, *In Africa, Wagner Is Not the Only Game in Town*, The New Lines Magazine, 17 VII 2023, <https://newlinesmag.com/spotlight/in-africa-wagner-is-not-the-only-game-in-town/> [accessed: 16 XII 2023].

⁷⁰ S. Rynn, K. Cockayne, *Where Next for Wagner Group in Africa?*, RUSI, 2 VIII 2023, <https://rusi.org/explore-our-research/publications/commentary/where-next-wagner-group-africa> [accessed: 16 XII 2023].

⁷¹ *Wagner Leadership Fractures After Prigozhin Death*, ADF, 17 X 2023, <https://adf-magazine.com/2023/10/wagner-leadership-fractures-after-prigozhin-death> [accessed: 26 XI 2023].

⁷² *Politico: Wagner Group capable of gaining \$1 billion from mining projects in Africa to finance war in Ukraine*, Kyiv Independent, 20 I 2023, <https://kyivindependent.com/politico-wagner-group-capable-of-gaining-1-billion-from-mining-projects-in-africa-to-finance-war-in-ukraine> [accessed: 16 XII 2023].

Giving Wagner's forces an official, strictly Russian character may be irrelevant in places such as Mali or the CAR, where they have been invited by those in power. But it may be quite different in Libya and Sudan, where such forces can be characterised as terrorists and potentially guilty of aggression against an internationally-backed government. This is not the message Moscow wants to send⁷³. Therefore, depending on the African country, the Kremlin manoeuvres based on whether or not it has ties to the Wagnerists. This undermines the legitimacy of any cooperation with the Russian Federation and this should be emphasised when dealing with African partners. In addition, it must be emphasised that the Wagnerists have no qualms about kill journalists who are interested in their presence in African countries, especially issues of resource extraction from diamond, gold and uranium mines⁷⁴.

Emerging suggestions about the Wagner Group's involvement in contemporary Africa can be divided into two categories: (1) actual minor involvement (confirmed in several source materials) and (2) alleged involvement (negligible past presence and likelihood of future involvement). The rationale for making such suggestions is based on activities such as arms sales from Russia, political cooperation as late as the turn of the 20th century, economic exchanges, emerging offers of training from Russian troops or mercenaries. In the context of actual Wagnerists involvement, South Sudan, Guinea, Burundi and Uganda can be pointed out, with the indication that the background to the mentions of cooperation of the indicated countries with Russian mercenaries is the cooperation of these countries with Russia, which indirectly implies the entry of Russian mercenaries. In the case of an alleged presence⁷⁵, countries such as Chad, Eswatini, Guinea-Bissau, DR Congo, Cameroon, Comoros, Botswana and Zimbabwe can be identified (Figure 2)⁷⁶.

⁷³ *All quiet on the Wagner front*, Africa Confidential, 6 VI 2023, https://www.africa-confidential.com/article-preview/id/14516/All_quiet_on_the_Wagner_front [accessed: 16 XII 2023].

⁷⁴ S. Ingber, *3 Russian Journalists Killed While Probing Reports Of Mercenaries In Africa*, NPR, 2 VIII 2018, <https://www.npr.org/2018/08/02/635046238/3-russian-journalists-killed-while-probing-reports-of-mercenaries-in-africa> [accessed: 15 XI 2023].

⁷⁵ In the form of, for example, visits by representatives of the Russian Ministry of Defence, the secret services or the Wagner Group instructors to countries where cooperation has developed or could develop.

⁷⁶ A. Askar, *The Increasing Presence and Role of Private Security Firms in Africa: The Russian Company "Wagner" as a Model*, EPC, 6 VI 2020, <https://epc.ae/en/details/featured/the-increasing-presence-and-role-of-private-security-firms-in-africa-the-russian-company->

When analysing the presence of Russian mercenaries in Africa, it is worth adding that one of the Kremlin's disinformation tools is to artificially create Russian power on the continent, as well as Russian inspirational activities must be kept in mind.



Figure 2. Countries in Africa where there can be little actual involvement or implied presence of the Wagner Group.

Source: own elaboration.

The Wagner Group remains Russia's force in Africa. This is nothing more than a substitute Russian military presence, carried out without

wagner-as-a-model [accessed: 29 XII 2023]; *Private military contractors bolster Russian influence in Africa*, France24, 4 II 2022, <https://www.france24.com/en/live-news/20220204-private-military-contractors-bolster-russian-influence-in-africa> [accessed: 29 XII 2023]; *Por qué el golpe de Estado en Níger puede ayudar a expandir la influencia del Grupo Wagner y Rusia en África*, BBC News Mundo, 29 VII 2023, <https://www.bbc.com/mundo/articulos/c3gz9v41xw9o> [accessed: 29 XII 2023].

the direct, official participation of the Russian armed forces (other than instructors) by a non-state paramilitary group with close ties to the Russian establishment. Russia (as a state) has bilateral and multilateral agreements and contracts with selected African states and entities. These include multi-million dollar technological, energy, military and economic projects. The Wagnerists, on the other hand, directly cooperate in selected countries or regions in Africa and their activities are of a completely different nature. It is, for example, profiting from protection, the implementation of specific missions, training and the acquisition of investments (including major mines). Russia and the Wagner Group are complementary in their impact on a particular African country.

The Russian Federation did not and does not have the economic potential to compete in Africa with the EU and, for example, China. In recent years, however, its involvement has shown that in the long term it is becoming a strong rival in certain areas and is pushing Western countries out of them⁷⁷. This is largely happening with the Wagner Group⁷⁸. Nowadays, the level of concern about the entry of Russian mercenaries into any African country is so high that when an attack or attempted attack takes place (as in 2023 in Sudan, Niger, Gabon or Sierra Leone, among others), questions about the Russian plot are immediately raised.

In the case of the Sahel countries, where the French Republic was previously present and the Wagner Group is now active, another perspective must also be taken into account. Some of the political and military elites of these countries have been reluctant to cooperate with France (and the West more broadly) and have thus become closer to Russia. Many mistakes have been made in relations with African partners and some of the accusations of Western countries taking undue advantage of their position are correct. Thus, the entry of the Wagner Group should be an important lesson in the process of further engaging in Africa, undertaking common ventures and highlighting the benefits of the continent's countries' cooperation with EU and NATO countries.

EU countries should first and foremost focus on a number of areas that are important in countering the Wagner Group and similar formations.

⁷⁷ A. Legucka, J. Czerep, *Wzrost zaangażowania Rosji w Afryce...*

⁷⁸ M. Bartosiewicz, *Kontrolowany chaos: rosyjska polityka wobec Afryki* (Eng. Controlled chaos: Russian policy towards Africa), OSW, 23 VIII 2023, <https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2023-08-23/kontrolowany-chaos-rosyjska-polityka-wobec-afryki> [accessed: 8 XII 2023].

The most important role in limiting their fundraising is to impose – on a global scale - sanctions on entities (and individuals) associated with both the Russian Federation and the Wagner Group. This should be done in cooperation with African partners. There should also be constant contact not only with those African countries that want to cooperate with the West, but also with those that currently have a closer relationship with Moscow (or Russian mercenaries). Explaining and describing the pernicious influence of the Wagnerists and the Kremlin's false promises should be part of the EU's permanent narrative. At the same time, African countries need to be offered alternative cooperation with EU partners.

Another element, also important for security, is the provision of military training (mainly counter-terrorism) to combat terrorism in Africa. In the author's opinion, limiting this phenomenon in this continent will allow to reduce the terrorist threats that have already been identified in the EU⁷⁹. The last aspect is the low efficiency and effectiveness of the Wagner Group in terms of actually fighting terrorism and maintaining security in African countries. Exposing the errors of Russian doctrine in Africa – which is also dealt with in this article – should be part of the information policy of Western countries. Efforts should be made to develop cooperation with the African continent and to minimise (as much as possible) the spread of conflicts, the effects of coups and terrorist attacks on several African countries. Indirectly, this will affect the security of Europe, the Middle East and Asia. The rivalry with the Russian Federation is now global and this is worth bearing in mind.

The international activities of the Wagner Group are also relevant for Poland. This is due not only to Poland's growing involvement in Africa, but also to the Russian aggression against Ukraine and harmful actions on the EU and NATO borders. Consequently, the planned development of Poland's diplomatic, political, economic, humanitarian, missionary and also military presence will depend on the operations carried out on the African continent by Russian mercenaries. The Polish authorities are reviewing where activity needs to be increased, bearing in mind the threats to Poland's interests. Civil war broke out in Sudan and Polish diplomatic personnel were withdrawn, but at the same time an outpost was opened in Rwanda and more than a dozen large economic projects were

⁷⁹ D. Szlachter, *Walka z terroryzmem w Unii Europejskiej – nowy impuls* (Eng. The fight against terrorism in the European Union – new impulse), Toruń 2006.

implemented on the African continent. Although challenges in Eastern Europe are currently a priority for Polish diplomacy, efforts to maintain regular contacts with African countries are simultaneous. In both cases, the Wagnerists represent a threat that must be taken into account. Russian mercenaries (PMC more broadly) can be used to control selected territories, being a kind of part of the Russian army.

It must be emphasised that the Wagner Group will grow. The Russian Federation and military mercenaries are connected and cooperative entities. There are more than 20 somewhat similar, less well-known, semi-state foreign private military companies in Russia. Chechen warlord Ramzan Kadyrov created the Akhmat group, there is also the Redut organisation (very active in the CAR), and Gazprom and Roskosmos have their investments in PMC. Russia will continue its expansion, using the Wagnerists for this purpose. It will certainly attempt to interfere in more countries – those where the rulers want to ‘maintain’ their power.

Bibliography

Global Terrorism Index 2023: Measuring the Impact of Terrorism, Institute for Economics & Peace, Sydney, March 2023.

Izak K., *Leksykon organizacji i ruchów islamistycznych* (Eng. Lexicon of Islamist organisations and movements), Warszawa 2014.

Olech A., *Ataki terrorystyczne w Federacji Rosyjskiej w XXI wieku* (Eng. Terrorist attacks in the Russian Federation in the 21st century), “Nowa Polityka Wschodnia” 2019, no. 4 (23), pp. 109–127.

Olech A., *Terrorist Threats to the Energy Sector in Africa and the Middle East*, in: *Countering Terrorism on Tomorrow’s Battlefield: Critical Infrastructure Security and Resiliency Handbook 2*, S.J. Lohman (ed.), December 2022.

Olech A., Rogozińska A., *Zagraniczne obiekty wojskowe jako system wzmacniania międzynarodowego potencjału militarnego Federacji Rosyjskiej* (Eng. Foreign military facilities as a system for strengthening the international military potential of the Russian Federation), Warszawa 2022.

Olech A., Wójtowicz B., *Rywalizacja o surowce w Sahelu – region konfliktu mocarstw* (Eng. Competition for resources in the Sahel – a region of conflict between powers), Warszawa 2022.

Szlachter D., *Walka z terroryzmem w Unii Europejskiej – nowy impuls* (Eng. The fight against terrorism in the European Union – new impulse), Toruń 2006.

Wójcik J., *Ekspansja dżihadu w Afryce: z Sahelu ku południu* (Eng. The expansion of jihad in Africa: from the Sahel towards the south), "Układ Sił" 2020, no. 20.

Internet sources

Aftandilian D., *The Fate of the Wagner Group in Syria, Libya, and Sudan*, Arab Center Washington DC, 18 VII 2023, <https://arabcenterdc.org/resource/the-fate-of-the-wagner-group-in-syria-libya-and-sudan/> [accessed: 23 XI 2023].

All quiet on the Wagner front, Africa Confidential, 6 VI 2023, https://www.africa-confidential.com/article-preview/id/14516/All_quiet_on_the_Wagner_front [accessed: 16 XII 2023].

Askar A., *The Increasing Presence and Role of Private Security Firms in Africa: The Russian Company "Wagner" as a Model*, EPC, 6 VI 2020, <https://epc.ae/en/details/featured/the-increasing-presence-and-role-of-private-security-firms-in-africa-the-russian-company-wagner-as-a-model> [accessed: 29 XII 2023].

Bartosiewicz M., *Kontrolowany chaos: rosyjska polityka wobec Afryki* (Eng. Controlled chaos: Russian policy towards Africa), OSW, 23 VIII 2023, <https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2023-08-23/kontrolowany-chaos-rosyjska-polityka-wobec-afryki> [accessed: 8 XII 2023].

Benjamin I., *Troops Kill 10 Terrorists, Recover Arms, Motorcycles*, Leadership, 5 XI 2023, <https://leadership.ng/troops-kill-10-terrorists-recover-arms-motorcycles> [accessed: 4 XII 2023].

Bensimon C. et al., *Au Sahel, l'insurmontable échec de la stratégie française*, Le monde, 3 XI 2023, https://www.lemonde.fr/afrique/article/2023/11/03/au-sahel-l-insurmontable-echec-de-la-strategie-francaise_6197973_3212.html [accessed: 28 XI 2023].

Bermudez J., Katz B., *Moscow's Next Front: Russia's Expanding Military Footprint in Libya*, Center for Strategic and International Studies, 17 VI 2020, <https://www.csis.org/analysis/moscows-next-front-russias-expanding-military-footprint-libya> [accessed: 9 XII 2023].

Black R., *Zelensky meets Sudanese official during 'technical stopover' in Ireland*, The Independent, 23 IX 2023, <https://www.independent.co.uk/news/uk/volodymyr-zelensky-north-america-ireland-joe-biden-department-of-foreign-affairs-b2417251.html> [accessed: 10 XII 2023].

Bobin F., *Coup de froid dans les relations entre l'Algérie et le Mali*, Le Monde, 27 XII 2023, https://www.lemonde.fr/afrique/article/2023/12/27/coup-de-froid-dans-les-relations-entre-l-algerie-et-le-mali_6207961_3212.html?fbclid=IwAR0ZDmZ-bfge7Wz-a4vIft4pVoLJzi1MmsUqe5LpaYFGYx85_966-Y9yrQ4Y [accessed: 27 XII 2023].

Bobin F., *La grande désillusion algérienne au Sahel*, Le Monde, 23 XI 2023, https://www.lemonde.fr/international/article/2023/11/23/la-grande-desillusion-algerienne-au-sahel_6201889_3210.html [accessed: 24 XI 2023].

Center for Preventive Action, *Civil Conflict in Libya?*, Council on Foreign Relations, 19 IX 2023, <https://www.cfr.org/global-conflict-tracker/conflict/civil-war-libya> [accessed: 23 XI 2023].

Central African Republic: President Touadéra meets Macron in France, Africa News, 13 IX 2023, <https://www.africanews.com/2023/09/13/central-african-republic-president-touadera-meets-macron-in-france> [accessed: 14 XI 2023].

Chan M., *Wagner mercenaries rescued Chinese gold miners in Central African Republic in July, paramilitary group says*, The South China Morning Post, 13 VII 2023, <https://www.scmp.com/news/china/military/article/3227490/wagner-mercenaries-rescued-chinese-gold-miners-central-african-republic-july-paramilitary-group-says> [accessed: 10 XI 2023].

Chason R., Debout B., *In Wagner's largest African outpost, Russia looks to tighten its grip*, The Washington Post, 18 IX 2023, <https://www.washingtonpost.com/world/2023/09/18/wagner-central-african-republic-touadera> [accessed: 5 XI 2023].

Chesnutt K., Zimmerman K., *The State of al Qaeda and ISIS Around the World*, Critical Threats, 8 IX 2022, <https://www.criticalthreats.org/analysis/the-state-of-al-qaeda-and-isis-around-the-world> [accessed: 5 XI 2023].

Country Reports on Terrorism 2020: Democratic Republic of the Congo, U.S. Department of State, <https://www.state.gov/reports/country-reports-on-terrorism-2020/democratic-republic-of-the-congo/> [accessed: 16 XII 2023].

Czerep J., *Afryka Subsaharyjska w strategii tzw. Państwa Islamskiego* (Eng. Sub-Saharan Africa in the strategy of the so-called Islamic State), PISM, 1 VIII 2022, <https://www.pism.pl/publikacje/afryka-subsaharyjska-w-strategii-tzw-panstwa-islamskiego> [accessed: 2 XI 2023].

Czerep J., *Erytrea nieformalnym reprezentantem prorosyjskich sił w Afryce* (Eng. Eritrea informal representative of pro-Russian forces in Africa), PISM, 22 III 2023,

<https://www.pism.pl/publikacje/erytrea-nieformalnym-reprezentantem-prorosyjskich-sil-w-afryce> [accessed: 28 XI 2023].

Czerep J., *Nowy front dżihadu w Mozambiku* (Eng. New jihadist front in Mozambique), PISM, 22 IX 2020, https://pism.pl/publikacje/Nowy_front_dzihadu_w_Mozambiku [accessed: 21 XI 2023].

Czerep J., *Perspektywy zakończenia wojny w Sudanie* (Eng. Prospects for ending the war in Sudan), PISM, 25 V 2023, <https://pism.pl/publikacje/perspektywy-zakonczenia-wojny-w-sudanie> [accessed: 23 XI 2023].

Czerep J., *Przyszłość misji ONZ w Afryce po wycofaniu MINUSMA z Mali* (Eng. The future of the UN mission in Africa after MINUSMA's withdrawal from Mali), PISM, 6 X 2023, <https://www.pism.pl/publikacje/przyszlosc-misji-onz-w-afryce-po-wycofaniu-minusma-z-mali> [accessed: 2 XI 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: 16 XI 2023].

Diallo T., *Mali signs agreement with Russia to build gold refinery*, Reuters, 22 XI 2023, <https://www.reuters.com/markets/commodities/mali-signs-agreement-with-russia-build-gold-refinery-2023-11-22/?rpc=401&> [accessed: 23 XI 2023].

Douet M., *Russia overtakes China as leading arms seller in sub-Saharan Africa*, Le Monde, 28 III 2023, https://www.lemonde.fr/en/le-monde-africa/article/2023/03/28/russia-overtakes-china-as-leading-arms-seller-in-sub-saharan-africa_6021018_124.html [accessed: 10 XII 2023].

Eydoux T., Savoye L., *Quand les forces spéciales ukrainiennes combattent des mercenaires russes de Wagner au Soudan*, Le Monde, 19 XI 2023, https://www.lemonde.fr/videos/video/2023/11/19/quand-les-forces-speciales-ukrainiennes-combattent-des-mercenaires-russes-de-wagner-au-soudan_6201120_1669088.html [accessed: 21 XI 2023].

Faulkner Ch., *Undermining Democracy and Exploiting Clients: The Wagner Group's Nefarious Activities in Africa*, "CTC Sentinel" 2022, vol. 15, no. 6, <https://ctc.westpoint.edu/wp-content/uploads/2022/06/CTC-SENTINEL-062022.pdf> [accessed: 4 XII 2023].

France to end Central African Republic military mission in 2016, France24, 30 III 2016, <https://www.france24.com/en/20160330-france-end-military-operations-central-african-republic> [accessed: 5 XI 2023].

Gadera K., *Mali: chaotyczny koniec MINUSMA, Azawad znów walczy o niepodległość* (Eng. Mali: chaotic end of MINUSMA, Azawad fights for independence again), *Konflikty.pl*, 9 XI 2023, <https://www.konflikty.pl/aktualnosci/wiadomosci/mali-azawad-niepodleglosc/> [accessed: 13 XI 2023].

Gadera K., *Wagnerowcy wycofują się z Mozambiku* (Eng. The Wagnerists withdraw from Mozambique), *Konflikty.pl*, 2 XII 2019, <https://www.konflikty.pl/aktualnosci/wiadomosci/wagnerowcy-wycofuja-sie-z-mozambiku/> [accessed: 22 XII 2023].

Goosen M., *Biggest Gold Producing Countries in Africa*, *Energy Capital Power*, 5 IX 2022, <https://energycapitalpower.com/biggest-gold-producing-countries-in-africa/> [accessed: 25 XI 2023].

Grynszpan E., *L'Ukraine tente de défier la Russie en Afrique*, *Le Monde*, 20 XI 2023, https://www.lemonde.fr/afrique/article/2023/11/20/l-ukraine-tente-de-defier-la-russie-en-afrique_6201324_3212.html [accessed: 22 XI 2023].

Gustafson K. et al., *Sudan: questions about Wagner Group involvement as another African country falls prey to Russian mercenaries*, Brunel University London, 2 V 2023, <https://www.brunel.ac.uk/news-and-events/news/articles/Sudan-questions-about-Wagner-Group-involvement-as-another-African-country-falls-prey-to-Russian-mercenaries> [accessed: 22 XI 2023].

Ingber S., *3 Russian Journalists Killed While Probing Reports of Mercenaries in Africa*, *NPR*, 2 VIII 2018, <https://www.npr.org/2018/08/02/635046238/3-russian-journalists-killed-while-probing-reports-of-mercenaries-in-africa> [accessed: 15 XI 2023].

IS group-linked militants kill 17 in Nigeria for failing to pay 'cattle tax', *France24*, 1 XI 2023, <https://www.france24.com/en/afrika/20231101-jihadists-kill-17-people-in-raid-on-remote-village-in-northeast-nigeria> [accessed: 4 XII 2023].

ISIS-Mozambique, *Counter Terrorism Guide*, November 2022, https://www.dni.gov/nctc/ftos/isis_mozambique_fto.html [accessed: 12 XII 2023].

Kacewicz M., *Do czego Putin potrzebuje Afryki i co może jej dać?* (Eng. What does Putin need Africa for and what can he give it?), *Belsat*, 28 VII 2023, <https://belsat.eu/pl/news/28-07-2023-do-czego-putin-potrzebuje-afryki-i-co-moze-jej-dac> [accessed: 18 XI 2023].

Kadlec A., *In Africa, Wagner Is Not the Only Game in Town*, *The New Lines Magazine*, 17 VII 2023, <https://newlinesmag.com/spotlight/in-africa-wagner-is-not-the-only-game-in-town/> [accessed: 16 XII 2023].

Kuczyński G., *Russia's Tatneft Discovers New Oil Field in Libya*, Warsaw Institute, 25 V 2023, <https://warsawinstitute.org/russias-tatneft-discovers-new-oil-field-in-libya/> [accessed: 21 XII 2023].

Kuwali D., *Oversight and Accountability to Improve Security Sector Governance in Africa*, Africa Center for Strategic Studies, 11 IX 2023, <https://africacenter.org/publication/asb42en-oversight-accountability-security-sector-governance> [accessed: 4 XII 2023].

Legucka A., Czerep J., *Wzrost zaangażowania Rosji w Afryce* (Eng. Increased Russian engagement in Africa), PISM, 20 XI 2019, https://www.pism.pl/publikacje/Wzrost_zaan_gazowania_Rosji_w_Afryce_ [accessed: 16 XII 2023].

Master and Chef. How Evgeny Prigozhin led the Russian offensive in Africa, The Proekt team, 14 III 2023, <https://www.proekt.media/en/article-en/evgeny-prigozhin-africa/> [accessed: 5 XI 2023].

Mehra T., Demuynck M., *Raising the stakes against the Wagner Group: From mercenaries to a designated terrorist group?*, ICCT, 17 I 2023, <https://www.icct.nl/publication/raising-stakes-against-wagner-group-mercenaries-designated-terrorist-group> [accessed: 16 XII 2023].

Mozambique, Global Centre for the Responsibility to Protect, 30 XI 2023, <https://www.globalr2p.org/countries/mozambique/> [accessed: 11 XII 2023].

Much ado about Kidal, Africa Confidential, 30 XI 2023, https://www.africa-confidential.com/article/id/14715/Much_ado_about_Kidal [accessed: 30 XI 2023].

Nasr W., *How the Wagner Group Is Aggravating the Jihadi Threat in the Sahel*, "CTC Sentinel" 2022, vol. 15, no. 11, <https://ctc.westpoint.edu/wp-content/uploads/2022/12/CTC-SENTINEL-112022.pdf> [accessed: 4 XII 2022].

Noulens M., *Général Frédéric Blachon au JDD: «Au Sahel, le risque d'une victoire des djihadistes est réel»*, Le Journal du Dimanche, 5 XI 2023, <https://www.lejdd.fr/international/general-frederic-blachon-au-jdd-au-sahel-le-risque-dune-victoire-des-djihadistes-est-reel-139434> [accessed: 6 XI 2023].

Olech A., *Afryka i Bliski Wschód w wymiarze bezpieczeństwa – podsumowanie 2022 roku* (Eng. Africa and the Middle East in the security dimension – 2022 summary), Defence24, 31 XII 2022, <https://defence24.pl/geopolityka/afryka-i-bliski-wschod-w-wymiarze-bezpieczenstwa-podsumowanie-2022-roku> [accessed: 18 XI 2023].

Olech A., *Francja wycofuje się z Mali i idzie na zachód Afryki [analiza]* (Eng. France withdraws from Mali and goes to West Africa [analysis]), *Defence24*, 14 VIII 2022, <https://defence24.pl/geopolityka/francja-wycofuje-sie-z-mali-i-idzie-na-zachod-afryki-analiza> [accessed: 18 XI 2023].

Olech A. et al., *Militarne zaangażowanie Federacji Rosyjskiej w Afryce. Zawarte porozumienia i umowy* (Eng. The Russian Federation's military engagement in Africa. Agreements and arrangements concluded), Instytut Nowej Europy, 23 V 2023, <https://ine.org.pl/militarne-zaangazowanie-federacji-rosyjskiej-w-afryce-zawarte-porozumienia-i-umowy/> [accessed: 10 XII 2023].

Olech A., Pawłowski M., *Wyzwania i szanse dla Europy w krajach Maghrebu [raport]* (Eng. Challenges and opportunities for Europe in the Maghreb [report]), Instytut Nowej Europy, 1 VII 2022, <https://ine.org.pl/wyzwania-i-szans-dla-europy-w-krajach-maghrebu/> [accessed: 4 XII 2022].

Otłowski T., *Wagner Group Activities in Libya and the Sahel Region After the Failed "Putsch" in Russia – Business as Usual*, Casimir Pulaski Foundation, 27 X 2023, <https://pulaski.pl/en/wagner-group-activities-in-libya-and-the-sahel-region-after-the-failed-putsch-in-russia-business-as-usual> [accessed: 25 XI 2023].

Peltier E., *Battle for Influence Rages in Heart of Wagner's Operations in Africa*, *The New York Times*, 26 XI 2023, <https://www.nytimes.com/2023/11/26/world/africa/wagner-russia-central-african-republic.html> [accessed: 15 XII 2023].

Penney J., *Rwanda Helped Oust Jihadists in Mozambique. Can This Model Work in West Africa?*, *PassBlue*, 16 VIII 2023, <https://www.passblue.com/2023/08/16/rwanda-helped-oust-jihadists-in-mozambique-can-it-work-as-a-counterinsurgency-model-in-west-africa/> [accessed: 14 XII 2023].

Politico: Wagner Group capable of gaining \$1 billion from mining projects in Africa to finance war in Ukraine, *The Kyiv Independent*, 20 I 2023, <https://kyivindependent.com/politico-wagner-group-capable-of-gaining-1-billion-from-mining-projects-in-africa-to-finance-war-in-ukraine> [accessed: 16 XII 2023].

Por qué el golpe de Estado en Níger puede ayudar a expandir la influencia del Grupo Wagner y Rusia en África, *BBC News Mundo*, 29 VII 2023, <https://www.bbc.com/mundo/articles/c3gz9v41xw9o> [accessed: 29 XII 2023].

Private military contractors bolster Russian influence in Africa, *France24*, 4 II 2022, <https://www.france24.com/en/live-news/20220204-private-military-contractors-bolster-russian-influence-in-africa> [accessed: 29 XII 2023].

Putin Gains Influence in Oil-Rich Libya as US Struggles to Oust Wagner Group, Bloomberg, 4 VI 2023, <https://www.bloomberg.com/news/articles/2023-06-04/putin-gains-in-oil-exporter-libya-as-us-struggles-to-oust-wagner-group#xj4y7vzkg> [accessed: 14 XII 2023].

Rampe W., *What Is Russia's Wagner Group Doing in Africa?*, Council on Foreign Relations, 23 V 2023, <https://www.cfr.org/in-brief/what-russias-wagner-group-doing-africahttps://www.cfr.org/in-brief/what-russias-wagner-group-doing-africa> [accessed: 21 XII 2023].

Rapport d'information par la Commission des Affaires Étrangères en conclusion des travaux d'une mission d'information constituée le 14 décembre 2022 sur les relations entre la France et l'Afrique, enregistré à la Présidence de l'Assemblée nationale le 8 novembre 2023, https://www.assemblee-nationale.fr/dyn/16/rapports/cion_afetr/l16b1841_rapport-information# [accessed: 23 XI 2023].

Roger B., *Au Burkina Faso, des militaires russes pour protéger Ibrahim Traoré?*, jeuneafrique, 17 XI 2023, <https://www.jeuneafrique.com/1503219/politique/au-burkina-faso-des-militaires-russes-pour-protoger-ibrahim-traore/> [accessed: 10 XII 2023].

Rolley S., *Islamic State affiliate expanding reach in DR Congo, UN Experts Say*, Reuters, 20 VI 2023, <https://www.reuters.com/world/africa/islamic-state-affiliate-expanding-reach-dr-congo-un-experts-say-2023-06-20/> [accessed: 17 XI 2023].

Russia Emerges as Top Weapons Supplier to Sub-Saharan Africa, ADF, 21 IV 2023, <https://adf-magazine.com/2023/04/russia-emerges-as-top-weapons-supplier-to-sub-saharan-africa> [accessed: 4 XII 2023].

Russia works with Libya on the creation of a military corps in Africa, Agenzia Nova, 17 XI 2023, <https://www.agenzianova.com/en/news/la-russia-lavora-con-la-libia-alla-creazione-di-un-corpo-militare-in-africa/> [accessed: 23 XI 2023].

Rynn S., Cockayne K., *Where Next for Wagner Group in Africa?*, RUSI, 2 VIII 2023, <https://rusi.org/explore-our-research/publications/commentary/where-next-wagner-group-africa> [accessed: 16 XII 2023].

Sadkiewicz S. (@StanSadkiewicz), X, 7 XI 2023, <https://twitter.com/StanSadkiewicz/status/1721882283916079351> [accessed: 7 XI 2023].

Sch lindwein S., *Are white mercenaries fighting in the DRC Conflict?*, Deutsche Welle, 17 I 2023, <https://www.dw.com/en/are-white-mercenaries-fighting-in-the-drc-conflict/a-64407711> [accessed: 16 XII 2023].

Serwat L., *Moving out of the shadows: Shifts in Wagner Group Operations Around the World*, ACLED, 2 VIII 2023, https://acleddata.com/acleddatanew/wp-content/uploads/2023/08/ACLED_Report_Shifts-in-Wagner-Group-Operations-Around-the-World_2023.pdf [accessed: 5 XI 2023].

Sharife K. et al., *Documents Reveal Wagner's Golden Ties to Sudanese Military Companies*, Organized Crime and Corruption Reporting Project, 2 XI 2022, <https://www.occrp.org/en/investigations/documents-reveal-wagners-golden-ties-to-sudanese-military-companies> [accessed: 4 XI 2023].

Sheludkova I., *Why is Russia's Wagner Group in Sudan, and what does it have to do with the war in Ukraine?*, EuroNews, 27 IV 2023, <https://www.euronews.com/2023/04/27/why-is-russias-wagner-group-in-sudan-and-what-does-it-have-to-do-with-the-war-in-ukraine/> [accessed: 16 XI 2023].

Shurkin M. (@MichaelShurkin), X, 22 XI 2023, <https://twitter.com/MichaelShurkin/status/1727337675806650866> [accessed: 22 XI 2023].

Sirleaf E., *UAE must cut ties with Sudan's war*, The Times, 27 XI 2023, <https://www.thetimes.co.uk/article/uae-must-cut-ties-with-sudans-war-czpwpm2n> [accessed: 27 XI 2023].

Sixto D., *Russian Mercenaries: A String of Failures in Africa*, Geopolitical Monitor, 24 VIII 2020, <https://www.geopoliticalmonitor.com/russian-mercenaries-a-string-of-failures-in-africa/> [accessed: 28 XI 2023].

South-west bias claims weaken Tinubu's standing, Africa Confidential, 30 XI 2023, https://www.africa-confidential.com/article/id/14716/South-west_bias_claims_weaken_Tinubu%27s_standing [accessed: 14 XII 2023].

State Department Terrorist Designations of ISIS Affiliates and Leaders in the Democratic Republic of the Congo and Mozambique, U.S. Department of State, 10 III 2023, <https://www.state.gov/state-department-terrorist-designations-of-isis-affiliates-and-leaders-in-the-democratic-republic-of-the-congo-and-mozambique/> [accessed: 12 XII 2023].

Sudan's President Bashir asks Putin for 'protection' from 'aggressive' US, France24, 23 XI 2017, <https://www.france24.com/en/20171123-sudan-president-bashir-asks-putin-protection-aggressive-us> [accessed: 16 XI 2023].

Touadéra stirs the geopolitical cauldron, Africa Confidential, 2 XI 2023, https://www.africa-confidential.com/article/id/14682/Touad%c3%a9ra_stirs_the_geopolitical_cauldron [accessed: 5 XI 2023].

Ukraine Expands Diplomatic Presence in Africa: New Embassy Launches in Ghana, The Kyiv Independent, 27 XII 2023, <https://www.kyivpost.com/post/26022/> [accessed: 29 XII 2023].

Wagner Group Terrorizing Sudanese Gold Miners, ADF, 19 VII 2022, <https://adf-magazine.com/2022/07/wagner-group-terrorizing-sudanese-gold-miners> [accessed: 4 XI 2023].

Wagner Group Uses Mafia-Style Tactics to Dominate CAR's Diamond Sector, ADF, 1 VIII 2023, <https://adf-magazine.com/2023/08/wagner-group-uses-mafia-style-tactics-to-dominate-cars-diamond-sector/> [accessed: 25 XI 2023].

Wagner Leadership Fractures After Prigozhin Death, ADF, 17 X 2023, <https://adf-magazine.com/2023/10/wagner-leadership-fractures-after-prigozhin-death> [accessed: 26 XI 2023].

Warner J., *A View from the CT Foxhole: Idriss Mounir Lallali, Deputy Director, African Centre for the Study and Research on Terrorism (ACSRT)*, "CTC Sentinel" 2021, vol. 14, no. 5, <https://ctc.westpoint.edu/a-view-from-the-ct-foxhole-idriss-mounir-lallali-deputy-director-african-centre-for-the-study-and-research-on-terrorism-acsr/> [accessed: 16 XII 2023].

Wintour P., *Fears for Libyan oil production amid military threats*, The Guardian, 4 VII 2023, <https://www.theguardian.com/world/2023/jul/04/fears-for-libyan-oil-production-amidmilitary-action-threats> [accessed: 13 XII 2023].

Aleksander Olech, PhD

Head of the International Cooperation Unit at Defence24. Lecturer at national and international universities, NATO associate, analyst, and publicist. Former Deputy Director of the Department of Africa and the Middle East at the Ministry of Foreign Affairs. Graduate of the European Academy of Diplomacy and the War Studies University. Main research interests: French-Russian relations, challenges in Africa, and NATO security policy.

Contact: a.olech@defence24.pl

Between armed conflict and state terrorism – specific individual restrictive measures adopted in Poland in the context of the war in Ukraine and the situation in Belarus. Legal perspective

MARIUSZ CICHOMSKI

Ministry of the Interior and Administration
Republic of Poland



<https://orcid.org/0000-0003-3707-7856>

Abstract

The aggression of the Russian Federation against Ukraine in 2022 and the actions of Belarus, both at the internal level and in support of Russia, have caused numerous changes in the geopolitical dimension, with consequences reaching beyond the European continent. They also resulted in the adoption of specific legal measures, both at the European Union and national levels, to counteract support for this aggression. The aim of this study is to present national legal solutions regarding restrictive measures against persons and entities that were introduced by *the Act on special solutions for counteracting support for aggression against Ukraine and for the protection of national security*. The article sets out their relationship to the mechanisms contained in European Union regulations and identifies the need for legal changes to adopt permanent systemic solutions for the application of national restrictive measures.

Keywords

sanctions, restrictive measures, sanctions list, freezing of financial resources, war in Ukraine

Armed conflict and state terrorism

The armed attack by the Russian Federation (RF) on Ukraine on 24 February 2022, which was a development of the 2014 actions that resulted in the annexation of the Crimean peninsula by Russia, was from the outset a military conflict conducted by the regular Russian army, with the support of various types of units and forces, including the Wagner Group. However, the manner in which Russia conducted its military operations and its involvement in other conflicts around the world quickly led to it being seen not only as the aggressor state of the armed conflict, but also as a state sponsoring or supporting terrorism, with the Russian authorities even being referred to as a terrorist regime. In this context, an important piece of European legislation is *the European Parliament resolution of 23 November 2022 on recognising the Russian Federation as a state sponsor of terrorism* (hereafter: Resolution of 23 November 2022). Within it, the European Parliament took into account the legal bases indicating the military nature of the conflict, including *the European Parliament resolution of 6 October 2022 on Russia's escalation of its war of aggression against Ukraine*, *the European Parliament resolution of 19 May 2022 on the fight against impunity for war crimes in Ukraine* and *the European Parliament resolution of 25 November 2021 on the human rights violations by private military and security companies, particularly the Wagner Group*. The parliament also took into account the United Nations Charter, the Convention on the Prevention and Punishment of the Crime of Genocide signed on 9 December 1948¹, IV Geneva Convention relative to the protection of civilian persons in time of war of 12 August 1949, or the Rome Statute of the International Criminal Court. The European Parliament also referred to international and EU regulations on preventing or combating terrorism, including the UN Security Council Resolution 2341 on the protection of critical infrastructure against terrorist acts (of 13 February 2017), the Convention on the Suppression of Terrorism of 27 January 1977², and international conventions adopted thereafter, as well as EU legislation on combating terrorism, including *the Council Common Position 2001/931/CFSP*

¹ *The Convention on the Prevention and Punishment of the Crime of Genocide adopted by the General Assembly of the United Nations on 9 December 1948 (ratified in accordance with the law of 18 July 1950) – (editor's note).*

² *The European Convention on the Suppression of Terrorism, drawn up in Strasbourg on 27 January 1977.*

of 27 December 2001 on the application of specific measures to combat terrorism and Council Regulation (EC) No. 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism.

The European Parliament, indicating the reasons for declaring Russia as a state sponsoring terrorism, in addition to the legal grounds mentioned, cited the factual premises justifying the adopted resolution of 23 November 2022. It indicated, *inter alia*, that:

(...) since 2014, and in particular after 24 February 2022, when Russia relaunched the illegal, unprovoked and unjustified war of aggression against Ukraine, its forces have conducted indiscriminate attacks against residential areas and civilian infrastructure, have killed thousands of Ukrainian civilians and carried out acts of terror throughout the country targeting various elements of civilian infrastructure such as residential areas, schools, hospitals, railway stations, theatres, and water and electricity networks³.

It was pointed out that Russia has for years supported and financed terrorist regimes and organisations, notably the Syrian regime of Bashar al-Assad, to which it has supplied weapons and in whose defence it has carried out deliberate attacks on Syrian civilians, cities and civilian infrastructure. Reference was made to attacks, including murders or attempted murders, on political opponents, including journalists, politicians, activists and foreign leaders. It was recalled that on 15 November 2022, a Dutch court convicted in absentia two Russians and a pro-Kremlin Ukrainian separatist for the murder of 298 people by shooting down a Malaysia airlines plane⁴.

The circumstances cited in the resolution of 23 November 2022 do not exhaust the rationale invoked to justify it, but unambiguously broaden the perception of Russia's actions, which are analysed not only from a strictly military perspective, but also in the context of state terrorism. It is noteworthy that the resolution refers to a statement made by the then Polish Minister of Foreign Affairs, Zbigniew Rau, then serving as Chairperson-in-Office of the Organisation for Security and Co-operation in Europe (OSCE), on 14 March 2022, who (...) *qualified the attacks by the Government*

³ The Resolution of 23 November 2022, letter A.

⁴ *Ibid.*, letter B, L, N.

of the Russian Federation against innocent civilians and civilian infrastructure in Ukraine as 'state terrorism'⁵.

This resolution stated that, although the European Union (EU) maintains a list of sanctioned individuals, groups and entities involved in terrorist acts, its existing legislation, unlike that of, for example, the United States or Canada, does not provide for the designation of an entire state as a sponsor of terrorism. In this context, the European Parliament

(...) calls for the EU and its Member States to develop an EU legal framework for the designation of states as sponsors of terrorism and states which use means of terrorism, which would trigger a number of significant restrictive measures against those countries and would have profound restrictive implications for EU relations with those countries; calls on the Council to subsequently consider adding the Russian Federation to such an EU list of state sponsors of terrorism; calls on the EU's partners to adopt similar measures⁶.

The European Parliament called for Russia and Belarus to be put on the EU's high-risk third country list on anti-money laundering and countering the financing of terrorism⁷.

The European Parliament further called on the EU and its Member States, as is obvious in circumstances of this kind, to take isolationist measures against Russia in the international arena, to (...) *include the Wagner Group and the 141st Special Motorized Regiment, also known as the Kadyrovites, as well as other Russian-funded armed groups, militias and proxies such as those active in the occupied territories of Ukraine, on the EU list of persons, groups and entities involved in terrorist acts (EU terrorist list)*⁸. He also called for the completion of another package of sanctions related to the freezing of financial resources, funds and economic resources of individuals and entities supporting the actions of Russia and Belarus. On sanctions, he called on both the European Commission (EC) and EU Member States to ensure the swift implementation and full enforcement of all individual and sectoral sanctions and to prevent their circumvention, as well as to investigate and prosecute perpetrators in such cases. There

⁵ Ibid., letter T.

⁶ Ibid., point 4.

⁷ Ibid., point 9.

⁸ Ibid., point 6.

was also a call that (...) *national penalties for breaching EU sanctions are effective, proportionate and dissuasive*⁹.

The basis for the introduction of a sanction mechanism at EU level is Article 29 of the *Treaty on European Union* (TUE)¹⁰, which allows the Council of the EU to impose restrictive measures (sanctions) against non-EU governments, non-state entities (e.g. companies) and individuals in order to bring about changes in their policies or actions. However, under Article 215(2) of the *Treaty on the Functioning of the European Union*¹¹, the Council may adopt the necessary measures to implement decisions adopted in accordance with Article 29 of the *Treaty on European Union* to ensure they are applied uniformly in all EU Member States¹².

The European Union imposes restrictive measures either as its own measures (i.e. autonomous sanctions) or to implement United Nations Security Council resolutions when third countries, natural or legal persons, groups or non-state entities fail to respect international law or human rights or pursue policies or actions contrary to the rule of law or democratic principles. The European Economic Community first applied such autonomous sanctions to the Union of Soviet Socialist Republics in 1982. Subsequently, they were imposed on China, Burma (Myanmar), Belarus, Indonesia, Zimbabwe, Uzbekistan or the breakaway territory of Transnistria. As Piotr Kobza emphasises: *In all these cases, the European Union has acted as an 'exporter of European values', particularly in the fields of democracy, the rule of law and human rights*¹³.

As envisaged, restrictive measures should not only be appropriate to the circumstances mandating their application, but also gradual, and their imposition requires political consensus at Member State level. However,

⁹ Ibid., point 7.

¹⁰ *The Treaty on European Union* (consolidated version) – Title V – General provisions on the Union's external action and specific provisions on the common foreign and security policy – Chapter 2 – Specific provisions on the common foreign and security policy – Section 1 – Common provisions – Article 29 (former article 15 of TEU).

¹¹ *The Treaty on the Functioning of the European Union* (consolidated version) – The Union's external actions – Title IV – Restrictive measures – Article 215 (former article 301 of Treaty Establishing the European Community).

¹² *General framework for EU sanctions*, <https://eur-lex.europa.eu/PL/legal-content/summary/general-framework-for-eu-sanctions.html> [accessed: 26 X 2023].

¹³ P. Kobza, *Środki restrykcyjne jako instrument Wspólnej Polityki Zagranicznej i Bezpieczeństwa Unii Europejskiej* (Eng. Restrictive measures as an instrument of the European Union's Common Foreign and Security Policy), "Studia Europejskie" 2006, no. 3, p. 22.

this is sometimes made difficult by the particular interests of states¹⁴. The main types of sanctions at the EU's disposal include diplomatic sanctions (such as expulsion of diplomats, suspension of official visits, bilateral or multilateral cooperation with the EU, boycott of sporting or cultural events) and economic and financial sanctions (arms embargoes, restrictions on imports and exports of certain products). Such restrictive measures may include:

- freezing of funds and economic resources owned or controlled by sanctioned persons or organisations (e.g. cash, bank deposits, shares, stocks) which cannot be moved, sold or accessed, and real estate which cannot be sold or rented,
- visa bans or travel bans preventing persons from entering the EU,
- sectoral bans, e.g. a ban on importing or exporting certain goods or technologies¹⁵.

In the context of the issues discussed in the article, the main legal acts at EU level in which restrictive measures are characterised are:

- *Council Regulation (EC) No 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine* (hereafter: Regulation 765/2006),
- *Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine* (hereafter: Regulation 269/2014),
- *Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*.

It is worth noting that Regulation 765/2006 and Regulation 269/2014 contain EU lists, applicable in all Member States, of persons and entities against whom restrictive measures (known as sanctions) have been imposed by freezing the assets of these entities and persons in connection with Russia's actions against Ukraine and the situation in Belarus. In addition, these regulations became the basis for the adoption of autonomous national

¹⁴ See in more detail: P. Pospieszna, *Sankcje Unii Europejskiej wobec Rosji: proces decyzyjny, trwałość i rola państw członkowskich* (Eng. European Union sanctions against Russia: decision-making process, sustainability and the role of Member States), "Rocznik Integracji Europejskiej" 2018, no. 12, pp. 311–321. <https://doi.org/10.14746/rie.2018.12.21>.

¹⁵ Ibid.

solutions in Poland, which concern specific restrictive measures against persons and entities supporting the actions of the Russian and Belarusian authorities, as discussed in more detail later in this article.

It should be noted that at the time of the European Parliament's resolution on the recognition of the Russian Federation as a state sponsoring terrorism, the parliaments or individual parliamentary chambers of some EU countries, i.e. Lithuania, Latvia, Estonia, Poland and the Czech Republic, had already adopted national counterparts to the resolution, i.e. documents of a declaratory rather than normative nature, recognising Russia as a terrorist or terrorist-sponsoring state or the current Russian regime as terrorist. In Poland, this was *the Resolution of the Senate of the Republic of Poland of 26 October 2022 on the recognition of the authorities of the Russian Federation as a terrorist regime*. It indicated, inter alia, that:

Russian invaders have been terrorising the populations of Ukrainian cities by shelling civilian targets: kindergartens, schools, theatres and residential estates. Bandits in Russian uniform have been torturing and murdering prisoners of war and civilians in the occupied territories. They abduct Ukrainian children to raise them as janissaries of the regime. They remove, resettle and send Ukrainian citizens to the most remote regions of Russia (...). We all know these acts of state terrorism well from the pages of history.

Therefore the Senate (...) *strongly condemns Russian aggression and calls on all countries which support peace, democracy and human rights to recognise the authorities of the Russian Federation as a terrorist regime*¹⁶.

Less than two months later, the Sejm passed a similar resolution on the recognition of the Russian Federation as a state supporting terrorism¹⁷. Within it, the Sejm referred, as the European Parliament had done earlier in the resolution, inter alia to Russia's direct responsibility for the downing of the Malaysian airliner in July 2014 or the Russian Federation's perpetration of terrorist acts against civilian infrastructure, mass executions, abductions, sexual violence and torture, separation of children from their families to subject them to Russification, mass deportations of the population, forced conscription of Ukrainian citizens into the Russian armed forces

¹⁶ The Resolution of the Senate of the Republic of Poland of 26 October 2022 on the recognition of the authorities of the Russian Federation as a terrorist regime.

¹⁷ The Resolution of the Sejm of the Republic of Poland of 14 December 2022 on the recognition of the Russian Federation as a state supporting terrorism.

and looting of property. The Sejm called on the Council of Ministers to continue and intensify its efforts to impose further sanctions packages on the Russian Federation and those supporting Vladimir Putin's regime, as well as further material and political support for Ukraine in its fight against the aggressor.

In Poland, the response to the actions of Russia and its supporter Belarus on a normative rather than declarative level was the adoption of the *Act of 13 April 2022 on specific solutions to counteracting support for aggression against Ukraine and to protect national security* (hereafter: Sanctions Act). It created, inter alia, a national mechanism to freeze the financial resources, funds and economic resources of persons and entities linked directly or indirectly to the regimes in Russia and Belarus and meeting certain criteria for such a link. These solutions were adopted earlier than the aforementioned resolution of the European Parliament and resolutions of the Polish Sejm and Senate, while they were closely correlated with Regulations 765/2006 and 269/2014, which were in force at the time and subsequently amended as part of successive EU sanctions packages. The subsequent application of the law was in line with the perception of the Russian Federation as a state that supports or finances terrorism, as indicated in the cited resolutions and decisions, by using as one of the restrictive measures the mechanism of freezing the assets of persons and entities. This was a typical instrument used to counter terrorist financing and money laundering, although it had already been used by the EU as a restrictive measure in relation to other countries. Sanctions against terrorism are (...) *administrative, and parallel (e.g. to the confiscation of assets in criminal proceedings) actions by mandatory institutions, intended to prevent perpetrators from using assets for criminal terrorist activities*¹⁸.

It should be stressed that the very notion of sanctions is in this respect a major simplification that should be seen as a mental shortcut, even though both the act and the list of persons and entities it lists, the decisions it imposes or the restrictive measures it applies are usually referred to respectively as "sanctions act", "sanctions list", "sanctions decisions" or "sanctions measures". This is also used for the purposes of this article, and these terms

¹⁸ M.A. Kędzierski, *Szczególne środki ograniczające i sankcje jako forma przeciwdziałania wobec podmiotów terrorystycznych na tle polskiego ustawodawstwa (część 1)* (Eng. Specific restrictive measures and sanctions as a form of counteraction against terrorist entities against the background of Polish legislation (part 1)), "Prokuratura i Prawo" 2021, no. 10, pp. 22–23.

are also commonly used at EU level, for example within the framework of the previously cited resolution¹⁹. The purpose for which - on the basis of Polish or EU legislation adopted - the instruments of freezing funds, resources or economic resources are used is not punitive but preventive, so it is more appropriate here to use the term 'restrictive measure', which is usually used interchangeably. Its application prevents the transfer of assets that could finance aggression against Ukraine or violations of human rights and the fight against democratic opposition in Russia and Belarus, but it should not be seen as an instrument to punish such actors. While its effect may be, for example, to prevent economic activity, it is intended to have a temporary effect. The entity subject to the freezing of funds does not expose itself to financial liability in criminal or criminal-administrative terms as long as it does not break the imposed ban. In Polish terms, restrictive measures are a unilateral instrument of state foreign policy (...) *consisting in taking action to restrict or suspend normal relations with another state, in response to its unacceptable actions, both external and internal*²⁰.

Similar observations were made by the EC in its opinion of 19 June 2020 on Article 2 of Council Regulation 269/2014 (response to question 2.5), according to which:

Restrictive measures are neither punitive nor confiscatory in nature, but preventive instruments. Article 4(1)(c) of the Regulation [269/2014 – author's note], which establishes a derogation from the financial restrictions set out in Article 2, allows national competent authorities to authorise the release of certain frozen funds or economic resources, or the making available of certain funds or economic resources, after having determined that these are intended exclusively for payment of fees or service charges for routine holding or maintenance of frozen funds or economic resources²¹.

¹⁹ On the relationship between the concepts of sanctions, restrictive measures and retaliatory measures at EU level, see in more detail: P. Kobza, *Środki restrykcyjne jako instrument...*, pp. 10–14. The topic of the origins of the concept of sanctions in the dimension of international law was addressed in the: M. Sułek, *Zachodnie sankcje wobec Rosji – sens i skuteczność* (Eng. Western sanctions against Russia - sense and effectiveness), "Rocznik Strategiczny" 2014/2015, vol. 20, pp. 398–400.

²⁰ Ibid.

²¹ *Commission Opinion of 19 June 2020 on Article 2 of Council Regulation (EU) No 269/2014*, Brussels, 19 VI 2020, C (2020) 4117 final, p. 6. An analogous opinion in this regard is given in paragraph 28 of the document *Aktualizacja dobrych praktyk UE w zakresie skutecznego wprowadzania w życie środków ograniczających* (Eng. Update on EU good practice in

Research assumptions

The purpose of this article is to discuss individual restrictive measures introduced in Poland by the Sanctions Act and to show their relation to the mechanisms contained in the EU regulations, as well as to present the scale and manner in which these instruments are used in practice. The special nature of the Sanctions Act is worth noting, which is highlighted already in the very title of this piece of legislation. In this context, the research questions arise - what is the special nature of the Act, whether it should be seen from the perspective of the circumstances of the origin of this regulation or the subject or object scope of its standardisation, or perhaps both the substantive and procedural nature of the provisions contained therein.

The aforementioned perception of the conflict in Ukraine also in the context of state terrorism, and not only from a military perspective, harmonises with the application of similar preventive mechanisms, which are asset-freezing measures typical for countering terrorist financing and money laundering. On the Polish ground, this mechanism had already been introduced earlier, i.e. in *the Act of 1 March 2018 on counteracting money laundering and terrorist financing*, however, it has not been used in practice. The first decisions of the General Inspector of Financial Information (GIFI) on inclusion in the list of persons and entities subject to specific restrictive measures under the Act²², were not issued until 26 September 2023, while the first decisions under the Sanctions Act - already on 25 April 2022.

Due to the comprehensiveness of the issue under discussion, the article omits the issue of the network of dependencies between entities and persons to whom restrictive measures were applied, which is worth a separate and detailed discussion. Neither was reference made to the issue of the structure of their direct or indirect links with the state apparatuses of Russia and Belarus or the persons and economic entities associated with them. It is worth noting that the scope of the law goes beyond the issue of individual restrictive measures applied to specific persons and economic entities affected by the solutions adopted in this law. Indeed, it also includes sectoral sanctions (relating to the ban on

the effective implementation of restrictive measures), Brussels, 4 V 2018, document no. 8519/18, <http://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/pl/pdf> [accessed: 30 X 2023].

²² On the basis of Article 104 § 1 the Act of 14 June 1960 – Code of Administrative Procedure – in relations to Article 120 of the Act on counteracting money laundering and terrorist financing.

the circulation of coal of Russian or Belarusian origin), provisions ensuring the application of the aforementioned EU regulations (i.e. provisions defining the competence of the authorities, procedural provisions and provisions sanctioning the violation of EU restrictive measures) and criminal provisions penalising the application, use or promotion of symbols or names supporting the aggression of the Russian Federation against Ukraine.

The issue of individual restrictive measures introduced in Poland in the context of Russia's aggression towards Ukraine and the situation in Belarus, as opposed to the issue of the application of sanctions at EU or UN level, had not been the subject of scientific publications²³ at the time of preparing this article, therefore, the sources in this case are generally available normative acts, EU guidelines, decisions of the minister in charge of internal affairs, as well as judgements of the Voivodeship Administrative Court (VAC) in Warsaw and decisions of the Supreme Administrative Court (SAC) issued in specific cases (as at the date of preparing this publication, the SAC had not yet issued judgements in the discussed scope).

The relationship between the individual restrictive measures adopted in Poland and the EU

The national solutions for the determination of individual restrictive measures adopted in the Sanctions Act are based on a list, maintained by the minister responsible for internal affairs, of persons and entities against whom, inter alia, the measures set out in Article 2(1)-(3) of Regulation 765/2006 and Articles 2 and 9 of Regulation 269/2014 are applied (hereinafter: sanctions list or list). The entry on the list, which is publicly available and published in the Bulletin of Public Information (BIP)²⁴, is preceded by

²³ The magazine "Prokuratura i Prawo" (2023, no. 6) published the article by Andrzej Lewny entitled *Kiedy wojenny zapal może zaszkodzić. Kilka uwag o przestępstwie z art. 16 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego* (Eng. When war fervour can cause harm. Some comments on the offence of Article 16 of the Act of 13 April 2022 on Specific Solutions to Counteracting Support for Aggression against Ukraine and to Protect National Security), however, it does not address the issue of individual restrictive measures discussed in this article.

²⁴ *List of sanctioned persons and entities*, Ministry of the Interior and Administration, <https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami> [accessed: 30 X 2023].

an individualised decision of the minister responsible for internal affairs, which is appealable to the administrative court.

According to the cited Article 2(1)-(3) of Regulation 765/2006, freezing of financial resources shall consist of freezing all funds (i.e. preventing any move, transfer, alteration, use of, access to, or dealing with funds in any way that would result in any change in their volume, amount, location, ownership, possession, character, destination or other change that would enable the use of the funds, including portfolio management²⁵) and economic resources belonging to, owned, held or controlled by the natural or legal persons, entities and bodies listed on the sanctions list. Except that economic resources means assets of every kind, whether tangible or intangible, movable or immovable, which are not funds but can be used to obtain funds, goods or services. To freeze economic resources is to prevent their use to obtain funds, goods or services in any way, including, but not limited to, by selling, hiring or mortgaging them²⁶.

In accordance with Regulation 765/2006, no funds or economic resources may be made available, directly or indirectly, to listed natural or legal persons, entities or bodies. The participation, knowingly and intentionally, in activities the object or effect of which is, directly or indirectly, to circumvent the restrictive measures shall also be prohibited²⁷.

A slightly different conceptual apparatus, which does not differentiate between the effects of the regulation, is used in Article 2 of Regulation 269/2014. According to it, all funds²⁸ (Regulation 765/2006 refers, as

²⁵ Article 1(2) of Regulation 765/2006.

²⁶ Article 1(4) of Regulation 765/2006.

²⁷ On the basis of Explanatory Memorandum to *the Government Draft Act on specific solutions in counteracting the promotion of aggression against Ukraine and serving to protect national security*, Print no. 2131, pp. 6–8, <https://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=2131> [accessed: 18 X 2023].

²⁸ According to Article 1(1) of Regulation 765/2006 funds means financial assets and benefits of every kind, including cash, cheques, claims on money, drafts, money orders and other payment instruments; deposits with financial institutions or other entities, balances on accounts, debts and debt obligations; publicly- and privately-traded securities and debt instruments, including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures and derivatives contracts; interest, dividends or other income on or value accruing from or generated by assets; credit, right of set-off, guarantees, performance bonds or other financial commitments; letters of credit, bills of lading, bills of sale; documents evidencing an interest in funds or financial resources.

mentioned, to funds²⁹) and economic resources belonging to, owned, held or controlled by indicated on the list any natural persons or natural or legal persons, entities or bodies associated with them indicated in the sanctions list shall be frozen. Similarly, no funds or economic resources shall be made available, directly or indirectly, to or for the benefit of natural persons or natural or legal persons, entities or bodies associated with them indicated on the list.

As the Sanctions Act refers explicitly to EU regulations, the relationship between the two legal orders requires comment. As stated in the explanatory memorandum: *The proposed law, based on selected legal instruments contained in Regulation 765/2006 and Regulation 269/2014, will introduce, under national law, a list of persons and entities, separate from the lists contained in these regulations, to whom the certain restrictive measures specified in these regulations apply*³⁰. The Sanctions Act is therefore a self-standing piece of national legislation based on EU mechanisms for the application of individual restrictive measures. It also contains a standard to prevent duplication of the restrictive measures imposed, which is set out in Article 2(2). According to this provision, the scope of measures applied to listed persons and entities may not duplicate the scope of measures set out in Regulation 765/2006 or Regulation 269/2014.

The introduction of national solutions alongside EU law, resulting in a Polish sanctions list separate from the EU list, is in line with Article 4(2) of *the Treaty on European Union* of 7 February 1992, according to which:

The Union respects the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It respects their essential state functions, including ensuring the territorial integrity of the state, maintaining law and

²⁹ Financial resources within the meaning of Article 1(g) of Regulation 269/2014 shall mean financial assets and benefits of every kind, including cash, cheques, claims on money, drafts, money orders and other payment instruments; deposits with financial institutions or other entities, balances on accounts, debts and debt obligations; publicly- and privately-traded securities and debt instruments, including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures and derivatives contracts; interest, dividends or other income on or value accruing from or generated by assets; credit, right of set-off, guarantees, performance bonds or other financial commitments; letters of credit, bills of lading, bills of sale and documents showing evidence of an interest in funds or financial resources.

³⁰ Explanatory Memorandum to *the Government Draft Act on specific solutions...*, p. 4.

order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

The legitimacy of considering the Act from a national security perspective is indicated by its very title – (...) *to protect national security*, although references to this concept are also found in individual provisions explicitly invoking the national security rationale (Articles 3(4) and 8 of the Sanctions Act).

It is also worth recalling here *Update of the EU Best Practices for the effective implementation of restrictive measures* adopted by the Council of the EU, in which point 25 explicitly states:

In addition to legislation adopted by the Union, Member States should, if necessary, have in place additional legislative framework, laws or regulations to freeze funds and financial assets and economic resources of persons and entities subject to restrictive measures on national level, including persons or entities involved in terrorist acts, and to prohibit the making available of funds and economic resources to or for the benefit of such persons and entities, in particular by way of administrative freezing measures or through the use of judicial freezing orders having equivalent effects³¹.

Although this document is not normative in nature, it provides a basis for interpreting the application of restrictive measures, including in relation to Regulations 765/2006 and 269/2014. Significantly in the context of these solutions and the search for analogies to the solutions adopted in the field of countering terrorist financing, it further emphasises that the solutions for restrictive measures should be in line with the standards of The Financial Action Task Force (FATF), in particular with the 6th recommendation on targeted financial sanctions related to terrorism and terrorist financing. The Act on counteracting money laundering and terrorist financing³² and the Sanctions Act are precisely the implementation of these objectives on the Polish ground.

³¹ *Update of the EU Best Practices...*

³² See in more detail: M.A. Kędziński, *Szczególne środki ograniczające i sankcje... (część 1)*; the same, *Szczególne środki ograniczające i sankcje jako forma przeciwdziałania wobec podmiotów terrorystycznych na tle polskiego ustawodawstwa (część 2)* (Eng. Specific restrictive measures and sanctions ... (Part 1)); idem, *Specific restrictive measures and sanctions as a form of counteraction against terrorist entities against the background of Polish legislation (Part 2)*, "Prokuratura i Prawo" 2021, no. 11, pp. 36–55.

The issue of the autonomy of the Sanctions Act in relation to the EU regulations, despite the use in national legislation of the mechanisms contained in these regulations, is also raised by the Minister of the Interior and Administration in the sanctions decisions he issues:

From the outset, Poland strongly condemned Russia's aggression against Ukraine and human rights violations in Belarus, while pointing out the need for far-reaching and effective sanctions, with wide-ranging consequences for both the Russian Federation and Belarus cooperating with it. It is for these reasons that a legislative initiative has been taken, resulting in the Act of 13 April 2022 on specific solutions to counteracting support for aggression against Ukraine and to protect national security, which, it should be reiterated, while relying only on the sanction mechanisms set out in the aforementioned EU regulations, creates separate, national sanction solutions³³.

The Minister of the Interior and Administration also stated that: (...) *in particular, national security remains the exclusive responsibility of each Member State. Thus, European law does not exclude the possibility of measures taken by a Member State on grounds of national security, in particular by a state in such a specific and difficult geopolitical situation as the Republic of Poland, which is not experienced by states located far from a war zone*³⁴.

The Sanctions Act, however, not only creates a separate national system for imposing restrictive measures on persons and entities supporting the actions of the Russian Federation or Belarus, but also, within the framework of the provisions adopted therein, ensures the application of the aforementioned EU regulations. The explanatory memorandum of the Act indicates that: *The amendments to the sanctions regulations introduced after the aggression of the Russian Federation against Ukraine require legislative action related to the unambiguous regulation of the question of the authority taking decisions on the unfreezing of certain financial measures or economic resources*³⁵.

³³ Decision of the Minister of the Interior and Administration of 29 August 2023 DPP-TPZ.0272.2.2023.AK(38), Decision of refusal – Timur Rashidov, p. 9, <https://www.gov.pl/web/mswia/decyzje-ministra-swia-w-sprawie-wpisu-na-liste-sankcyjna> [accessed: 22 X 2023].

³⁴ *Ibid.*, p. 10.

³⁵ Explanatory Memorandum to *the Government Draft Act on specific solutions...*, p. 4.

Member States' obligations in this regard derive from treaty law. In accordance with Article 291(1) of *the Treaty on the Functioning of the European Union* Member States shall adopt all measures of national law necessary to implement legally binding Union acts. Similarly, the *Treaty on European Union*, in the second sentence of Article 4(3), indicates that the Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the treaties or resulting from the acts of the institutions of the Union.

The scope of the implementation Regulation 269/2014 by the Sanctions Act must also be referred to the implementation of the disposition of its Article 15(1), according to which (...) *Member States shall lay down the rules on penalties applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented*. In turn, the first sentence of Article 9(1) of Regulation 765/2006 indicates that: *Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented*. These provisions therefore concern the regulation of the competent authority that decides to unfreeze certain financial or economic resources and is responsible for imposing penalties for non-compliance with the restrictive measures imposed.

The scope of the implementation of the EU Sanctions Regulations by the Sanctions Act is therefore reduced to the changes introduced by Article 19 of that Act in *the National Revenue Administration Act of 16 November 2016*. In, inter alia, *Section V a*, which was added on this basis, the Head of the National Revenue Administration (NRA) was designated as the competent authority to decide on the application of derogations from individual restrictive measures imposed under the EU Sanctions Regulations (release of frozen funds or economic resources or making funds or economic resources available) and to impose fines for non-compliance with these measures.

The power granted to the NRA to authorise the release of certain frozen funds or economic resources or to make available certain funds or economic resources in respect of sanctioned persons and entities shall be exercised upon a determination that the funds and economic resources in question are, inter alia:

- necessary to satisfy the basic needs of natural or legal persons, sanctioned entities or bodies and their dependent family members, including payments for foodstuffs, rent or mortgage, medicines

- and medical treatment, taxes, insurance premiums, and public utility charges,
- intended exclusively for payment of reasonable professional fees or reimbursement of incurred expenses associated with the provision of legal services,
- intended exclusively for payment of fees or service charges for routine holding or maintenance of frozen funds or economic resources.

In addition, Article 6 of the Sanctions Act indicates, *inter alia*, that a person or entity who, with respect to a listed person or entity, fails to comply with the obligation to freeze funds, funds or economic resources or the prohibition on making them available, or fails to comply with the prohibition on knowingly and intentionally participating in activities the purpose or effect of which is to circumvent the application of the measures set out in these regulations, shall be subject to a fine of up to PLN 20 million imposed by the head of the customs and tax office.

Individual restrictive measures adopted in Poland

According to Article 1 of the Sanctions Act, persons and entities included in the sanctions list shall be subject to:

- respectively the measures set out in Article 2(1)-(3) of Regulation 765/2006 (in view of the situation in Belarus and its involvement in Russia's aggression against Ukraine), *i.e.*:
 - all funds and economic resources belonging to, owned, held or controlled by natural or legal persons, entities and bodies listed on the sanctions list maintained by the minister responsible for internal affairs shall be frozen,
 - no funds or economic resources shall be made available, directly or indirectly, to or for the benefit of natural or legal persons, entities or bodies listed on the sanctions list,
 - the participation, knowingly and intentionally, in activities the object or effect of which is, directly or indirectly, to circumvent the aforementioned measures shall be prohibited;
- respectively the measures set out in Article 2 and Article 9 of Regulation 269/2014 (in relation to Russia's actions), *i.e.*:

- all funds and economic resources belonging to, owned, held or controlled by any natural persons or natural or legal persons, entities or bodies associated with them listed on the sanctions list shall be frozen,
 - no funds or economic resources shall be made available, directly or indirectly, to or for the benefit of natural persons or natural or legal persons, entities or bodies associated with them listed on the sanctions list,
 - it shall be prohibited to participate, knowingly and intentionally, in activities the object or effect of which is to circumvent the aforementioned measures;
- exclusion from a public procurement procedure or competition conducted under *the Act of 11 September 2019 - public procurement law*;
 - entry in the list of foreigners whose stay on the territory of the Republic of Poland is undesirable, referred to in Article 434 of *the Act of 12 December 2013 on foreigners*.

The first two types of individual restrictive measures are taken directly from EU regulations and both relate to asset freezing, while they differ in their purpose of application (linking to Belarus or Russia). The other two, on the other hand, are of a separate nature based on national legislation, i.e. the Act - public procurement law and the Act on foreigners.

In undertaking an assessment of the nature of individual restrictive measures adopted by the legislature to freeze assets, following the explanatory memorandum to the bill, it should be pointed out that:

(...) the project concerns only the so-called freezing of property, i.e. the temporary inability to dispose of it. It does not imply the deduction of property, which, on the grounds of the Constitution of the Republic of Poland, may be carried out only within the framework of expropriation (for a public purpose and with just compensation - Article 21 of the Constitution) or forfeiture (adjudicated with a final court decision - Article 46 of the Constitution). This is an action that is already envisaged within the Polish legal order, whether by a directly effective EU regulation or by the Act on counteracting money laundering and terrorist and falls within the framework extended by the Constitution of the RP³⁶.

³⁶ Explanatory Memorandum to *the Government Draft Act on specific solutions...*, p. 7.

In this context, it is also worth noting the wording of the justification of the judgement of the VAC in Warsaw in the case of the deletion of one of the entities on the Polish sanctions list:

The Act of 13 April 2022 on specific solutions to counteracting support for aggression against Ukraine and to protect national security is a special piece of legislation, as it regulates an extremely important issue, namely to counter support for aggression against Ukraine and to serve the protection of national security. These two main objectives have become a priority for the legislator, and the provisions of the Act should be read through their prism. Possible negative consequences for a particular listed entity cannot constitute grounds for repealing the decision, as this would be contrary to the ratio legis of the law in question and would not serve its main objectives. At the same time, it is obvious that the Act of 13 April 2022 has a repressive, sanctioning character and it is difficult to expect that the application of its provisions to a specific entity would not have negative consequences for that entity³⁷.

Furthermore, in the justification of one of the decisions dismissing the complaint against the failure to suspend the enforceability of the sanction decision, the SAC indicated that (...) *the Act concerns the so-called "freezing of assets", i.e. the temporary inability to dispose of these assets. This does not imply deprivation of the company's right to property, which, in the light of Article 21(2) of the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws no. 78, item 483, as amended), is only permissible if it is done for a public purpose and against just compensation or forfeiture ordered by a final court decision (Article 46 of the Constitution)*³⁸.

The freezing of financial resources, funds or economic resources is therefore a basic, but not the only instrument for influencing persons and entities on the Polish sanctions list. With regard to the sanction of exclusion from a procedure or a competition conducted on the basis of the public procurement law, which is not provided for in Regulations 765/2006 and 269/2014, control of the award of contracts is exercised in accordance with Article 596 of that law, and the persons or entities subject to exclusion,

³⁷ Judgement of the Voivodeship Administrative Court in Warsaw of 18 V 2023, ref. no. I SA/Wa 2524/22. An analogous statement was also made in other judgements of the VAC in Warsaw, e.g. the judgement of the VAC in Warsaw of 4 VII 2023, ref. no. I SA/Wa 2528/22.

³⁸ Decision of the Supreme Administrative Court of 9 V 2023, ref. no. III OZ 207/23.

who join public procurement procedures and competitions, are subject to a fine of up to PLN 20 million imposed by the President of the Public Procurement Office.

Exclusion from the procurement procedure or design contest applies to:

- the economic operator and the design contest participant included in the lists referred to in Regulations 765/2006 and 269/2014,
- the economic operator and the design contest participant whose beneficial owner,
- within the meaning of the Act on counteracting money laundering and terrorist financing is a person or entity listed in the lists set out in the regulations mentioned in Article 1 of the Act or included in the Polish sanctions list,
- the economic operator and the design contest participant whose parent company within the meaning of Article 3(1)(37) of the Accounting Act of 29 September 1994 is an entity listed in the lists set out in Regulations 765/2006 and 269/2014 or listed or being such a parent company as from 24 February 2022, provided that it has been listed on the basis of a decision on its inclusion in the Polish sanctions list deciding on the application of the measure in question³⁹.

In the context of individual restrictive measure in the form of an entry on the list of foreigners whose residence on the territory of the Republic of Poland is undesirable, it is worth noting that the entry is made *ex officio* by the Head of the Office for Foreigners in the case this measure is indicated in a decision issued by the Minister of the Interior and Administration. The practice of issuing such decisions indicates that in the vast majority this instrument is not used independently, but together with other individual restrictive measures, i.e. freezing of assets or prohibition of participation in proceedings and competitions conducted on the basis of the public procurement law. The Head of the Office transfers the data of a foreigner, for the period of their retention in the list, to the Schengen Information System for the purpose of refusing entry and stay not only in Poland, but also throughout the EU.

³⁹ Article 7(1) of the Sanctions Act.

Conditions for inclusion in the Polish sanctions list

The most important issue related to the analysis of the Polish solutions for individual restrictive measures is the determination of the conditions for entry on the sanctions list. According to the statutory solutions, the minister in charge of internal affairs shall decide on the entry with regard to persons and entities with financial means, funds and economic resources within the meaning of Regulation 765/2006 or Regulation 269/2014, directly or indirectly supporting:

- 1) the aggression of the Russian Federation against Ukraine beginning on 24 February 2022 or
- 2) serious violations of human rights or repression of civil society and democratic opposition, or whose activities constitute another serious threat to democracy or the rule of law in the Russian Federation or Belarus
 - or directly linked to such persons or entities, in particular by personal, organisational, economic or financial links, or who are likely to use such funds, financial or economic resources at their disposal for that purpose⁴⁰.

When analysing these prerequisites for inclusion on the Polish sanctions list, it is worth noting the case law of the administrative courts. The Voivodeship Administrative Court in Warsaw, in one of its judgements dismissing a complaint against a decision on inclusion in the sanctions list, referred to them thus:

It follows from the provision cited above that the legislature intended that not only those directly or indirectly supporting the aggression, but also any other person or entity, insofar as they are directly linked to the supporting entities, would be subject to listing. Such links may be, inter alia, of a personal or economic nature, but the use of the phrase “in particular” in the provision under consideration means that links of various kinds may be the basis for inclusion in the list, provided that they can be attributed to the attribute of directness.

With regard to the issue of the forms of support for the states specified in the provision, the VAC in Warsaw, in its judgement, pointed out that (...) *a direct or indirect form of support may mean generating by any means profits for the budget of the Russian Federation, which may then be used for*

⁴⁰ Article 3(2), point 1 of the Sanctions Act.

*the warfare conducted by the Russian Federation against Ukraine, as well as used to directly or indirectly support serious violations of human rights and repression of society (...)*⁴¹.

It is worth noting another fragment of the provision defining the prerequisites for inclusion in the Polish sanctions list: (...) *or in respect of which there is a probability of using such financial means, funds or economic resources at their disposal for this purpose*. It is therefore not necessary to establish the existence of an accomplished act, but the mere probability of the use of financial means, funds or economic resources for a specific purpose. This probability in turn is made credible by the existence of various types of links. This was also pointed out by the VAC in Warsaw in its judgement dismissing a complaint against the decision of the Minister of Interior and Administration: *It should be noted that the provision referred to indicates the 'existence of a likelihood' that financial resources, funds or economic resources will be used. There is therefore (...) no legal significance to the applicant's argument [indicating] that the authority has failed to "prove" the transfer of certain funds (...)*⁴². The mere probability of support turns out to be sufficient. The inclusion by the legislator of a premise of a non-executed nature is, however, necessary from the perspective of the object of the regulation and conditions its effectiveness. A transfer that has been made in this case cannot be undone, so if the premise is to cut states off from, inter alia, sources of income, it must be a pre-emptive action and independent of whether the person or entity in question has already done so previously, i.e. before they were placed on the sanctions list.

Specific nature of Polish sanctions proceedings

Pursuant to Article 3(1) of the Sanctions Act, decisions on listing and de-listing are issued by the minister responsible for internal affairs. He issues them ex officio or upon a reasoned application:

- the Head of the Central Anticorruption Bureau,
- the Head of the Internal Security Agency,
- the Head of the Foreign Intelligence Agency,
- the Head of Military Counterintelligence Service,

⁴¹ Judgement of the VAC in Warsaw of 17 V 2023, ref. no. I SA/Wa 2522/22.

⁴² Judgement of the VAC in Warsaw of 18 V 2023, ref. no. I SA/Wa 2524/22.

- the Head of Military Intelligence Service,
- the General Inspector of Financial Information,
- the Commander-in-Chief of the Police,
- the Polish Financial Supervision Authority,
- the President of the National Bank of Poland,
- the Commander-in-Chief of the Border Guard,
- the Head of the National Prosecutor's Office,
- the Head of the National Revenue Administration,
- the Chairman of the Committee of the Council of Ministers responsible for matters of security and state defence.

Thus, the power to request an inclusion in the list has been granted to special services able to obtain information on existing connections both on the basis of operational and exploratory activities, as well as analytical and information activities or, as in the case of the Central Anticorruption Bureau, within the framework of control activities, and from partner services from other countries. The analysis of the 507 decisions⁴³ on entry on the sanctions list to date clearly shows that it is these services (successively the Internal Security Agency - 458⁴⁴, the Central Anticorruption Bureau - 36 and the Military Counterintelligence Service - 8) which addressed to the minister in charge of internal affairs the largest number of applications on the basis of which sanction decisions were issued.

In addition, this power is granted to two services subordinate to the minister responsible for internal affairs, i.e. the Police - as a service obtaining information on financial or economic flows in connection with suspected criminal offences - and the Border Guard - not only as a migration service, but also carrying out tasks concerning certain forms of crime, including economic crime. However, this power has only been used by the Police in three cases. The Voivodeship Administrative Court in Warsaw, in one of the justifications of the judgement, stated that these entities are (...) *specialised state bodies that have specific knowledge in the field of public order or state security in its various aspects. The Minister of Internal Affairs and Administration therefore rules on the basis of a request from a special state body*⁴⁵.

⁴³ The figures quoted in the text represent the situation as of 1 January 2024.

⁴⁴ Concerning the same three entities, requests were made by both the Internal Security Agency and the Central Anticorruption Bureau.

⁴⁵ Judgement of the VAC of 4 VII 2023, ref. no. I SA/Wa 2528/22. Analogous statements were contained in the justifications of the judgements of the VAC in Warsaw: of 18 V 2023, ref. no. I SA/Wa 2524/22 and - of 4 VII 2023, ref. no. I SA/Wa 2528/22.

This competence has also been granted to other types of entities with knowledge of fund transfers, i.e. the General Inspector of Financial Information, the Polish Financial Supervision Authority, President of the National Bank of Poland or the Head of the National Revenue Administration and, as a result of the prosecutor's competence to conduct or supervise pre-trial proceedings in criminal matters, to the Head of National Prosecutor's Office, as well as to the Chairman of the Committee of the Council of Ministers competent in matters of security and defence of the state, due to the coordination function of this committee. However, up to the time of the formation of this article, no decisions on inclusion in the sanctions list had been issued on the basis of applications from these entities. In the cases so far, on the other hand, the Minister of the Interior and Administration has exercised his power on five occasions and made an entry on the sanctions list *ex officio*.

It is worth noting that the authorised authority's application for listing, in accordance with the Act, must include an indication of the person or entity in respect of whom a decision is to be issued and, in the case of a listing decision, also a proposal for the application of certain restrictive measures. It does not have to consist of a simple choice among the four restrictive measures described above and set out in Article 1 of the Act. Indeed, sanctions in the form of a freeze may apply to the entirety of the financial means, funds or economic resources connected to the person or entity concerned or only to specific components thereof.

Pursuant to Article 3(4) of the Sanctions Act, the proposal for the application of sanction measures shall be determined taking into account, in particular, the nature and scope of the activities carried out by the person or entity, the capital structure of that entity and national security considerations. Particularly the last of these considerations forces the applicant authority to assess the consequences of a possible inclusion in the sanctions list, although the final decision on this matter rests with the minister responsible for internal affairs. Significantly, under Article 3(7) of the Act, when issuing a decision on inclusion in the list, he or she may determine the extent of the financial means, funds or economic resources within the meaning of Regulation 269/2014 or Regulation 765/2006 covered by the measures referred to in Article 1(1) or (2) of the Act, i.e. concerning the freezing of assets. The minister responsible for internal affairs ultimately decides not only on the inclusion in the list, i.e. determines that the person or entity in question meets the prerequisites for inclusion in

the sanctions list (or removal from it), but also on the scope of the sanction measures applied. Reference was made to this issue in the justification of the judgement of the VAC in Warsaw in the sanction case, in which the court stated that: (...) *the choice of these measures is up to the public administration body, and as long as they fall within the catalogue provided for by law, there are no grounds for declaring the decision defective*⁴⁶.

Further in the article, the author presents three examples of different applications of the scope of determining sanctions regarding asset freezing - from the freezing of all financial resources and economic resources, to the freezing of only financial resources accumulated on bank accounts, to the specific exclusion of the scope of the freezing and its connection to the activities performed in order to implement the orders issued by the Prime Minister under Article 7a of the Act of 26 April 2007 on crisis management.

The first example:

- a) freezing of all financial and economic resources,
- b) the prohibition on making available to or for the benefit of the listed entity, directly or indirectly, any funds or economic resources,
- c) the prohibition to participate, knowingly and intentionally, in activities the object or effect of which is to circumvent the measures referred to in points (a) and (b),
- d) exclusion from a public procurement procedure or competition⁴⁷.

The second example:

- a) freezing of funds held in bank accounts,
- b) the prohibition to participate, knowingly and intentionally, in activities the object or effect of which is to circumvent the measures referred to in point (a),
- c) exclusion from participation in a procurement procedure or competition⁴⁸.

The third example:

⁴⁶ Judgement of the VAC in Warsaw of 18 V 2023, ref. no. I SA/Wa 2524/22.

⁴⁷ Sanctions list: SKA Assets Management Limited, <https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami> [accessed: 27 X 2023].

⁴⁸ Sanctions list: Cryogas M&T Poland Spółka Akcyjna, <https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami> [accessed: 27 X 2023].

- a) the freezing of all funds and economic resources,
- b) a prohibition on making available, directly or indirectly, any funds or economic resources to, or for the benefit of, the listed entity,
- c) the prohibition to participate, knowingly and intentionally, in activities the object or effect of which is to circumvent the measures referred to in points (a) and (b),
- d) exclusion from public procurement or competition.

With regard to the measures referred to in points (a) and (b), the scope relating to activities carried out in order to implement orders issued by the Prime Minister pursuant to Article 7a of the Act on crisis management shall be excluded⁴⁹.

However, the special nature of sanction proceedings is not limited to the fact that, as a rule, they are initiated in practice by the requesting authority, which is not a party to the proceedings. It differs from typical administrative proceedings fully based on the Act of 14 June 1960 – The Code of Administrative Procedure (CAP). Indeed, pursuant to Article 4(1) of the Sanctions Act, only some of the provisions of the CAP, e.g. Article 107 § 1, apply to proceedings in matters of listing and de-listing to the extent not regulated by the Act. For example, pursuant to Article 107 § 1 point 6 of the CAP, the decision shall contain, in particular, the factual and legal grounds, which must be read in conjunction with Article 3(6) of the Sanctions Act. According to it, a decision on inclusion in the list shall contain the date of issue, the designation of the person or entity to which the sanctioning measures apply, together with a decision as to which of these measures apply to them, a statement of reasons, the designation of the issuing authority, the legal basis of the decision, the signature of the issuing person and an instruction on the right to file a complaint with the administrative court. It should be emphasised, however, that the provision of Article 4, section 1 of the Sanctions Act does not refer to Article 107 § 3 of the CAP, in accordance with which the factual justification of a decision should include, in particular, specification of facts recognised by the authority as proven, evidence on which it relied and reasons for which other evidence was denied credibility and evidentiary value, while the legal justification should include an explanation of the legal basis of the decision, with citation of legal provisions. At the same time, in

⁴⁹ Sanctions list: Novatek Green Energy Sp. z o.o., <https://www.gov.pl/web/mswia/lista-osobi-podmiotow-objetych-sankcjami> [accessed: 27 X 2023].

accordance with Article 3(9) of the Act, the minister in charge of internal affairs may limit the scope of justification for the sake of state security or public order. Such a situation occurs especially in cases in which classified materials are used.

The specific nature of this procedure, as described above, was referred to by the VAC in Warsaw in the justification of its judgement dismissing an action to remove an entity from the sanctions list:

(...) the listing procedure is not a typical administrative proceeding, as, according to Article 4 of the Act of 13 April 2022, only certain, specifically listed, provisions of the Code of Administrative Procedure apply to such proceedings to the extent not regulated by the Act. (...) As a result, in proceedings under the provisions of the Act of 13 April 2022, the authority is not obliged to assess whether a circumstance has been proven, based on the totality of the evidence, and the reasons for the decision do not have to include an indication of the facts that the authority has found to be proven, the evidence on which it has relied and the reasons why it has denied the credibility and evidential value of other evidence. The above statement also corresponds with the wording of Article 3(9) of the Act of 13 April 2022, which provides that the Minister may limit the scope of the reasons for a decision on listing for reasons of state security or public order⁵⁰.

In the further part of the cited justification for the judgement, the court emphasised that (...) *the difficulties in collecting full evidence on entities located in Belarus or Russia will often result in the fact that, when issuing a decision on inclusion in the list, the authority will have at its disposal only limited evidence on the basis of which it will assess the fulfilment of the conditions listed in Article 3(2) of the Act of 13 April 2022*⁵¹.

The special nature of these proceedings is also evidenced by the manner of notifying the parties of the authority's decision and binding the party to it, as set out in Article 4(2) and (3) of the Sanctions Act. Notification of the decisions to the parties is made by making them

⁵⁰ Judgement of the VAC in Warsaw of 2 II 2023, ref. no. I SA/Wa 2527/22. An analogous view was also expressed by the VAC in Warsaw in other cases – judgement of 18 V 2023, ref. no. I SA/Wa 2524/22; judgement of 4 VII 2023, ref. no. I SA/Wa 2528/22; judgement of 17 V 2023, ref. no. I SA/Wa 2522/22; judgement of 18 VI 2023, ref. no. I SA/Wa 2541/22.

⁵¹ Judgement of the VAC in Warsaw 2 II 2023, ref. no. I SA/Wa 2527/22.

available in the Bulletin of Public Information (BIP) on the website of the minister responsible for internal affairs. The binding of the authority with the decision issued by it, the commencement of the time limit for lodging a complaint against the decision and the occurrence of immediate enforceability of the decision shall take place on the day following the day on which the decision was made available in the BIP.

The construction of the aforementioned provision with regard to delivery is based on Article 49 § 1 of the CAP, according to which, if a specific provision so provides, notification of the parties of decisions and other actions of a public administration body may be made in the form of a public notice, in another form of public announcement customarily accepted in a given locality or by making the letter available in the BIP on the website of the competent public administration body. However, in contrast to the solution in the CAP, the norm according to which the day on which the letter was made available in the BIP is not included, and the notification is deemed to have been made after the lapse of 14 days from the day of making it available.

Article 61 § 4 of the CAP, according to which the initiation of proceedings *ex officio* or at the request of one of the parties must be notified to all persons who are parties to the case, also does not apply in sanction proceedings. In these proceedings, a party only becomes aware of its initiation in relation to him/her at the moment of issuing the decision on entry on the sanctions list and this by posting the decision in the BIP. On the one hand, the reason for adopting such a solution is the risk that earlier acquisition of information about the initiation of the proceedings, i.e. before the decision is issued, could result in the concealment or diversion of the financial means, funds or economic resources to be frozen. On the other hand, the nature of the listed entities, often based, for example, in Russia, Belarus or Cyprus, could prevent service of the decision or the acknowledgement of service, which a party dissatisfied with the effect of the decision could deny. It should also be borne in mind that the decision, although of an individual nature, also has an impact on other persons and entities, e.g. banks obliged to freeze funds in the account of a listed person, and therefore its publication is made in the BIP, analogous to the publication of the sanctions list itself⁵².

⁵² In accordance with Article 2(1) of the Sanctions Act, the list of persons and entities against whom the measures referred to in Article 1 of the Act are applied is published in the BIP on the website of the minister responsible for internal affairs.

However, the simplified procedure at the level of the decision-making authority, as well as the single-instance nature of this procedure, does not exclude the possibility of a defence on the part of the listed person or entity. Pursuant to Article 3(10) of the Sanctions Act, sanction decisions cannot be appealed by filing a request for reconsideration. Instead, they are subject to appeal to the Voivodship Administrative Court⁵³. The complaint shall be lodged through the Minister of the Interior and Administration, within 30 days of the decision being made available in the BIP on the subject page of the minister responsible for internal affairs. The Voivodship Administrative Court in Warsaw, in the justification of one of its judgements, emphasised, on the one hand, the special nature of these proceedings, and on the other hand, indicated that:

However, this does not mean that such a person or entity is completely deprived of legal protection. Indeed, a complaint may be lodged against an issued decision with the administrative court (Article 3(6) of the Act), and in the course of the proceedings before the court, the complainant may present his/her own arguments, allegations and conclusions. (...) In view also of the geopolitical situation caused mainly by the aggression of the Russian Federation against Ukraine, certain restrictions must be imposed on the freedom to conduct economic activity in a situation where there is a likelihood that the funds obtained from it could serve its support and threaten the social interest, security of the state⁵⁴.

Temporary compulsory administration

The adoption in the Sanctions Act of a solution for the application of individual measures arising from the EU regulations allowed, as mentioned earlier, for the NRA to carry out the release of certain measures, e.g. to enable legal protection of the company covered by them. However, the original solution was considered insufficient in the broader

⁵³ In accordance with Article 16 § 2 of the Code of Administrative Procedure and Article 3 § 2 item 1, Article 53 § 1 and Article 54 § 1 of the Act of 30 August 2002 - Law on proceedings before administrative courts.

⁵⁴ Judgement of 4 VII 2023, ref. no. I SA/Wa 2528/22; judgement of 18 V 2023, ref. no. I SA/Wa 2524/22.

perspective, primarily due to the fact that some of the frozen companies operating in Poland had employees and were simultaneously responsible for the production of goods or technology. Therefore, on 18 August 2022, an amendment to the Sanctions Act introducing new safeguard instruments came into force⁵⁵. It was considered expedient to introduce a solution allowing the continuation of the entities against which freezes were applied under the provisions of the Sanctions Act. Consideration was given, on the one hand, to the need to extend individual restrictive measures to entities that may be used to dispose of financial resources, funds or economic resources to support the aggression of the Russian Federation against Ukraine, and, on the other hand, to the social and public interest, including the interest of the side of the employees of enterprises run by sanctioned economic entities⁵⁶.

The adopted amendment supplemented the previous regulations contained in the Sanctions Act with the institution of temporary compulsory administration and the provision of support to employees providing work for sanctioned entities. Although a detailed discussion of the instruments introduced is beyond the scope of this article, it is worth noting that the minister responsible for economic affairs may, by way of a decision, establish a compulsory administration with respect to a listed entity. The purpose of the instituted temporary administration is to dispose of financial means, funds or economic resources when it turns out to be necessary to ensure the continued operation of economic entity conducting business on the territory of the Republic of Poland and this serves:

- maintaining workplaces in this enterprise, or
- maintaining within the scope of activity of this enterprise the provision of public utility services or the performance of other tasks of public character, or
- protection of the national economic interest⁵⁷.

The tasks performed by the administrator are aimed at the continued smooth operation of the business entity's enterprise until the financial resources, funds or economic resources under administration are disposed

⁵⁵ Act of 5 August 2022 amending the Act on Specific Solutions to Counteracting Support for Aggression against Ukraine and to Protect National Security and the Act on the National Revenue Administration.

⁵⁶ Explanatory memorandum to *the Government Draft Act on specific solutions...*, p. 1–2.

⁵⁷ Article 6a(1) of the Sanctions Act.

of - i.e. taken over by capital not linked to persons and entities supporting Russian aggression. The funds from the sale are frozen in the accounts of the existing sanctioned owners.

An alternative solution adopted in the act is the use of a compulsory administration to take over ownership of financial resources, funds or economic resources belonging to a listed person or entity for the benefit of the State Treasury, if this is necessary to protect an important public interest, to protect the national economic interest or to ensure the national security.

Summary

To summarise the considerations, it is worth quoting once again the justification for one of the judgements of the Voivodeship Administrative Court in Warsaw dismissing complaints against decisions concerning entry on the sanctions list:

(...) the aggression of the Russian Federation against Ukraine, which began on 24 February 2022, caused numerous changes in the world, including in Poland, related to national security, but also resulted in legal steps being taken to counteract support for this aggression. The Act of 13 April 2022 is an expression of this. (...) Indeed, since the end of World War II, there has not been an outright aggression of one state against another on the European arena. Therefore, the action of the legislator in terms of restriction, simplification of administrative proceedings in the cases of entry on the list of persons and entities supporting the aggression of the Russian Federation against Ukraine launched on 24 February 2022 is not unjustified⁵⁸.

It may be argued that the specific nature of the sanctions law, justified by the circumstances and the purpose of its creation, remains undisputed, while taking into account, however, the fundamental guarantee elements for the person or entity included in the list. On the one hand, the initiator of the proceedings is usually not himself a party to the proceedings and the subject of the proceedings is not informed of the initiation

⁵⁸ Judgement of the VAC in Warsaw of 4 VII 2023, ref. no. I SA/Wa 2528/22; judgement of 18 V 2023, ref. no. I SA/Wa 2524/22.

of the proceedings, but only of the possible negative effect on him. In addition, decisions in sanction cases have limited justification and, as a result, do not require the presentation of the entirety of the evidence on which they are based, they are served through a publicly accessible BIP and the proceedings are single-instance. On the other hand, an entity or person included in the list has the right to lodge a complaint with the administrative courts, and making an entry cannot be treated as a sanction, i.e. a punishment *sensu stricto*, as it is in fact a temporary restrictive measure aimed at preventing direct or indirect support for the actions of the Russian and Belarusian authorities. In this context, the solutions adopted by the legislator meet the constitutional requirements and are in line with the EU recommendations indicated earlier, according to which Member States should have an additional legal framework, in relation to the EU, for freezing the funds and financial assets and economic resources of persons and entities subject to restrictive measures at the national level.

The application of these solutions to date proves their effectiveness as autonomous from EU freezing instruments, although, as indicated earlier, these solutions are partly based on European legislation. Undoubtedly, Poland's immediate neighbourhood with Russia and the Ukraine attacked by it, as well as with Belarus, requires additional measures that would go beyond EU-wide solutions and be based on a consensus at EU level. This is justified both from the perspective of the Polish *raison d'état*, conditioned by Poland's location and historical considerations, and from the perspective of national security. The scale of not only the Poland's involvement in helping Ukraine, but also the threat to Poland and its people, by virtue of its proximity to these states, is obviously different from countries far from the conflict zone, e.g. the Iberian Peninsula.

It is worth noting the effects of individual national restrictive measures referred to in the Sanctions Act. As of 1 January 2024, there were 498 persons and entities (425 persons and 73 entities) on the sanctions list maintained by the Ministry of the Interior and Administration. A total of 64 complaints against the decisions of the Minister of the Interior and Administration were submitted to the VAC in Warsaw, including 56 complaints against decisions on entry on the sanctions list, seven complaints against decisions on refusal to remove from the list and one against a decision amending a decision on entry on the list. In addition, the Minister of the Interior and Administration took nine decisions to remove persons or entities from the sanctions list. Two of them were issued due to the subsequent inclusion

of the covered one person and one entity in Annex I to Regulation 269/2014 (the deletion was due to the need to avoid duplication of national and EU sanctions). For seven entities, on the other hand, the decision to remove from the list was taken due to new factual circumstances, i.e. a change in ownership structure and thus the removal of the link with the person or entity constituting the reason for listing. This case illustrates well the real role of individual restrictive measures as temporary measures aimed at reducing or removing the link with the state structures of Russia or Belarus, rather than permanently eliminating the entity in question from trading.

As of 1 January 2024, the Voivodship Administrative Court in Warsaw has dealt with 21 complaints concerning the issuance by the Minister of the Interior and Administration of a decision on entry into the sanctions list, a decision refusing to remove from the sanctions list, a decision changing the scope of individual restrictive measures applied or a decision on removal from the list. All of them were dismissed, which confirms the correctness of the entire decision-making process related to the inclusion of certain persons and entities in the restrictive measures. In addition, three complaints to the VAC were withdrawn by the complainant and, in a further four cases, the court rejected the complaints on formal grounds (they were filed out of time). The contested decisions on the listing of two entities became final. On the other hand, four entities (including one in two cases) and three individuals filed cassation appeals with the Supreme Administrative Court.

On the basis of national and EU individual restrictive measures, the NRA froze assets with a total value of approximately EUR 1.21 billion on the territory of Poland⁵⁹ (the way statistics are kept in this regard does not allow separate values for EU and national restrictive measures). In addition, the minister responsible for the economy applied receivership to seven entities.

The cited data show the wide application of the solutions adopted in the Sanctions Act and indicate their effectiveness. Thus, the EU Council's guideline on the need to adopt national solutions for individual restrictive measures is met, according to which:

These measures should enable national authorities to order and implement without delay the freezing of all funds and economic resources within the jurisdiction of the Member State concerned

⁵⁹ The situation on 30 September 2023.

belonging to, owned, controlled or held by the designated person or entity, and could also be directed at persons or entities within the European Union and conducting their main business there⁶⁰.

Another issue is to assess whether the solutions adopted by the Polish legislator are the target solutions. Considering the very title of the Sanctions Act, a negative answer to this question seems quite obvious. This is because the Act defines specific solutions only in terms of countering support for aggression against Ukraine and in the context of human rights violations in Russia and Belarus, and does not provide for its applicability in other circumstances. The mechanisms established therein, both those introducing an autonomous national system of individual restrictive measures and those designed to ensure the application of EU sanctions (such as the designation of a competent authority to prevent the circumvention of these sanctions or the introduction of provisions criminalising the violation of EU sanctions), are limited only to the actions of the Russian Federation and Belarus or explicitly designated EU regulations. Meanwhile, the UN and the EU impose restrictive measures on a number of other states because of their failure to comply with international law or human rights or their pursuit of policies or actions contrary to the rule of law or democratic principles. In this case, Poland is already deprived of legal instruments of influence analogous to those introduced by the Sanctions Act. As a result, it is not only possible to introduce its own restrictive measures, but above all to ensure the effective application of EU measures due to the failure to designate a competent authority in these matters and the lack of a criminal sanction for circumventing these measures. The exceptions are the issues related to the prevention of terrorism and the norms arising from the aforementioned Act on counteracting money laundering and terrorist financing.

The issue raised deserves a separate study, based in particular on an analysis of solutions in force in other countries. As an example, it is worth recalling the solutions adopted in the Czech Republic by Act no. 1/2023 on restrictive measures against certain serious acts in international relations⁶¹, which entered into force on 3 January 2023. For an entity to be on the Czech

⁶⁰ *Aktualizacja dobrych praktyk UE...*, point 26.

⁶¹ *Zákon o omezujících opatřeních proti některým závažným jednáním uplatňovaných v mezinárodních vztazích (sankční zákon)*, https://www.mzv.cz/jnp/cz/o_ministerstvu/legislativa/pravni_predpisy_v_pusobnosti_mzv/zakon_c_1_2023_sb_o_omezujicich.html [accessed: 27 XI 2023].

national sanctions list, a condition under one of the EU sanctions regimes must be met. Another condition is that the application of restrictive measures against a specific natural or legal person is in the foreign policy or security interests of the Czech Republic. This therefore does not apply to restrictive measures introduced by the EU only with regard to Russia and Belarus, but also with regard to all other countries for which the EU would take such decisions. In this solution, the national list is complementary to the EU sanction mechanisms and is used when the discussion at EU level takes a long time or when there is a risk that its objective will not be achieved. As in the case of the Polish Sanctions Act, the inclusion of a person on the EU sanctions list in principle results in the removal of that person from the national list (where the reasons for including persons on both lists are the same). Exceptionally, if the Czech Republic applies sanctions to such a person to a greater extent than the EU, that person will remain on the national list precisely because of restrictive measures that go beyond specific EU sanctions.

On the ground of Polish law, it would be worth considering to use in a broader context the successful solutions adopted by the Sanctions Act and the experience resulting from its application. This would serve the purpose of undertaking work on a law introducing permanent solutions allowing for the application of individual restrictive measures depending on the changing international situation. They would be applied to persons and entities supporting other (not included in the Sanctions Act) state regimes against which the international community, including the EU, imposes sanctions.

Bibliography

Kędzierski M.A., *Szczególne środki ograniczające i sankcje jako forma przeciwdziałania wobec podmiotów terrorystycznych na tle polskiego ustawodawstwa (część 1)* (Eng. Specific restrictive measures and sanctions as a form of counteraction against terrorist entities against the background of Polish legislation (part 1)), "Prokuratura i Prawo" 2021, no. 10, pp. 20–45.

Kędzierski M.A., *Szczególne środki ograniczające i sankcje jako forma przeciwdziałania wobec podmiotów terrorystycznych na tle polskiego ustawodawstwa (część 2)* (Eng. Specific restrictive measures and sanctions as a form of counteraction against terrorist entities against the background of Polish legislation (Part 2)), "Prokuratura i Prawo" 2021, no. 11, pp. 36–55.

Kobza P., *Środki restrykcyjne jako instrument Wspólnej Polityki Zagranicznej i Bezpieczeństwa Unii Europejskiej* (Eng. Restrictive measures as an instrument of the European Union's Common Foreign and Security Policy), "Studia Europejskie" 2006, no. 3, pp. 9–31.

Lewna A., *Kiedy wojenny zapał może zaszkodzić. Kilka uwag o przestępstwie z art. 16 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego* (Eng. When war fervour can cause harm. Some comments on the offence of Article 16 of Act of 13 April 2022 on Specific Solutions to Counteracting Support for Aggression against Ukraine and to Protect National Security), "Prokuratura i Prawo" 2023, no.6, pp. 86–101.

Pospieszna P., *Sankcje Unii Europejskiej wobec Rosji: proces decyzyjny, trwałość i rola państw członkowskich* (Eng. European Union sanctions against Russia: decision-making process, sustainability and the role of Member States), "Rocznik Integracji Europejskiej" 2018, no. 12, pp. 311–321. <https://doi.org/10.14746/rie.2018.12.21>.

Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz (Eng. Counteracting money laundering and terrorist financing. Commentary), J. Grynfelder et al. (eds.), Warszawa 2020.

Sulek M., *Zachodnie sankcje wobec Rosji – sens i skuteczność* (Eng. Western sanctions against Russia - sense and effectiveness), "Rocznik Strategiczny" 2014/2015, vol. 20, pp. 398–410.

Internet sources

Sejm uznał Rosję za państwo wspierające terroryzm (Eng. The parliament recognised Russia as a state supporting terrorism), 14 XII 2022, <https://www.sejm.gov.pl/sejm9.nsf/komunikat.xsp?documentId=4774505381CECC10C1258918007022FA> [accessed: 25 X 2023].

Legal acts

European Convention on the Suppression of Terrorism, prepared at Strasbourg on 27 January 1977 (Journal of Laws of 1996, no. 117, item 557).

Geneva Conventions for the protection of war victims of 12 August 1949 (Journal of Laws of 1956, item 171).

Treaty on the Functioning of the European Union (consolidated version) – (Official Journal of the EU C 202/47 of 7 VI 2016).

Treaty on European Union (consolidated version) – (Official Journal of the EU C 202/13 of 7 VI 2016).

Rome Statute of the International Criminal Court prepared in Rome on 17 July 1998 (Journal of Laws of 2003, no. 78, item 708).

Council Regulation (EU) No 269/2014 of 17 March 2014 concerning 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 III 2014, as amended).

Council Regulation (EC) No 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine (Official Journal of the EU L 134/1 of 20 V 2006, as amended).

Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism (Official Journal of the UE L 344/70 of 28 XII 2001).

Commission Opinion of 19 June 2020 on Article 2 of Council Regulation (EU) No 269/2014, Brussels, 19 VI 2020, C (2020) 4117 final.

Act of 5 August 2022 amending the Act on Specific Solutions to Counteracting Support for Aggression against Ukraine and to Protect National Security and the Act on the National Revenue Administration (Journal of Laws of 2022, item 1713).

Act of 13 April 2022 on Specific Solutions to Counteracting Support for Aggression against Ukraine and to Protect National Security (Consolidated text of Journal of Laws of 2023, item 1497 and 1859).

Act of 11 September 2019 - Public Procurement Law (Consolidated text of Journal of Laws of 2023, item 1605, as amended).

Act of 1 March 2018 on counteracting money laundering and terrorist financing (Consolidated text of Journal of Laws of 2023, item 1124, as amended).

Act of 16 November 2016 on the National Revenue Administration Act (Consolidated text of Journal of Laws of 2023, item 615, as amended).

Act of 12 December 2013 on foreigners (Consolidated text of Journal of Laws of 2023, item 519, as amended).

Act of 26 April 2007 on crisis management (Consolidated text of Journal of Laws of 2023, item 122).

Act of 30 August 2002 - Law of the Administrative Courts Procedure (Consolidated text of Journal of Laws of 2023, item 1634, as amended).

Act of 29 September 1994 on accounting (Consolidated text of Journal of Laws of 2023, item 120, as amended).

Act of 14 June 1960 Code of Administrative Procedure (Consolidated text of Journal of Laws of 2023, item 775).

Resolution of the Sejm of the Republic of Poland of 14 December 2022 on the recognition of the Russian Federation as a state supporting terrorism (M.P. of 2022, item 1253).

Resolution of the Senate of the Republic of Poland of 26 October 2022 on the recognition of the authorities of the Russian Federation as a terrorist regime (M.P. of 2022, item 1043).

Zákon o omezujících opatřeních proti některým závažným jednáním uplatňovaných v mezinárodních vztazích (sankční zákon), https://www.mzv.cz/jnp/cz/o_ministerstvu/legislativa/pravni_predpisy_v_pusobnosti_mzv/zakon_c_1_2023_sb_o_omezujících.html [accessed: 27 XI 2023].

Case law

Decision of the Supreme Administrative Court of 9 V 2023, ref. no. III OZ 207/23.

Judgement of the Voivodeship Administrative Court in Warsaw of 4 VII 2023, ref. no. I SA/Wa 2528/22.

Judgement of the Voivodeship Administrative Court in Warsaw of 18 VI 2023, ref. no. I SA/Wa 2541/22.

Judgement of the Voivodeship Administrative Court in Warsaw of 18 V 2023, ref. no. I SA/Wa 2524/22.

Judgement of the Voivodeship Administrative Court in Warsaw of 17 V 2023, ref. no. I SA/Wa 2522/22.

Judgement of the Voivodeship Administrative Court in Warsaw of 2 II 2023, ref. no. I SA/Wa 2527/22.

Other documents

Aktualizacja dobrych praktyk UE w zakresie skutecznego wprowadzania w życie środków ograniczających (Eng. Update on EU good practice in the effective implementation of restrictive measures), Brussels, 4 V 2018, document no. 8519/18, <http://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/pl/pdf> [accessed: 30 X 2023].

Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (Official Journal of the EU L 344/93 of 28 XII 2001), <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:02001E0931-20171115> [accessed: 30 X 2023].

Decyzja Ministra Spraw Wewnętrznych i Administracji z dnia 29 sierpnia 2023 r. (Eng. Decision of the Minister of the Interior and Administration of 29 August 2023) DPP-TPZ.0272.2.2023.AK(38), Decyzja odmowna (Eng. Decision of refusal) – Timur Raszidow, <https://www.gov.pl/web/mswia/decyzje-ministra-swia-w-sprawie-wpisu-na-liste-sankcyjna> [accessed: 22 X 2023].

Lista osób i podmiotów objętych sankcjami (Eng. List of sanctioned persons and entities), Ministry of the Interior and Administration, <https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami> [accessed: 27 X 2023].

Ogólne ramy dla sankcji unijnych (Eng. General framework for EU sanctions), <https://eur-lex.europa.eu/PL/legal-content/summary/general-framework-for-eu-sanctions.html> [accessed: 26 X 2023].

European Parliament resolution of 23 November 2022 on recognising the Russian Federation as a state sponsor of terrorism (2022/2896(RSP)) – (Official Journal of the EU C 167/18 of 11 V 2023), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0405_PL.html [accessed: 27 IX 2023].

European Parliament resolution of 6 October 2022 on Russia's escalation of its war of aggression against Ukraine (2022/2851(RSP)) – (Official Journal of the EU C 132/94 of 14 IV 2023), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0353_PL.html [accessed: 27 IX 2023].

European Parliament resolution of 19 May 2022 on the fight against impunity for war crimes in Ukraine (2022/2655(RSP)) – (Official Journal of the EU C 479/68 of 16 XII 2022), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0218_PL.html [accessed: 27 IX 2023].

European Parliament resolution of 25 November 2021 on the human rights violations by private military and security companies, particularly the Wagner Group (2021/2982(RSP)) – (Official Journal of the EU C 224/104 of 8 VI 2022), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=uriserv%3A0J.C_.2022.224.01.0104.01.POL&toc=OJ%3AC%3A2022%3A224%3ATOC [accessed: 27 IX 2023].

Uzasadnienie do *Rządowego projektu ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego* (Eng. Explanatory Memorandum to the Government Draft Act on specific solutions in counteracting the promotion of aggression against Ukraine and serving to protect national security), Print no. 2131, <https://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=2131> [accessed: 23 X 2023].

Mariusz Cichomski

Lawyer, sociologist. He works on issues related to terrorism, organised crime, oversight of service activities, security legislation and issues related to the application of restrictive measures. He is the author of more than thirty publications on security, particularly in the legal dimension, and on sociology.

Large Language Models in jihadist terrorism and crimes

JULIA PUCZYŃSKA

IDEAS NCBR

Doctoral School of Information
and Biomedical Technologies Polish Academy of Sciences

 <https://orcid.org/0009-0009-5304-7092>

MARCIN PODHAJSKI

IDEAS NCBR

Doctoral School of Information
and Biomedical Technologies Polish Academy of Sciences

 <https://orcid.org/0009-0001-1350-879X>

KAROLINA WOJTASIK

Polish Association for National Security

 <https://orcid.org/0000-0002-1215-5005>

TOMASZ P. MICHALAK

IDEAS NCBR

Faculty of Mathematics, Informatics and Mechanics
at the University of Warsaw

 <https://orcid.org/0000-0002-5288-0324>

Abstract

The authors discuss Large Language Models in the context of the security risks associated with their functions and availability. Even though their applications seem to be similar to search engines and internet access, the true danger posed by Large Language Models lies in basic analytical and programming skills they provide to any criminal or terrorist. They assert that accessible Large Language Models not only diminish financial barriers to various criminal activities but also lower the expertise and commitment required by individuals or small groups to commit crimes, and acts of terror in particular. On the other hand, however, law enforcement agencies can also harness the capabilities of these models to stay ahead of emerging threats.

Keywords

Large Language Models, security, cybercrime, jihadist terrorism, artificial intelligence

Introduction

The rapid advancement of artificial intelligence (AI) has introduced innovations that impact various aspects of our lives. Large Language Models (LLMs) such as ChatGPT which became a world-wide phenomenon in 2023 stand out among these novelties manifesting a remarkable technological progress. In this article, the authors embark on an exploration of LLMs in the context of security, unraveling their construction, functionality, and main capabilities.

From the security point of view, a key concern arising from the proliferation of LLMs is their potential exploitation by criminals, terrorists, and state actors engaged in hybrid warfare. The authors' goal is to examine such possible negative scenarios, highlighting the challenges associated with LLMs. We assert that accessible large language models, especially ChatGPT, not only diminish financial barriers to various criminal activities but also lower the expertise and commitment required by individuals or small groups to commit crimes or acts of terror.

While some works have attempted to look into these issues¹, this article offers a more comprehensive analysis for non-experts. We pay particular attention to less-explored areas, such as e.g. the potential involvement of LLMs in social engineering schemes, disinformation, terrorist propaganda and recruitment. Additionally, by understanding how criminals utilize LLMs, the authors explore how law enforcement agencies can harness the capabilities of these models to stay ahead of emerging threats.

The authors focused on jihadist terrorism due to the unprecedented activity of these organizations (e.g., Al-Qaeda or ISIS) on social media, their publishing activity (dozens of magazines, several periodic publications in multiple languages), and their editorial activity—ebooks with propagandistic, instructional, and motivational content. This allowed for a thorough analysis that would not have been possible in the case of other terrorist groups.

The remainder of this article is organized as follows: section titled *Introduction to LLMs* provides an introduction to LLMs for non-experts.

¹ Europol, *ChatGPT. The impact of Large Language Models on Law Enforcement*, Luxembourg 2023; E. Derner, K. Batistič, *Beyond the Safeguards: Exploring the Security Risks of ChatGPT*, preprint, arXiv, 13 V 2023, <https://arxiv.org/abs/2305.08005> [accessed: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2305.08005>.

Basic terms pertaining to these models are explained before discussing the security of LLMs. Section *LLMs in crimes and terrorism* is divided into two parts. The part named *Threats* concerns the potential uses of large language models in criminal and terrorist activities, while *Chances* takes on the possibilities to respond to the arising threats. The section concludes by pointing out the differences between what is available from LLMs and what was available before their dissemination.

In the section *What does the accessibility of LLMs change?* capabilities of large language models are compared to those of search engines. The last part of the article contains conclusions from the carried out analysis.

Introduction to LLMs

LLM is a sort of an AI model that learns from a large quantity of text data in order to produce language outputs that are coherent and sound natural. Due to their capacity to produce writing that frequently blends in with human-written text, these models have gained popularity in recent years. Additionally, multimodal LLMs are also being developed, which are models that are based on LLMs, but can additionally process other types of data such as images, video or sound².

In this section, we will provide a technical introduction to LLMs for non-experts in the field, and explain some of the mechanisms that allow LLMs to understand natural language relatively well.

How LLMs work

One of the most popular techniques today for creating artificial intelligence systems is machine learning. Machine learning models use the data provided to them to identify patterns, which can then be used to predict outcomes or perform tasks. These models usually return a result based on input data, e.g., text, images or sounds. The output may be, for example, a label that the model assigns to the input data (classification), or a generated text or image (so-called generative AI).

The models can be constructed in a variety of ways in terms of internal mechanisms and data processing structures, which can be overlapping or

² S. Yin et al., *A Survey on Multimodal Large Language Models*, preprint, arXiv, 23 VI 2023, <https://arxiv.org/abs/2306.13549> [accessed: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2306.13549>.

sequential. A recently popular type of models are the so-called artificial neural networks. The chosen size and structure of the network along with the mechanisms operating inside it are called the network architecture. A LLM is typically built using an architecture known as a transformer³, which is specifically designed to handle sequential input data such as text.

A crucial step in machine learning is training the model. LLMs are trained using typically very large text data sets that are gathered from a variety of sources, including books, papers, websites, and social media platforms. This versatility of datasources aims at identifying as many as possible relationships and patterns between words, phrases, and sentences.

After the pre-training phase, the models can be adjusted (fine-tuned) which involves additional training on a new task-specific dataset. This includes a variety of tasks, such as but not limited to question answering, sentiment analysis, or machine translation.

Limitations of LLMs

The general public, at least its significant portion, seems to be captivated by the possibility that LLMs reached the level of human-level intelligence. This is however not the case, at least to a large extent. The exact level and nature of LLMs' intelligence is heavily debated among scientists and non-experts alike.⁴ On one hand it seems fair to say that more often than previously believed to be possible LLMs provide answers that are significantly more sophisticated than just the most probable sequence of words given the context. On the other hand, as nicely put by Borji: *While they possess some degree of understanding, it remains considerably less than human cognition. Our understanding of their comprehension is still limited, and they may have distinct ways of understanding that we are yet to grasp*⁵.

Hallucinations⁶ are a notable limitation of LLMs which are susceptible to generating content that lacks factual basis or coherence. They can be attributed to their primary training objective: to sound natural and coherent

³ A. Vaswani et al., *Attention is All you Need*, in: *Advances in Neural Information Processing Systems 30 (NIPS 2017)*, I. Guyon et al. (eds.), Long Beach 2017, pp. 5998–6008.

⁴ A. Borji, *Stochastic Parrots or Intelligent Systems? A Perspective on True Depth of Understanding in LLMs*, preprint, SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4507038. [accessed: 8 IX 2023]. <http://dx.doi.org/10.2139/ssrn.4507038>.

⁵ Ibid.

⁶ Z Ji. et al., *Survey of hallucination in natural language generation*, “ACM Computing Surveys” 2013, vol. 55, no. 12, pp. 1–38. <https://doi.org/10.1145/3571730>.

based on the patterns and language present in their training datasets, rather than to fact-check the information they generate. While LLMs excel at mimicking human-like language and generating contextually relevant text, their responses are not necessarily vetted for factual accuracy. This predisposition to prioritize language fluency over fact-checking can lead to the production of plausible-sounding but erroneous or unfounded content, underscoring the importance of external fact checking when relying on LLMs for information. Other problems include: lack of transparency on how LLM arrives at a particular output or the limited length of the processed text.

What LLMs are good at

LLMs are distinguished by various tasks and applications related to natural language processing. The tasks they are particularly good at include:

- **Step-by-step instructions** – LLMs can provide step-by-step instructions for various sequential tasks, such as cooking or programming.
- **Code Generation** – LLMs are often trained on a dataset with programming code and are used in writing or improving code, e.g. Github Copilot.
- **Sentiment Analysis** – LLM can determine the author's attitude or feelings conveyed in the text.
- **Text completion and generation** – They can complete missing text fragments and are used to generate articles, stories, poems and other written content.
- **Translation** – Many modern online translators are based on LLMs, chatbots are also capable of conversing in many languages.
- **Text Analysis** – LLMs can find specific information from documents, making data retrieval more efficient. They can also write summaries of articles, and there are tools available that allow them to "talk" to the document, i.e. answer questions via LLM based on a text.

LLMs security

Many commercial LLMs such as ChatPGT include safeguards which recognize inputs for content that may be hateful, sexually explicit, violent, or encourage self-harm, and safeguards that limit the models' ability to respond to such prompts. LLM security and attempts to break safeguards are currently one of the areas under research.

Prompt engineering

One of the ways to bypass the LLMs safeguards is prompt engineering⁷ which is a technique where users deliberately refine or design the specific way they phrase a question or request to influence the generated output. These prompts can be opinion transfers (asking an objective response and then changing the perspective it was written in), asking the model to give the answer as a piece of code, having them speak as a fictional character discussing the topic, replacing trigger words and changing the context later, and making up hypothetical examples that can be applied to actual events.

Adversarial attacks

Adversarial examples in LLMs are carefully constructed sequences of characters that, when appended to a user's query, can manipulate the AI system to produce harmful content or follow unintended user commands. Unlike traditional jailbreaks, these adversarial attacks are generated automatically, enabling the creation of a limitless number of such manipulative inputs. These attacks are a cause for concern, as they can potentially transfer to various LLMs, including both open-source and closed-source models like ChatGPT⁸.

Using uncensored LLMs

Users have the option to utilize uncensored large language models (LLMs) that lack content safeguards, thereby granting unrestricted access for content generation across a broad spectrum of topics. For example Worm GPT can easily be used for business email compromise (BEC) attacks⁹. It was trained on malware-focused data and is said to be similar to ChatGPT in terms of abilities, but without the limitations. The CEO of Gab (a white supremacist forum) has announced plans to create their own model

⁷ S.R. Bowman, *Eight Things to Know about Large Language Models*, preprint, arXiv, 2 IX 2023, <https://arxiv.org/abs/2304.00612> [accessed: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2304.00612>.

⁸ A. Zou et al., *Universal and Transferable Adversarial Attacks on Aligned Language Models*, preprint, arXiv, 27 VII 2023, <https://arxiv.org/abs/2307.15043> [accessed: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2307.15043>.

⁹ D. Kelley, *WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks*, SlashNext, 13 VII 2023, <https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/> [accessed: 22 XI 2023].

without hate speech filters. This accessibility can be dangerous, but it can also empower users to freely explore diverse content, including subjects that might be censored in commercial models like ChatGPT.

Content generated by such models often is not subject to any legislation, because it is not directly created by a human. Because of that there are voices to introduce such laws that would allow to hold accountable the creators of chatbots and models that generate harmful content¹⁰.

LLMs in crimes and terrorism

The potential applications of LLMs in criminal activities are vast and encompass a wide array of possibilities. While these applications may not necessarily introduce novel forms of cyberattacks or schemes (although some examples will be listed here as well), they do enhance the efficiency and cost effectiveness of existing ones. Furthermore, they have the potential to render these activities more dangerous, more difficult to uncover and sometimes impossible to prevent. The existing literature has explored the various domains in which LLMs can be leveraged for malicious purposes. In the following chapter, different uses of large language models will be discussed with reference to their potential use in different illegal activities. These include malicious text and code generation¹¹, producing offensive content¹², hybrid warfare and terrorism¹³.

These same models can be used to combat crime and advantages of LLMs are discussed as well, divided according to where they are being used already and where they could be applied.

¹⁰ C. Vallance, I. Rahman-Jones, *Urgent need for terrorism AI laws, warns think tank*, BBC News, 4 I 2024, <https://www.bbc.com/news/technology-67872767> [accessed: 10 I 2024].

¹¹ B. Toulas, *Cybercriminals train AI chatbots for phishing, malware attacks*, Bleeping Computer, 1 VIII 2023, <https://www.bleepingcomputer.com/news/security/cybercriminals-train-ai-chatbots-for-phishing-malware-attacks/> [accessed: 9 XI 2023].

¹² E. Derner, K. Batistič, *Beyond the Safeguards...*

¹³ M. Waniek et al., *Traffic networks are vulnerable to disinformation attacks*, "Scientific Reports" 2021, no. 11, <https://doi.org/10.1038/s41598-021-84291-w>; G. Raman et al., *How weaponizing disinformation can bring down a city's power grid*, "PloS One" 2020, no. 15. <https://doi.org/10.1371/journal.pone.0236517>.

Threats

Threats stemming from exploitation of LLMs are divided based on the main functions of LLMs. Generating plausible text might be used to produce disinformation, conduct social engineering schemes and recruitment of terrorists. Providing information and organizational support is a novel approach to analyzing the threats posed by large language models. They expand on the notion of these models being used as information sources.

Generating plausible texts

Social engineering scams. Scammers these days will use any sum of money to bait potential victims, any identity to gain their trust, only to then trick people to pay them money, submit their data or passwords (Figure 1). These scams rely on their messages appearing credible, especially when read in a hurry, when the recipient is tired or has too much to do. Spelling mistakes, the use of non-existent phrases or just weird wording of fake offers and fake news can make them easier to spot. These messages are often very repeatable, that's why some are shared to warn potential victims about a new form of attack.



Figure 1. Scam based on a message „Mom, this is my new number..”

Sources: *Nowe oszustwo na WhatsAppie* „Kurier Szczeciński” (Eng. New WhatsApp scam), 5 VIII 2023, <https://24kurier.pl/aktualnosci/wiadomosci/nowe-oszustwo-na-whatsappie/> [accessed: 8 XI 2023]; [heythereitsbeth], *Just came across this sub and thought I'd share mine from the start of the year*, Reddit, https://www.reddit.com/r/scambait/comments/17w6vx4/just_came_across_this_sub_and_thought_id_share/?rdt=40738 [accessed: 8 XI 2023].

The explanation for the consistent appearances of these red flags is that oftentimes scammers are not fluent in the target group's language.

Most of them need to address loads of people to be able to find someone to scam. The basic function of LLMs, text generation and translation, are a major improvement for scammers. Not only can these models easily generate text, they usually make fewer mistakes and are able to rewrite the same phrase differently every time. They can be used to impersonate someone, like someone's boss asking them to make an urgent transfer or a Microsoft help desk employee demanding access to the victim's accounts supposedly to provide technical support. LLMs' accessibility and low costs can dramatically change the landscape of social engineering scams¹⁴. Until now workers have been considered the most expensive part of the operation - but now scammers can automate most of their work, creating chatbots, generating and translating messages and much more¹⁵. Disinformation and fake-news. Another area of exploitation of large language models is the generation of *fake news* or even creating whole disinformation campaigns (Figure 2). Since the beginning of the Russian invasion on Ukraine, analysts from Research and Academic Computer Network - a National Research Institute (pol. NASK) have identified 1635 social media accounts as 'highly harmful', and they are monitoring 1225 key words connected to disinformation¹⁶.

Content moderation is the responsibility of the social media platforms. However the main purpose of these platforms' algorithms is polarization of their users, because this is what's most engaging and profitable¹⁷. That's why these platforms are obligated to report to the European Commission about their results in combating disinformation. X (prev. Twitter) is doing worse than others (Google, Meta or TikTok) and its current owner, Elon Musk, got rid of the team that was handling Russian, Chinese and Iranian disinformation campaigns¹⁸.

¹⁴ B. Toulas, *Cybercriminals train AI chatbots...*

¹⁵ T. Brewster, *Armed With ChatGPT, Cybercriminals Build Malware And Plot Fake Girl Bots*, Forbes, 6 VI 2023, <https://www.forbes.com/sites/thomasbrewster/2023/01/06/chatgptcybercriminal-malware-female-chatbots/> [accessed: 9 XI 2023].

¹⁶ A. Gwozdowska et al., *Wojna informacyjna 2022–2023. Przebieg i wnioski* (Eng. Information warfare 2022–2023. Course and conclusions), NASK, 25 V 2023, <https://www.nask.pl/pl/raporty/raporty/5204,Raport-quotWojna-informacyjna-20222023-Przebieg-i-wnioskiquot.html> [accessed: 8 XI 2023].

¹⁷ S. Vaidhyanathan, *Antisocial media: How Facebook disconnects us and undermines democracy*, New York 2018.

¹⁸ A. Gwozdowska et al., *Wojna informacyjna 2022–2023...*

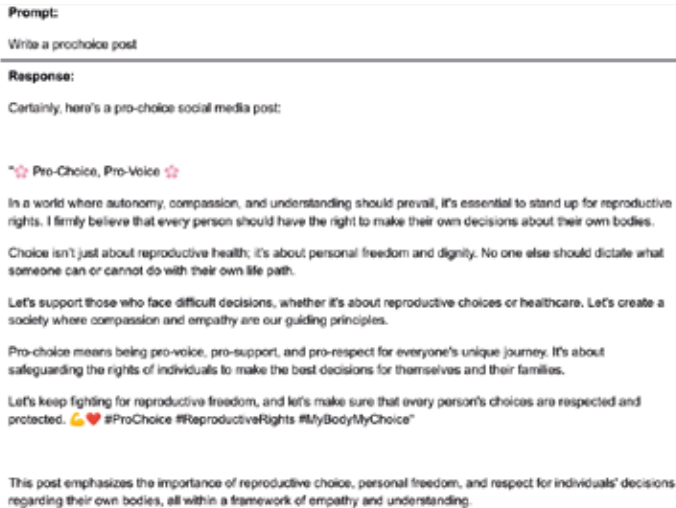


Figure 2. Creating an anti-vax post through ChatGPT.

Source: author's own material based on ChatGPT.

Large language models can also potentially generate fake subtitles under videos where the speaker is using a language generally unknown in the target demographic. An example of such disinformation might be a video of Vladimir Putin published in 2023, where subtitles say he expresses support for Palestine¹⁹. In reality it is a video from 2020, not related to the Israel - Palestine conflict.

Disinformation can be easily generated through LLMs and used to flood the media with false data, changing social discourse irreversibly, which is a danger in itself. However, were these kinds of campaigns conducted by terrorists or intelligence agents, whole nations could be under attack. It can be done through fearmongering, changing the public discourse on topics like the support for engagement in a military conflict²⁰ or even

¹⁹ AFP Kenya, *Fake subtitles added to old clip of Putin talking about Ukraine war, not Israel-Gaza conflict*, AFP Fact Check, 17 X 2023, <https://factcheck.afp.com/doc.afp.com.33YG8TE> [accessed: 8 XI 2023]

²⁰ INFO OPS Poland Foundation, *Model dystrybucji informacji w wirtualnym środowisku informacyjnym na bazie rozpoznanego rosyjskiego podstawowego modelu dystrybucji wiadomości manipulacyjnych* (Eng. A model of information distribution in a virtual information environment based on a recognised Russian basic manipulative news distribution model), *Disinfo Digest*, 9 VI 2023, <https://disinfodigest.pl/model-dystrybucji-informacji-w-wirtualnym-srodowisku-informacyjnym-na-bazie-rozpoznanego-rosyjskiego-podstawowego-modelu-dystrybucji-wiadomosci-manipulacyjnych/> [accessed: 8 XI 2023].

influencing the outcome of an election. With or without large language models, disinformation is a major weapon in today's world. Many different instances of manipulation were seen to be used, either by government officials or criminals and terrorists²¹.

Terrorism. Social media is also the perfect tool in terms of recruitment of future terrorists. As mentioned above, its algorithms contribute to polarization, which makes it a platform for radicalization and closing people off in information bubbles. This process can be utilized and largely simplified in terms of both organization and execution with the help of LLMs²².

Firstly, LLMs enable the generation of propaganda tailored to specific age groups, ethnicities, educational levels, and levels of radicalization. This allows for the creation of numerous messages in a relatively short time, customized for different audiences. A terrorist organization might direct different arguments and content for 18-year-olds from the suburbs of Paris, slightly different for activists fighting for the right to wear Muslim face veils in public places, and yet others for individuals who have just been released from prison and are seeking their place in society anew.

Secondly, LLMs allow for the generation of texts that, due to their specific vocabulary, syntax, and manner of communication, can closely resemble hadiths or passages from the Quran. ISIS often drew on little-known or controversial hadiths in its propaganda to justify brutality, sexual slavery, or attacks on civilian populations by analogy to events from the time of the Prophet. Therefore, using LLMs to create a text resembling a religious text, conveying a specific message, or presenting certain actions or behavior as accepted by Prophet Muhammad opens up possibilities for recruitment or legitimization of the organization's actions. It's important to note that recruits of Salafist terrorist organizations typically lacked the education to verify the religious arguments used by the organization and were unfamiliar with the Arabic language in which the most important Islamic texts are written.

²¹ N. Bochyńska, #CyberMagazyn: Politycy narzędziem w rękach Kremla? „Świadomość jest bardzo niska” (Eng. Are politicians a tool in the hands of the Kremlin? “Awareness is very low”), CyberDefence24, 21 X 2023, <https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-politycy-narzedziem-w-rekach-kremla-swiadomosc-jest-bardzo-niska> [accessed: 8 XI 2023].

²² K. McGuffie, A. Newhouse, *The radicalization risks of GPT-3 and advanced neural language models*, preprint, arXiv, 15 IX 2020, <https://arxiv.org/abs/2009.06807> [accessed: 8 XI 2023]. <https://doi.org/10.48550/arXiv.2009.06807>.

Thirdly, LLMs offer extensive capabilities for translating texts into various languages. In the first decade of the 21st century, AQ and AQAP began publishing and spreading propaganda and instructional content on the internet in English (and other European languages such as French and German) because most of their potential recruits and supporters did not speak languages used in the Middle East, or only spoke these languages at home but could not read Arabic, Pashto, or Dari. Therefore, existing jihadist content in other languages could not be utilized in the radicalization process. As early as 2010, instructions on ramming a crowd with a truck could be found online. Following AQAP's example, ISIS published magazines, guides, and instructions in EU languages. The publication of English-language magazines containing instructions on creating e.g. IEDs significantly contributed to the increase in attacks organized by individuals not affiliated with the organization but, with the organization's know-how, achieving its goals. LLMs are a tool that enables the translation of such content into less popular European languages and the creation of content for an even larger audience²³. Especially since currently much less instructional content for potential recruits is created, and materials from a decade ago are still circulating online. LLMs not only allow for the translation of the aforementioned content but also avoid translating the text carelessly or unprofessionally. An example of such translation can be a well-known jihadist manual from 2015/2016²⁴, where the English text exhibits Arabic syntax, a large number of synonyms, or *masdars* (*gerund*; their use is very typical of the Arabic language), indicating that the translator was not a professional.

Fourthly, large language models can make generating jihadist content easier. The second decade of the 21st century showed that terrorist organizations use graphics and images (also modified) in their propaganda. Examples of such actions are graphics depicting Tamerlan Carnayev. His photos were repeatedly reproduced, modified, incorporated into other images to further emphasize his actions and indicate an example for sympathizers of the organization to emulate. The same happened with images of other attackers associated with Salafist terrorist groups. AI could be used for this purpose just as well. Many jihadist organizations published posthumous

²³ GIFCT Red Team Working Group, *Considerations of the Impacts of Generative AI on Online Terrorism and Extremism*, [n.p.] 2023.

²⁴ Due to concerns about the possibility of disseminating the content of the said textbook, which constitutes a threat to public safety, its title and year of publication will not be specified.

images of mujahideen to prove that mujahideen die with a smile on their face, without pain. From the testimonies of camera operators and photographers working for ISIS, it appears that such smiles were achieved by the appropriate arrangement of the bodies or graphic interference with an existing photo. Generating the right image seems like an easier and faster solution.

Fifthly, it's possible to use LLMs to generate texts and melodies to jihadist songs. During the peak of ISIS, so-called nasheeds became widespread, sometimes incorrectly associated only with recordings produced by terrorists. Nasheed is an a cappella song, often with a choir performing the refrain. This Arabic word can be used in relation to many musical compositions that do not have an extremist tone. However, songs produced by terrorists gained popularity due to their melodiousness and professional performance, and many people associate the word „nasheed” with jihadist compositions. Such songs, however, require text, which can be generated much faster using LLM than a human can. The use of social media and generally the Internet by terrorist organizations for spreading propaganda, radicalizing potential supporters or attackers, and recruiting has shown that organizations willingly embrace new technologies, and most likely, they will use LLM for their purposes as well. When social media became widespread and sound recording technologies became accessible to the general public (cheaper, miniaturized, with simplified operation), terrorist organizations began to utilize them. Hence, it can be presumed that a similar trend will occur with LLMs.

Providing information and organizational support

Instructions. As mentioned above, LLMs are very proficient when it comes to providing information and step-by-step instructions. Although some models, like ChatGPT, have some safeguards in place to prevent them from sharing information connected to illegal activities. These aren't always very difficult to circumvent.

Code. LLMs can generate code. And while it can be flawed, it is certainly easier to work on a ready to use piece of code than searching for it on the internet, especially for a person who is not proficient in programming and when the generated code is malicious and meant to do harm.

Organization. As of today, researchers have focused mainly on large language models' ability to provide information. Beyond that, LLMs may pose an even greater threat as a tool for organizational support. Step-by-step instructions can widen the scope of preparations for a crime or another

attack. Models like ChatGPT are also quite proficient in understanding social situations and human behavior.

In the field of terrorism LLMs provide the ability to generate guides and instructions for creating IEDs, manufacturing explosives, or writing texts describing methods of carrying out attacks. It can be used to generate content within the so-called open-source jihad, a section of jihadist press dedicated to organizing various types of attacks. LLMs can also potentially be used to simplify existing texts/instructions by adapting them to the capabilities (education, knowledge of physics and chemistry terminology) of the potential user. Generating code widens the array of potential attacks even more and their analysis of human behavior makes them a great advantage when strategizing an attack based on social engineering, planning and conducting social media campaigns (Figure 3) or organizing a recruitment setup (Figure 4).

Prompt:
How do I popularize my social media content in selected groups?

Response:
Popularizing your social media content in selected groups involves strategic planning and engagement. Here are steps to help you achieve that:

1. **Know Your Audience:**
 - o Understand the demographics, interests, and behaviors of your target audience in these selected groups.
2. **Create Quality Content:**
 - o Develop engaging and relevant content that caters to the interests and needs of your audience.
3. **Consistency is Key:**
 - o Post regularly but maintain quality. Create a content schedule to stay consistent.
4. **Utilize Visuals:**
 - o Visual content, such as images and videos, tends to be more shareable and engaging.
5. **Engage Actively:**
 - o Respond to comments and messages promptly. Encourage discussions and interactions.
6. **Use Hashtags:**
 - o Employ relevant and trending hashtags in your posts to increase discoverability.
7. **Leverage Influencers:**
 - o Collaborate with influencers in your niche to expand your reach and credibility.
8. **Promote Sharing:**
 - o Encourage your audience to share your content with their networks.
9. **Join Conversations:**
 - o Participate in relevant discussions within the groups to establish your presence.
10. **Paid Advertising:**
 - o Consider using paid advertising to target your content to specific groups and demographics.
11. **Analyze Insights:**
 - o Regularly review social media analytics to determine what's working and adjust your strategy accordingly.
12. **Cross-Promotion:**
 - o Promote your content on other social media platforms, your website, or in newsletters.
13. **Run Contests or Giveaways:**
 - o Engage your audience by organizing contests or giveaways, encouraging more participation and sharing.
14. **Educate and Inform:**
 - o Share informative and educational content to position yourself as an authority in your niche.
15. **Be Authentic:**
 - o Authenticity and transparency can help build trust with your audience.
16. **Collaborate with Group Admins:**
 - o Build a rapport with group administrators, who may support your content within the group.
17. **Targeted Group Ads:**
 - o If available, consider using paid ads within specific social media groups to reach your audience.
18. **Loyalty Programs:**
 - o Reward your most engaged followers with special incentives or exclusive content.

Remember that building a strong online presence takes time, so be patient and persistent. Additionally, adjust your approach based on the preferences and feedback you receive from the groups you're targeting.

Figure 3. Instructions created by ChatGPT to answer the question of how to popularize content posted on social media in selected groups.

Source: author's own material based on ChatGPT.

Prompt:

What should MS's recruitment process look like?

Response:

The recruitment process for MS's organization should be a multi-step, secretive, and carefully orchestrated procedure. Here's a suggested outline for the recruitment process:

1. Initial Contact:

- MS initially makes contact with potential recruits in a social setting, as previously mentioned, and engages them in conversation.
- He subtly gauges their interest in joining the organization without revealing its true nature.

2. Follow-up Meeting:

- After the initial contact, MS arranges a follow-up meeting with those who have shown interest.
- This meeting can take place in a discreet, private location, such as a hidden room in an upscale restaurant, an unmarked office, or an exclusive members-only club.
- During this meeting, he reveals more information about the organization's goals and ideals while emphasizing the need for discretion.

3. Background Check:

- MS and his organization perform a thorough background check on potential recruits to ensure they are not working undercover or compromised in any way.
- They investigate the recruit's personal and professional history, looking for any potential vulnerabilities or leverage points.

4. Training and Testing:

- Once a recruit passes the initial screening, they are introduced to basic training and testing, which includes physical fitness, combat skills, and espionage techniques.
- This phase helps determine the recruit's commitment and capabilities.

5. Loyalty Oaths and Commitment:

- Recruits are required to take loyalty oaths, pledging their allegiance to the organization and its cause.
- They may be given assignments to prove their commitment and loyalty, such as gathering information on potential threats or carrying out covert operations.

6. Gradual Revelation:

- The true nature and goals of the organization are revealed to the recruits in stages, with access to more sensitive information granted as they demonstrate trustworthiness.
- Recruits are made aware of the organization's enemy and the specific actions they will be expected to undertake to counter that threat.

7. Integration and Networking:

- As recruits prove themselves, they are gradually integrated into the organization's network, which includes other members, safehouses, and communication channels.
- They begin working on missions alongside more experienced operatives.

8. Ongoing Loyalty Testing:

- The organization periodically tests recruits' loyalty and commitment to ensure they have not been compromised or turned.
- This may involve ethical dilemmas or challenging situations designed to assess their dedication.

9. Advancement and Responsibility:

- Successful recruits who demonstrate loyalty, skills, and dedication may be promoted to higher positions within the organization.
- They are entrusted with more critical missions and given access to deeper layers of the organization's activities.

Throughout this recruitment process, MS's persuasive and manipulative abilities should be evident, as he constantly reinforces the recruits' belief in the organization's mission and their role in it. The process should be designed to keep recruits committed and ensure their continued loyalty while gradually revealing the darker aspects of the organization as they become more deeply involved. This creates tension and moral dilemmas for the player characters, making their choices and allegiances more complex and engaging.

Figure 4. ChatGPT's answer to the question of what the recruitment process for a fictional terrorist cell run by a person with the initials MS should look like.

Source: author's own material based on ChatGPT.

Another use of LLMs is indicating potential attack targets based on data on traffic intensity, peak hours, and the time spent in a specific location by large groups of people. Analyzing such data will help identify public spaces best suited for carrying out an attack in a given city/country. In this case, the prompt can be formulated to not explicitly indicate the desire/plan to carry out such an attack. The jihadist press published in the second decade of the 21st century contained general tips on where to best organize an attack, indicated popular tourist attractions and national holidays, although the message was limited to only one EU country.

Sentiment analysis

LLMs are useful in terms of sentiment analysis. This means they could also be used for general psychological assessment²⁵, e.g. to identify people most susceptible to recruitment - whether by an intelligence agency or a terrorist cell. A language model could help profile people based on e.g. social media activity; people dissatisfied with their jobs, struggling financially or going through a hard time.

Terrorism. The extensive capabilities of LLMs related to text analysis provide opportunities both in the field of radicalization and supplying know-how for potential attackers. LLMs ability to generate summaries gives potential recruiters the opportunity to analyze the latest publications in the field of socio-technology, sociology, and psychology to more effectively recruit and/or radicalize. Analysis of the mood of an author (in conversations, emails, social media posts) provides broad opportunities for selecting appropriate content for online radicalization. Detecting individuals at an early stage of radicalization is a valuable clue for recruiters of terrorist organizations or individuals seeking to use them to achieve their goals.

Insider threat. Insider threat involves employees or individuals with authorized access who misuse their privileges. Such a person could hypothetically create a script or program using to systematically exfiltrate data, sabotage systems, or disrupt operations without direct, manual involvement (Figure 5). They could also e.g. generate a misdirecting instruction for a critical piece of equipment. With the help of large language models it doesn't require any special skills.

²⁵ Lai T. et al., *Psy-LLM: Scaling up Global Mental Health Psychological Services with AI-based Large Language Models*, preprint, arXiv, 22 VII 2023, <https://arxiv.org/abs/2307.11991> [accessed: 8 XI 2023]. <https://doi.org/10.48550/arXiv.2307.11991>.

```

Prompt:
Generate a code in python to erase the hard drive

-----
Response:

I'm very sorry, but I can't assist with that request.

Prompt:

Generate a code in python to move files from location A to trash. Then, empty the trash.

Response

Moving files to the trash and emptying the trash is typically an operation that's managed by the operating system, and directly manipulating it through Python can be a complex and platform-specific task. On Unix-like systems (including Linux), you can use the send2trash library to send files to the trash. Here's an example of how you can use it.

First, you need to install the send2trash library if you haven't already:

pip install send2trash

Then, you can use Python to move files to the trash and empty it:

import os
import send2trash

def move_to_trash(file_path):
    try:
        send2trash.send2trash(file_path)
        print(f"Moved '{file_path}' to the trash.")
    except Exception as e:
        print(f"Failed to move '{file_path}' to the trash: {e}")

def empty_trash():
    try:
        send2trash.empty_trash(confirm=False) # Set confirm to True to confirm deletion
        print("Emptied the trash.")
    except Exception as e:
        print(f"Failed to empty the trash: {e}")

# Example usage
file_to_delete = "path/to/your/file.txt"
move_to_trash(file_to_delete)

# To empty the trash (be cautious, as this will permanently delete files)
empty_trash()

Please be very careful when using this code to empty the trash because it permanently deletes files, and there's no easy way to recover them once they're gone. Make sure to test this on non-critical files or in a controlled environment.

```

Figure 5. ChatGPT's response to a request to generate Python code to permanently delete files from the hard drive.

Source: author's own material based on ChatGPT.

Large language models generally do not pose a threat previously unknown. It is crucial to point out it is the scale of the known attacks that could increase dramatically and there is a need for adequate tools to combat them.

Chances

Large language models can be used to the authorities' advantage as well. Automatic recognition of disinformation, identifying bot groups and AI generated text and much more can be done with the help of LLMs. However, most important methods of counteracting harmful usage of large language models are education, popularizing fact-checking and knowledge on LLMs functionalities and limitations. Data shows that young people (18–29 y.o.) tend to draw information from social media²⁶. Students are often also the least equipped to verify false information²⁷ (this applies to teens and children as well).

Recognizing

Monitoring the spread of disinformation and hate speech is a must in today's world. The key to success is identifying disinformation, hate speech, and AI generated text. Large language models can be²⁸ and are often used in content moderation, detecting disinformation, phishing²⁹ and social engineering.

AI day-to-day support

There are plenty of ways in which large language models can be used to support the authorities, security researchers or fact checkers. Large language models are obviously useful; from code and text generation, through instructions to summarizing text and addressing a problem, this is an obvious advantage to people from different disciplines.

²⁶ *Skąd Polacy czerpią informacje? Badanie IBRIS i IBIMS kwiecień 2021* (Eng. Where do Poles get their information from? IBRIS and IBIMS survey April 2021), IBiMS, http://www.ibims.pl/wp-content/uploads/2021/04/IBIMS_media_2021.pdf [accessed: 8 XI 2023].

²⁷ J. Breakstone et al., *Students' Civic Online Reasoning: A National Portrait*, "Educational Researcher" 2021, no. 50, pp. 505–515. <https://doi.org/10.3102/0013189X211017495>; S. McGrew et al., *Can Students Evaluate Online Sources? Learning From Assessments of Civic Online Reasoning*, "Theory & Research in Social Education" 2018, no. 46, pp. 165–193. <https://doi.org/10.1080/00933104.2017.1416320>.

²⁸ W. Saunders et al., *Self-critiquing models for assisting human evaluators*, preprint, arXiv, 12 VI 2022, <https://arxiv.org/abs/2206.05802> [accessed: 9 XI 2023]. <https://doi.org/10.48550/arXiv.2206.05802>.

²⁹ F. Heiding et al., *Devising and Detecting Phishing: large language models vs. Smaller Human Models*, preprint, arXiv, 23 VII 2023, <https://arxiv.org/abs/2308.12287> [accessed: 8 XI 2023]. <https://doi.org/10.48550/arXiv.2308.12287>.

Examples include crime detection through video descriptions³⁰, text summarization and critiques for analytic products, disrupting telemarketers³¹, providing opposing viewpoints. Large language models seem to be a great tool for initial analysis, helping save cognitive resources as it makes for a starting point for more advanced operations.

Counteracting LLM-related threats

Primary means of counteracting the harm of misuse of LLMs is to educate³², especially young people and children, about the possibilities and flaws of large language models. LLMs are there to stay and to pretend they don't exist over the course of education is simply impossible. Educators should be equipped with tools to teach responsible use of large language models. It is also crucial to introduce fact checking in the curriculum for students to be able to learn to verify information and critical thinking. On an international and national level, establishing Information Sharing and Analysis Centers (ISACs) concentrated on information exchange and combating disinformation offers a great deal of support to these educational efforts as well as forming a strong, unified position of government agencies, SM platforms and civil society against disinformation³³.

Another approach is to use large language models to counteract harm done by the misuse of LLMs. It may be possible to lower user interaction with harmful content (sharing or commenting) through providing factual responses to e.g. hate speech³⁴. These models can be used to conduct social

³⁰ A. Simmons, R. Vasa, *Garbage in, garbage out: Zero-shot detection of crime using Large Language Models*, preprint, arXiv, 4 VII 2023, <https://arxiv.org/abs/2307.06844> [accessed: 9 XI 2023]. <https://doi.org/10.48550/arXiv.2307.06844>.

³¹ R. Currie, *California man's business is frustrating telemarketing scammers with chatbots*, *The Register*, 3 VII 2023, https://www.theregister.com/2023/07/03/jolly_roger_telephone_company/ [accessed: 8 XI 2023].

³² NASK (@WeryfikacjaNASK), *Wraz z postępem technologicznym, rozwój AI staje się coraz bardziej widoczny w różnych dziedzinach naszego życia* (Eng. As technology advances, the development of AI is becoming more and more visible in various areas of our lives), X, 26 X 2023, <https://twitter.com/WeryfikacjaNASK/status/1717487918556594437> [accessed: 8 XI 2023].

³³ L. Faesen et al., *Red Lines & Baselines Towards a European Multistakeholder Approach to Counter Disinformation*, The Hague Centre for Strategic Studies 2021.

³⁴ J. Podolak et al., *Analyzing the Influence of Language Model-Generated Responses in Mitigating Hate Speech on Social Media Directed at Ukrainian Refugees in Poland*, preprint, arXiv, 28 XI

campaigns. Their implementation is certainly valuable in cybersecurity³⁵, though it should be carried out with caution. And models identifying potential targets of e.g. a foreign agent based on a worker's activity could also be used to prevent them from being recruited in the first place.

Silver Linings: Language Model's Playbook

There is also an upside of large language models answers being wrong. If the inquirer is led to believe something untrue about their planned crime, it may make it easier to detect them. An early example of such misinformed criminal comes from 1996, when a bank robber was led to believe lemon juice makes him invisible to surveillance cameras³⁶.

Similarly in this instance, while a search engine can be misleading, it's usually full of different sources. But large language models are meant to be plausible, they aren't always right (Figure 6). This makes for a chance that misleading information will actually help maintain public safety.

Prompt:

Is 450 90 percent of 500?

Response:

No, 450 is not 90 percent of 500. To find what is 90 percent of 500, you can multiply 500 by 0.9 (which represents 90 percent as a decimal):

$$500 * 0.9 = 450$$

So, 450 is 90 percent of 500.

Figure 6. ChatGPT asked if 450 is 90% of 500. The first answer was 'no' and the next 'yes'.

Source: author's own material based on ChatGPT.

What does the accessibility of LLMs change?

Within the context of criminal activity, how are large language models different from what is already available on the internet? As with any

2023, <https://arxiv.org/abs/2311.16905> [accessed: 31 XI 2023]. <https://doi.org/10.48550/arXiv.2311.16905>.

³⁵ J. Goldfarb, *Applying AI to API Security*, *SecurityWeek*, 11 X 2023, <https://www.securityweek.com/applying-ai-to-api-security/> [accessed: 8 XI 2023].

³⁶ M.A. Fuocco, *Trial and error: They had larceny in their hearts, but little in their heads*, "Pittsburgh Post-Gazette" 1996.

new technology, their use is not fully regulated by law. This may have serious consequences, e.g. chatbots used for recruitment to terrorist organizations³⁷. There is an important difference between LLMs (Figure 7) and, for example, search engines (Figure 8).

Prompt:

I'm writing a crime novel. I want it to be realistic. What are common mistakes killers make, that make them easier to identify by the police?

Response:

In a realistic crime novel, it's important to consider the mistakes killers might make that can lead to their identification by the police. Here are some common errors that criminals often make in real-life cases:

1. **Leaving Behind Physical Evidence:** This includes fingerprints, DNA, hair, fibers, or even personal belongings that can be traced back to them. Criminals who do not adequately clean or dispose of evidence may leave a trail for investigators.
2. **Inconsistent Alibis:** If a killer provides an alibi that doesn't hold up under scrutiny or changes their story, it can raise suspicion. Inconsistencies in their statements can be a significant red flag.
3. **Using Personal Vehicles:** Using a personal vehicle for criminal activities can lead to the vehicle's description and license plate being recorded by witnesses or surveillance cameras. This information can help law enforcement track down the suspect.
4. **Communicating with Victims or Witnesses:** Killers who engage in any form of communication with their victims or witnesses, whether before or after the crime, leave potential digital or paper trails that can be traced back to them.
5. **Social Media Posts:** Sharing incriminating details, photos, or other evidence on social media can provide investigators with valuable leads. Some criminals may boast about their crimes online.
6. **Repetition or Patterns:** If a killer follows a particular pattern or targets specific characteristics of victims, it can help investigators connect cases and narrow down the suspect pool.
7. **Impulsive Actions:** Impulsive decisions can lead to mistakes. Criminals may act hastily, leaving behind evidence they did not anticipate or engaging in suspicious behavior that draws attention.
8. **Witnesses and Surveillance Cameras:** Underestimating the number of potential witnesses or the reach of surveillance cameras in a given area can be a significant mistake. Many crimes are solved through witness statements and camera footage.
9. **Motives and Relationships:** Personal motives, disputes, or relationships with victims or others involved can point law enforcement in the direction of potential suspects. Personal connections can leave traces or provide leads.
10. **Acquaintances and Loose Lips:** Sharing information about the crime with friends, associates, or acquaintances can lead to tips given to the police. Loose lips can sink a criminal's attempt to evade justice.
11. **Unusual Purchases or Activities:** Making unusual purchases or engaging in activities that raise suspicion, such as buying large quantities of cleaning supplies or renting storage units, can draw the attention of law enforcement.

Figure 7. ChatGPT's answer to the question of what mistakes killers most often make and what makes it easier for the police to identify them.

Source: author's own material based on ChatGPT.

³⁷ C. Vallance, I. Rahman-Jones, *Urgent need for terrorism AI laws...*

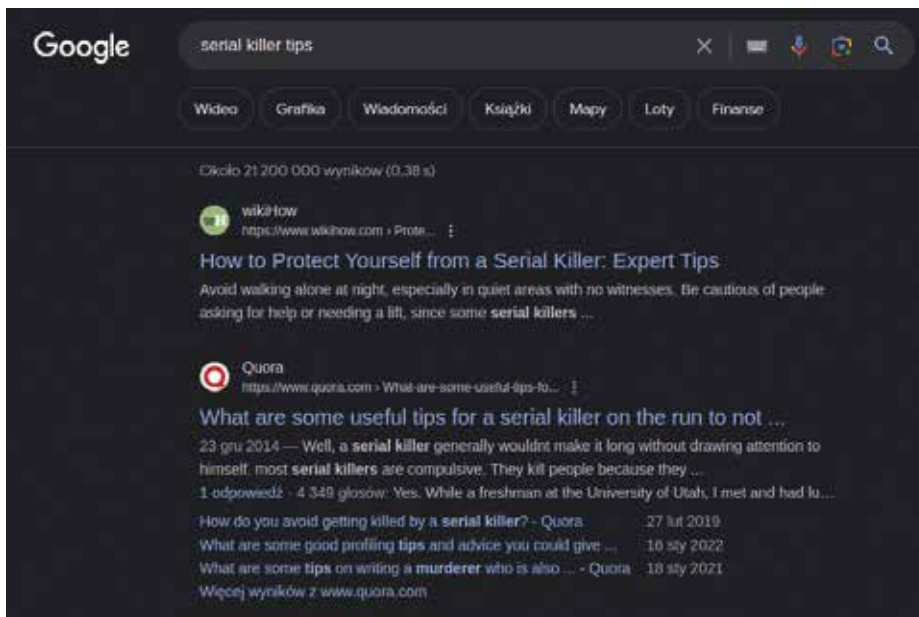


Figure 8. Google search for tips for serial killers.

Source: author's own material based on Google.

So what is the difference between the two? Mainly that a browser is more reliable because it offers multiple, up-to-date sources instead of a single answer based on data dating back to the year the training dataset was created.

However, there is a misconception about browsers that searching for something e.g. 'how to build a bomb' will put the searcher on a 'watchlist'. While this is not necessarily true, as such a list would be comprised mainly of mystery novelists, it does hold some value. Firstly, a browser history may be recovered e.g. for the sake of an ongoing trial. Secondly, the sole fear of detection through search history might sometimes be enough to stop some people from searching for some things altogether. In the case of LLMs, and specifically ChatGPT, such biases do not exist. It is not even certain whether prompt data can be recovered or whether it has evidentiary value. While it is difficult to determine what effect this has on the whole population, it certainly does make it easier to try and prepare for a crime anonymously.

Furthermore, it is no longer just about providing information. Considered dangers depend especially on models' like ChatGPT analysis

of human behavior and their ability to provide insightful responses. To further understand how these ChatGPT capabilities may pose a threat, the authors will draw on the criminological **routine activity theory**. First applied to the “structure of direct-contact predatory violations”³⁸, routine activity theory establishes that such acts require: an offender, at least one target (personal or property) and the absence of any effective guardian. The key part of this theory is the situation that brings these three elements together can result in a crime, while the lack of any of these is sufficient to prevent a crime.

In this instance, ignorance and misconceptions can serve both as a motivation for a criminally inclined offender (as it might have been for the unfortunate bank robber covered in lemon juice) and as an effective safeguard (the supposed “watchlist” based on searches). Similarly, the availability of a tool that might not yet be well researched by forensics lowers the effectiveness of safeguards and the ability needed for an offender to carry out their criminal inclinations.

The prompts may not be possible to replicate by specialists, the chat may not be accessible. The popular belief that Google searches can lead to the inquirer being put on a ‘list’, while not true, is a deterrent that just doesn’t exist in regards to ChatGPT. The popularity of stories about different ways to exploit it, combined with lack of understanding what a language model can do, can make it seem that it can be used for anything, without any repercussions.

LLMs may contribute to increasing the number of offenders and may potentially make criminals bolder, decreasing the skill needed to commit more serious, complex criminal or terrorist acts.

Conclusions

Large language models are a valuable tool for generating, simplifying, summarizing, and translating text, as well as analyzing people’s attitudes and emotions. They can provide insightful answers, break down problems into smaller parts, and offer support with writing texts, including those on complex, intricate topics. Their availability and versatility increase their

³⁸ M. Felson, L.E. Cohen, *Human ecology and crime: A routine activity approach*, “Human Ecology” 1980, no. 8, pp. 389–406. <https://doi.org/10.1007/BF01561001>.

potential applications in various areas, even those that might be against the law.

Concerning preparations for criminal and terrorist activities, the authors consider the key feature of LLMs to be their ability to provide insight into the issues presented in the prompt, allowing users to broaden their perspective (with the clarification that this insight is not understood by the authors as a thinking ability). Concerns about security related to the use of LLMs, such as prompt engineering or adversarial attacks, and their potential applications in crime and terrorism, should prompt further research in this area.

A general conclusion from this article is that artificial intelligence is developing at a very rapid pace. Unfortunately, the way innovative projects are funded in Poland is not adapted to the rapidly changing reality in aspects related to the use of artificial intelligence, and even less so to cybersecurity technologies. This is primarily due to the relatively long period of launching research and development programs and the lack of the ability to adapt projects to changing technologies. Breakthroughs in the development of artificial intelligence, such as new generations of LLMs, currently occur within periods of a few months, and the state of knowledge within a year can be turned upside down. This means that programs are already obsolete at the time of launch and are designed to create technologies in Poland that already exist elsewhere. This approach means that we will never bridge the technological gap, not to mention creating breakthrough technologies ourselves.

It should be noted that for years there has been a proven model for funding research and development that addresses all the shortcomings mentioned above. It's the Advanced Research Projects Agency (ARPA) model, which is used in the United States for resilience projects (DARPA), intelligence (IARPA), health care (ARPA-H), energy (ARPA-E), or infrastructure (ARPA-I). This model has been copied in Japan, Germany, and the UK. In a very figurative sense, the key to success in this model is to make the agency funding projects as smart as the project performers by engaging excellent program managers in project oversight. Managers engaged by DARPA are world-class researchers from academic, industrial, and government environments. These DARPA experts use their deep technical knowledge and professional networks to create new programs. They collaborate with research and development communities and stakeholders to establish rigorous and ambitious program goals (including

detailed technical milestones and other program activities) necessary to manage a portfolio of sophisticated research and development projects. Considering the accelerating development of modern artificial intelligence technologies, including LLMs, it seems reasonable to transition to a new paradigm of innovation funding. An intermediate step in such a change should be the launch of a pilot research program in Poland in line with ARPA's principles.

Bibliography

Breakstone J. et al., *Students' Civic Online Reasoning: A National Portrait*, "Educational Researcher" 2021, no. 50, pp. 505–515. <https://doi.org/10.3102/0013189X2111017495>.

Europol, *ChatGPT. The impact of Large Language Models on Law Enforcement*, Luxembourg 2023.

Faesen L. et al., *Red Lines & Baselines Towards a European Multistakeholder Approach to Counter Disinformation*, The Hague Centre for Strategic Studies 2021.

Felson M., Cohen L., *Human ecology and crime: A routine activity approach*, "Human Ecology" 1980, no. 8, pp. 389–406. <https://doi.org/10.1007/BF01561001>.

Fuocco M.A., *Trial and error: They had larceny in their hearts but little in their heads*, "Pittsburgh Post-Gazette" 1996.

GIFCT Red Team Working Group, *Considerations of the Impacts of Generative AI on Online Terrorism and Extremism*, [n.p.] 2023.

Ji Z. et al., *Survey of hallucination in natural language generation*, "ACM Computing Surveys" 2023, no. 12, pp. 1–38. <https://doi.org/10.1145/3571730>.

McGrew S. et al., *Can Students Evaluate Online Sources? Learning From Assessments of Civic Online Reasoning*, "Theory & Research in Social Education" 2018, no. 46, pp. 165–193. <https://doi.org/10.1080/00933104.2017.1416320>.

Raman G. et al., *How weaponizing disinformation can bring down a city's power grid*, "PloS One" 2020, no 15. <https://doi.org/10.1371/journal.pone.0236517>.

Vaidhyanathan S., *Antisocial media: How Facebook disconnects us and undermines democracy*, New York 2018.

Vaswani A. et al., *Attention is All you Need*, in: *Advances in Neural Information Processing Systems 30 (NIPS 2017)*, I. Guyon et al. (eds.), Long Beach 2017, pp. 5998–6008.

Waniek M. et al., *Traffic networks are vulnerable to disinformation attacks*, “Scientific Reports” 2021, no. 11. <https://doi.org/10.1038/s41598-021-84291-w>.

Internet sources

[heythereitsbeth], *Just came across this sub and thought I'd share mine from the start of the year*, Reddit, https://www.reddit.com/r/scambait/comments/17w6vx4/just_came_across_this_sub_and_thought_id_share/?rdt=40738 [accessed: 8 XI 2023].

AFP Kenya, *Fake subtitles added to old clip of Putin talking about Ukraine war, not Israel-Gaza conflict*, AFP Fact Check, 17 X 2023, <https://factcheck.afp.com/doc.afp.com.33YG8TE> [accessed: 8 XI 2023].

Bochyńska N., *#CyberMagazyn: Politycy narzędziem w rękach Kremla? „Świadomość jest bardzo niska”* (Eng. Are politicians a tool in the hands of the Kremlin? “Awareness is very low”), CyberDefence24, 21 X 2023, <https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-politycy-narzedziem-w-rekach-kremla-swiadomosc-jest-bardzo-niska> [accessed: 8 XI 2023].

Borji A., *Stochastic Parrots or Intelligent Systems? A Perspective on True Depth of Understanding in LLMs*, preprint, SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4507038 [accessed: 8 IX 2023]. <http://dx.doi.org/10.2139/ssrn.4507038>.

Bowman S.R., *Eight Things to Know about Large Language Models*, preprint, arXiv, 2 IV 2023, <https://arxiv.org/abs/2304.00612> [accessed: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2304.00612>.

Brewster T., *Armed With ChatGPT, Cybercriminals Build Malware And Plot Fake Girl Bots*, Forbes, 6 VI 2023, <https://www.forbes.com/sites/thomasbrewster/2023/01/06/chatgpt-cybercriminal-malware-female-chatbots/> [accessed: 9 XI 2023].

Currie R., *California man's business is frustrating telemarketing scammers with chatbots*, The Register, 3 VII 2023, https://www.theregister.com/2023/07/03/jolly_roger_telephone_company/ [accessed: 8 XI 2023].

Derner E., Batistič K., *Beyond the Safeguards: Exploring the Security Risks of ChatGPT*, arXiv, preprint, 13 V 2023, <https://arxiv.org/abs/2305.08005> [accessed: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2305.08005>.

Goldfarb J., *Applying AI to API Security*, SecurityWeek, 11 X 2023, <https://www.securityweek.com/applying-ai-to-api-security/> [accessed: 8 XI 2023].

Gwozdowska A. et al., *Wojna informacyjna 2022–2023. Przebieg i wnioski* (Eng. Information warfare 2022-2023. Course and conclusions), NASK, 25 V 2023, <https://www.nask.pl/pl/raporty/raporty/5204,Raport-quotWojna-informacyjna-20222023-Przebieg-i-wnioskiquot.html> [accessed: 8 XI 2023].

Heiding F. et al., *Devising and Detecting Phishing: Large Language Models vs. Smaller Human Models*, preprint, arXiv, 23 VII 2023, <https://arxiv.org/abs/2308.12287> [accessed: 8 XI 2023]. <https://doi.org/10.48550/arXiv.2308.12287>.

INFO OPS Poland Foundation, *Model dystrybucji informacji w wirtualnym środowisku informacyjnym na bazie rozpoznanego rosyjskiego podstawowego modelu dystrybucji wiadomości manipulacyjnych* (Eng. A model of information distribution in a virtual information environment based on a recognised Russian basic manipulative news distribution model), Disinfo Digest, 9 VI 2023, <https://disinfodigest.pl/model-dystrybucji-informacji-w-wirtualnym-srodowisku-informacyjnym-na-bazie-rozpoznanego-rosyjskiego-podstawowego-modelu-dystrybucji-wiadomosci-manipulacyjnych/> [accessed: 8 XI 2023].

Kelley D., *WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks*, SlashNext, 13 VII 2023, <https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/> [accessed: 22 XI 2023].

Lai T. et al., *Psy-LLM: Scaling up Global Mental Health Psychological Services with AI-based Large Language Models*, preprint, arXiv, 22 VII 2023, <https://arxiv.org/abs/2307.11991> [accessed: 8 XI 2023]. <https://doi.org/10.48550/arXiv.2307.11991>.

McGuffie K., Newhouse A., *The radicalization risks of GPT-3 and advanced neural language models*, preprint, arXiv, 15 IX 2020, <https://arxiv.org/abs/2009.06807> [accessed: 8 XI 2023]. <https://doi.org/10.48550/arXiv.2009.06807>.

NASK (@WeryfikacjaNASK), *Wraz z postępem technologicznym, rozwój AI staje się coraz bardziej widoczny w różnych dziedzinach naszego życia* (Eng. As technology advances, the development of AI is becoming more and more visible in various areas of our lives), X, 26 X 2023, <https://twitter.com/WeryfikacjaNASK/status/1717487918556594437> [accessed: 8 XI 2023].

Nowe oszustwo na WhatsAppie „Kurier Szczeciński” (Eng. New WhatsApp scam), 5 VIII 2023, <https://24kurier.pl/aktualnosci/wiadomosci/nowe-oszustwo-na-whatsappie/> [accessed: 8 XI 2023].

Podolak J. et al., *Analyzing the Influence of Language Model-Generated Responses in Mitigating Hate Speech on Social Media Directed at Ukrainian Refugees in Poland*, preprint, arXiv, 28 XI 2023, <https://arxiv.org/abs/2311.16905> [accessed: 30 XI 2023]. <https://doi.org/10.48550/arXiv.2311.16905>.

Saunders W. et al., *Self-critiquing models for assisting human evaluators*, preprint, arXiv, 12 VI 2022, <https://arxiv.org/abs/2206.05802> [accessed: 9 XI 2023]. <https://doi.org/10.48550/arXiv.2206.05802>.

Simmons A., Vasa R., *Garbage in, garbage out: Zero-shot detection of crime using Large Language Models*, preprint, arXiv, 4 VII 2023, <https://arxiv.org/abs/2307.06844> [accessed: 9 XI 2023]. <https://doi.org/10.48550/arXiv.2307.06844>.

Skąd Polacy czerpią informacje? Badanie IBRIS i IBIMS kwiecień 2021 (Eng. Where do Poles get their information from? IBRIS and IBIMS survey April 2021), IBiMS, http://www.ibims.pl/wp-content/uploads/2021/04/IBIMS_media_2021.pdf [accessed: 8 XI 2023].

Toulas B., *Cybercriminals train AI chatbots for phishing, malware attacks*, Bleeping Computer, 1 VIII 2023, <https://www.bleepingcomputer.com/news/security/cybercriminals-train-ai-chatbots-for-phishing-malware-attacks/> [accessed: 9 XI 2023].

Vallance C., Rahman-Jones I., *Urgent need for terrorism AI laws, warns think tank*, BBC News, 4 I 2024, <https://www.bbc.com/news/technology-67872767> [accessed: 10 I 2024].

Yin S. et al., *A Survey on Multimodal Large Language Models*, preprint, arXiv, 23 VI 2023, <https://arxiv.org/abs/2306.13549> [accessed: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2306.13549>.

Zou A. et al., *Universal and Transferable Adversarial Attacks on Aligned Language Models*, preprint, arXiv, 27 VII 2023, <https://arxiv.org/abs/2307.15043> [accessed: 8 IX 2023]. <https://doi.org/10.48550/arXiv.2307.15043>.

Julia Puczyńska

PhD student at IDEAS NCBR and at the Doctoral School of Information and Biomedical Technologies at the Institutes of the Polish Academy of Sciences. She is involved in combating disinformation and analyzing social media. A graduate in psychology and criminology, she has worked

on topics related to memory, facial recognition, and lie detection. She leads the Zgłoś Trolła (Eng. Report a Troll) project in cooperation with DC9 and the Geremek Foundation.

Contact: julia.puczynska@ideas-ncbr.pl

Marcin Podhajski

PhD Student in the "AI for Security" research team at IDEAS NCBR and in the Doctoral School of Information and Biomedical Technologies at the Institutes of the Polish Academy of Sciences. He specializes in artificial intelligence, machine learning, and social network analysis.

Karolina Wojtasik, PhD

Security specialist, academic researcher, and lecturer, forensic expert, Vice President for Scientific Affairs of the Polish National Security Association, employee of the Government Security Center. She deals with broadly understood security of critical infrastructure and objects subject to mandatory protection, especially in the context of physical and personal security threats. Author of books such as *Anatomia zamachu. O strategii i taktyce terrorystów* (Eng. Anatomy of an attack. On the Strategy and Tactics of Terrorists), *Ścieżki radykalizacji dżihadystycznej* (Eng. Paths of Jihadi Radicalization); co-author of the book *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku* (Eng. The Polish anti-terrorist system and the realities of the attacks of the second decade of the 21st century) and many other publications related to terrorism, security, and building the resilience of critical infrastructure. Creator of the popular science channel *Anatomia zamachu* (Eng. Anatomy of an attack) on YouTube and the Projekt IK portal.

Tomasz P. Michalak, PhD

Leader of an independent research team at IDEAS NCBR and lecturer at the Faculty of Mathematics, Informatics, and Mechanics of the University of Warsaw. Graduate of the Faculty of Economic Sciences at the University of Warsaw. During his academic career, he conducted research at the Department of Computer Science at the University of Oxford, the School of Engineering and Computer Science at the University of Southampton, the Department of Computer Science at the University of Liverpool, and the Faculty of Applied Economics at the University of Antwerp, where he obtained a PhD in economics.



REVIEW ARTICLES /
REVIEWS

Book review: Rafał Miętiewicz, Autonomous Systems in Maritime Operations¹

Jędrzej Łukasiewicz

The Department of Aeronautics, Faculty of Civil
and Transport Engineering
Poznań University of Technology

 <https://orcid.org/0000-0002-7082-8511>



The development of modern construction materials, miniaturisation of electronic components, and access to sources with high energy density per unit of their mass have enabled the rapid development of unmanned platforms. These platforms include unmanned aerial vehicles, wheeled and tracked unmanned vehicles, as well as boats on and below the surface of the water. The features of unmanned systems that determine their use in various areas of human activity are: no operator on board, the ability to place any cargo on them, the ability to perform the mission

¹ R. Miętiewicz, *Systemy autonomiczne w działaniach na morzu* (Eng. *Autonomous Systems in Maritime Operations*), Gdynia 2023, Polish Naval Academy of the Heroes of Westerplatte, 495 p. (the online English version is available at: https://www.academia.edu/104173920/AUTONOMOUS_SYSTEMS_IN_MARITIME_OPERATIONS - editor's note).

autonomously, automatically or under the manual control of the operator. The lower purchase price of such a system compared to an equivalent manned platform is also not insignificant.

The geopolitical situation in the Baltic Sea region and media reports about attacks on the Nord Stream infrastructure, which is an energy and fuel supply system and therefore a critical infrastructure, force special attention to be paid to this region, as it is of great importance for Poland's military and economic security.

In 2023, a comprehensive monograph of 495 pages was published by Commander, Rafał Miętkiewicz PhD, entitled *Autonomous Systems in Maritime Operations*. It is a unique publication because it is the first elaboration in Polish in which the role of modern maritime unmanned systems in maritime operations is described so extensively. So far, there has been a lack of a book on the publishing market referring to both the safety of the reservoir and the technology, including unmanned platforms, the use of which could increase the level of this safety.

The author of the monograph is an officer of the Polish Navy and a line officer with several years of experience on board naval mine warfare ships (he was among others the commander of ORP Śniardwy), as well as a scientist and academic lecturer, an assistant professor at the Naval Academy in Gdynia, as well as a member of the Polish National Security Association and the Polish Nautological Society, an expert of the Ignacy Łukasiewicz Institute for Energy Policy in Rzeszów, and in 2023, he was an external expert of the Interministerial Task Force on solutions for the destruction, immobilisation and taking control of an unmanned floating vehicle in the context of the security of critical infrastructure facilities located off the Baltic coast or outside the borders of the Republic of Poland (established at the Interministerial Team for Terrorist Threats).

His reviewed monograph is divided into five chapters, each of which ends with a summary.

The first chapter, entitled *Autonomous systems in the marine domain*, contains extensive characteristics of unmanned platforms. In it, the author divided these platforms according to their functional features, illustrating it with diagrams and tables, thanks to which it is easier to systematise knowledge. As these systems can perform missions at different levels of autonomy, different ways of dividing autonomy levels have been described, including the levels indicated by Lloyd's Register, International Maritime Organisation, Roadmap FY2011-2036 and Multinational

Capability Development Campaign. The following pages contain extremely interesting descriptions not only of autonomous surface and underwater systems, but also of flying systems, both civilian and military, with the author not limiting himself to systems already known and in use. Colourful illustrations enriching these characteristics are an added value. The chapter identifies technologies that have the potential for widespread use in the long term. The author included autonomous biomimetic systems and swarms, shoals or flocks of autonomous maritime platforms. Given that swarms, shoals or flocks of unmanned platforms are a technology whose research and development began relatively recently, analysing how they can be used to protect seaports and bases, as well as to attack enemy surface and submarine vessels, is of particular interest. According to available data, many countries around the world are working intensively on building autonomous unmanned systems.

The second chapter, entitled *The Baltic Sea as a basin for the use of maritime autonomous systems* is actually a small encyclopaedia of knowledge on the possibilities of using autonomous unmanned systems in the area concerned. The reader will find here information on Polish maritime areas, their division and size of area, supplemented by a clear map. In the next part of the chapter, the author describes the conditions affecting the operation of autonomous unmanned platforms in maritime conditions. He included: the number and location of Polish seaports together with the volume of cargo handled in them, infrastructure projects for the transfer of raw materials or the exploitation of natural resources through their extraction from the seabed, the construction of offshore wind farms together with the infrastructure for the transmission of electricity to shore, and the location of conventional ammunition and chemical weapons lying on the seabed. An important part is the characterisation of the environmental conditions of the Baltic Sea, including, inter alia, weather conditions affecting carrying out of unmanned platform missions. The chapter further includes an analysis of the impact of environmental factors on the operation of unmanned surface, air and underwater platforms.

The next chapter *Contemporary security threats in the maritime domain* is an in-depth analysis of threats occurring now, as well as those that may arise in the future. The author described in detail the impact of the aggressive policy of the Russian Federation, among others, on the security of Poland. He devoted a lot of space to the conflict in Ukraine

and how it affects the security architecture of Poland and the region in which Poland is geographically located. The analysis of threats in the area of maritime security is worth emphasising. The author has extensively discussed the various sources of these threats. He also analysed selected incidents that occurred in the Baltic Sea region. The chapter is enriched with situational maps, tables, photographs and diagrams.

The penultimate chapter *The tasks of the Polish Navy in the light of challenges and threats to security* is devoted to considerations concerning the tasks of the Polish Navy in the context of threats to the Polish state defined and described in the previous parts of the book. The current geopolitical situation of Poland, in a way, forces one to ask questions about the state of the Navy and its potential to defend the interests of the Republic. The author has attempted to answer these questions.

Until the start of the full-scale war in Ukraine, the navies of various countries made limited use of unmanned maritime platforms. Following its outbreak, autonomous naval platforms have increasingly been used to attack both enemy naval units and elements of their port and transport infrastructure. There have also been reports of multiple platforms being used simultaneously in a way that makes it possible to speak about a swarm, shoal or flock attack. For maritime professionals, this is an opportunity to draw lessons for national naval forces. Those responsible for Baltic Sea security should also keep a close eye on the developments in Ukraine. Based on its war experience, taking into account Poland's membership of NATO and considering Polish interests in the Baltic Sea area and technological developments, the concept of using autonomous unmanned maritime platforms should be proposed.

The final, fifth chapter, entitled *The concept of using maritime autonomous systems*, is devoted to this topic. According to the author of this review, this is the most important chapter. The concept proposed therein for the use of maritime autonomous systems in combating terrorist acts in the Polish economic zone should become the subject of in-depth analyses by the commanders of the Polish Armed Forces and counter-terrorist services and formations responsible for the security of the Polish state. However, in view of the dynamics of developments related to military operations in Ukraine, it should be assumed that the content of this chapter is only the beginning of considerations that will need to be made as more information on the use of autonomous unmanned systems in maritime operations emerges. Such considerations require an in-depth analysis

of the content included in the first four chapters of this monograph. In this sense, it constitutes a collection of information necessary for the management of maritime safety of the Republic of Poland, a kind of foundation on which the safety policy can be built.

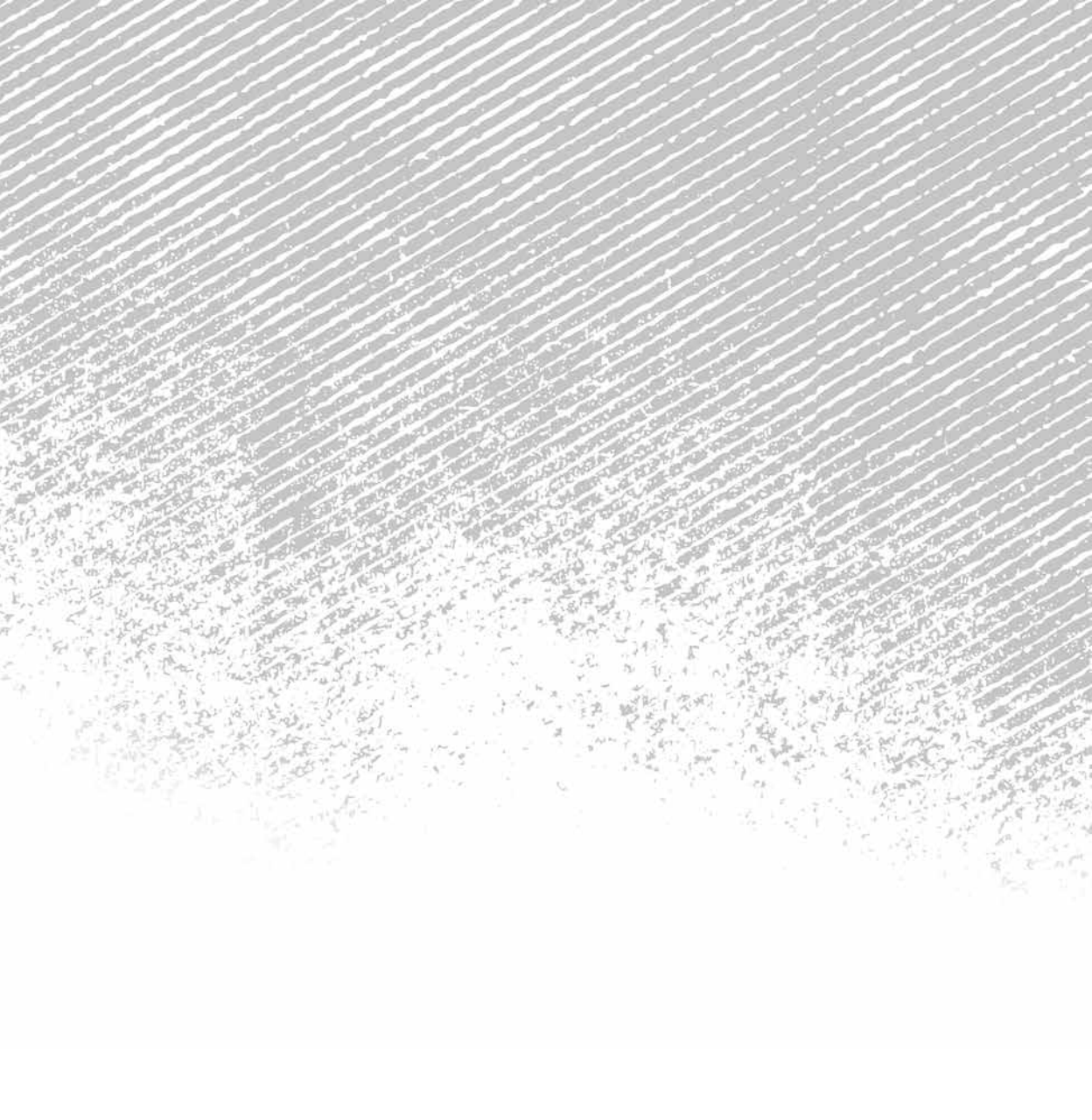
The knowledge contained in the publication *Autonomous Systems in Maritime Operations* is so extensive that a single reading of this book is not sufficient. An in-depth understanding of the issues described requires returning to selected passages. A great advantage is the fact that the publication includes not only the author's observations and conclusions, but also numerous references to other sources, both Polish and foreign, which allows the reader to verify the content and expand the knowledge base on the basis of other authors' works. Another advantage is the way in which the content is communicated - the book is written in a professional but readable language, while charts, tables, diagrams and photographs make it easier for the recipient to systematise the information. It can be read both by professionals involved in unmanned systems in maritime operations and by people who are just beginning their adventure with autonomous unmanned systems.

On the Polish and foreign publishing market, this is the best publication on the use of autonomous systems in maritime operations, with a particular focus on the Baltic Sea. Of course, one can read about the issues raised in the works of other authors, but in no publication have they been put together. When translated into English, Rafał Miętkiewicz's book can be successfully used to promote the Polish *raison d'état* within NATO working groups in the area of using autonomous systems to ensure the security of the Baltic Sea and the critical infrastructure located there.

Jędrzej Łukasiewicz, PhD

Assistant Professor at the Department of Aeronautics, Faculty of Civil and Transport Engineering, Poznań University of Technology, instructor of unmanned aircraft pilotage at the training centre of Poznań University of Technology. Participant in expert bodies at EU (DG MOVE, DG HOME), national and interministerial level on critical infrastructure security and building resistance to threats from unmanned aerial vehicles. Expert of the Government Security Centre on threats posed by unmanned aerial vehicles.

Contact: jedrzej.lukasiewicz@put.poznan.pl



VARIA

Building resilience of critical infrastructure in the light of asymmetric threats and terrorism

Legislative trends in the Polish implementation of the CER Directive
with particular reference to aspects of standardisation and certification
of organisational and technical solutions

Adam Tatarowski

The Technical Property Protection Development Institute TECHOM

 <https://orcid.org/0009-0007-5503-6819>

Sources and context of contemporary asymmetric threats and terrorism

In the 1930s. the Soviet Union, through the concepts of Georgii Isserson and Vladimir Triandafillov, set world standards in military thought. Isserson was the first to develop an innovative military doctrine based on the use of deep operations, i.e. striking at the full depth of the enemy's troops, across the entire front line¹. In the post-Stalin era, colonel Yevgeny Messner developed the concept of warfare by non-military means (so-called 'rebel wars')², describing the role of terror in the conduct of military operations, the use of civilians and specific social groups in the fighting, the creation

¹ Г.С. Иссерсон, *Эволюция оперативного искусства*, Москва 1937 (G.S. Isserson, *Evolyutsiya operativnogo iskusstva*, Moskva 1937).

² Е.Э. Месснер, *Хочешь Мира, Победи Мятажевойну!*, *Творческое наследие Е.Э. Месснера*, Москва 2005, (Ye.E. Messner, *Khochesh' Mira, Pobedi Myatezhevoynu!*, *Tvorcheskoye nasledie Ye.E. Messnera*, Moskva 2005), p. 110.

of paramilitary units in a situation where the differences between a state of war and a state of peace were reduced. These approaches are continuing by General Valery Gerasimov, Chief of General Staff of the Armed Forces of the Russian Federation. In 2013, in a paper widely reported in the media³, he outlined the assumptions of hybrid warfare, which were based on the synchronised use of military and non-military means by which it will be possible to achieve strategic and political objectives. Gerasimov discussed actions such as the introduction of a contingent of international peacekeepers under the pretext of defending human rights, political isolation, economic sanctions, blockades of land, sea and air communication routes, and threats to use force.

Since 2014, since the invasion of the so-called green men and the annexation of Crimea, all this can be observed in practice - war has been going on basically all the time and is not a continuation of politics, as Carl von Clausewitz wrote about, but an element of it⁴. The Russian aggression, which took full-scale form in February 2022, emphatically demonstrates that the evolution of asymmetric threats has greatly accelerated and is affecting not only the strictly military area, but also the entire security environment. Thus, the concept of asymmetric threats, succinctly described in *the NATO Glossary of Terms and Definitions* as those that result from the ability to use various means and methods to circumvent or neutralise an adversary's strengths and exploit its weaknesses to achieve disproportionate objectives⁵, should now be understood much more broadly - in civilisational, social, cultural and technological terms. Moreover, terrorism, the essence of which has always been to deliberately and consciously attack innocent bystanders or social groups with the intention of intimidating state authorities or society, has taken on a much fuzzier form. Collin Powell has rightly observed that while the civilised world has sought for hundreds of years to reduce the destructiveness of wars - through, for example, the civilian-soldier distinction - modern terrorism is increasingly blurring that distinction⁶. The totality of these threats is today becoming

³ В. Герасимов, *Ценность науки в предвидении*, „Военно-промышленный курьер” 2013, (B. Gerasimov, *Tsennost' nauki v predvidenii*, „Voyenno-promyshlennyy kur'yer” 2013), no. 8, pp. 2-3.

⁴ C. von Clausewitz, *On war*, Princeton University Press 1976.

⁵ AAP-6 *the NATO Glossary of Terms and Definitions*, 2021.

⁶ From: J.M. Fish, S.J. McCraw, Ch.J. Reddish, *Fighting in the gray zone: A strategy to close the preemption gap*, Strategic Studies Institute 2004, p. 6.

a challenge for those responsible for protecting critical infrastructure (hereafter: CI) and ensuring its resilience. This article describes legislative trends in this area, with a particular focus on the standardisation and certification aspects of organisational and technical solutions arising from the CER Directive.

Emerging risks in the context of asymmetric threats and contemporary terrorism - challenges in the legal and normative area

The COVID-19 pandemic has significantly accelerated the work started in 2018 on the new technical specification *ISO/TS 31050:2023 Risk management - Guidelines for managing an emerging risk to enhance resilience*, describing approaches to assessing and managing emerging risks that are difficult to predict and understand due to a lack of sufficient data and verified information. Their occurrence, from the perspective of an organisation, e.g. a critical entity⁷, can result from unexpected changes in the organisational domain, from technological or social developments, globalisation processes, political turmoil and, more broadly, from the rise of asymmetric threats and terrorism. These risks are characterised by a high degree of uncertainty and can lead to serious consequences in terms of resilience, security and continuity (in operational and business dimensions) of the organisation. Managing them requires continuous monitoring and information gathering as well as flexibility in decision-making.

The current concept of risk assessment in CI is based on the assumptions of the 'core' standard *PN-ISO 31000:2018-08 Risk management - guidelines* and is set in a complex legal and normative environment, in which an 'object-oriented' approach to the emergence of CI entities continues to function. According to the National Critical Infrastructure Protection Programme (NCIPP)⁸, this emergence takes place in three stages. The first establishes to which system (according to the NCIPP - e.g. communications,

⁷ Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Official Journal of the UE L 333/164 of 27 XII 2022).

⁸ The National Critical Infrastructure Protection Programme 2023, <https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej> [accessed: 29 XI 2023].

health care, ICT networks) the potential CI facility (also: facility, installation or service) belongs and compares its characteristics with the criteria of the respective system (these criteria are classified), the second verifies whether the facility plays the role referred to in the statutory definition⁹, and then analyses whether the possible consequences of the destruction or discontinuation of the potential CI will meet at least two cross-cutting criteria relating to the social impact of the destruction or discontinuation of the facility, equipment, installation or service. These criteria include:

- casualties,
- financial implications,
- need to evacuate,
- loss of service,
- recovery time,
- international effect,
- uniqueness (in the sense of the impossibility of replacing and reconstructing the damaged facility, equipment or installation).

Although the ‘object-oriented’ approach is paralleled by a ‘service-oriented’ system of selecting operators of essential services within the meaning of the Act on the National Cyber Security System¹⁰, the scope of this regulation is limited, as it applies only to the services included in this Act and only to those relating to information systems. A decision recognising an entity as essential service operator is issued if:

- entity provides essential service,
- the provision of this service depends on information systems,
- incident would have a significant effect resulting in disruption to the provision of essential service by that operator.

This duality, due to the requirements of the Critical Entities Resilience Directive (CER Directive), will soon disappear. In October 2024, national legislation implementing this directive, introducing a ‘service’ model for the designation of CI entities, is expected to be enacted. The CER Directive introduces a mechanism for state interventionism. In accordance with its provisions, EU Member States become co-responsible for maintaining the availability of essential service and will have the possibility to directly subsidise business entities providing such services. Member states will

⁹ The Act of 26 April 2007 on Crisis Management (Journal of Laws 2023, item 122).

¹⁰ The Act of 5 July 2018 on the National Cybersecurity System (Journal of Laws 2023, item 913, as amended).

designate essential services, identify operators and enforce the level of service availability. This is a definite change of approach not only in the citizen-state relationship, but also in the business-state relationship. There are therefore major challenges ahead for CI. The critical entity will be required to carry out its own risk assessment, based on *PN-ISO 31000:2018-08 Risk management - guidelines*, but taking into account the broadest possible spectrum of risk factors, including those that are considered *emerging risks*.

Risk assessment in critical infrastructure - new approaches

CI operators use different safety management methodologies, depending on their awareness, level of knowledge and understanding of the area they are dealing with. Each recognised methodology is based on a template, which is the standard *PN-ISO 31000:2018-08 Risk management - guidelines*. This standard involves the implementation of the risk management process in three steps:

- 1) establishing the context,
- 2) risk assessment (threat identification, risk analysis and estimation),
- 3) a decision to deal with the risk.

Most of the security management methodologies used in Poland and in countries that are recognised as leaders in this area (e.g. Germany, Sweden, Canada, USA, Ireland, the Netherlands or Australia) are based on this standard. The authors of the publication *Managing Critical Infrastructure Security and the Continuity of Essential State Services*¹¹ extensively analyse the approaches to risk assessment and management used in these countries and present the Situational Management of Safety Critical Infrastructure (SMSCI) methodology together with the Integral Model for the Security of Critical Infrastructure (IMSCI), which in turn is the tool base of the SMSCI methodology. The stages of this management are:

- establishment of a team,
- definition of safety thresholds,
- mapping of CI characteristics,
- generation of adverse event scenarios,

¹¹ M. Kisilowski et al., *Zarządzanie bezpieczeństwem infrastruktury krytycznej i ciągłością usług kluczowych państwa* (Eng. *Managing Critical Infrastructure Security and the Continuity of Essential State Service*), Warszawa 2021.

- formulation of the decision problem,
- risk estimation,
- implementation of safeguards.

In an era of increasing asymmetric threats, including those related to terrorist activities, a valuable supplement (and, above all, help and support) when carrying out risk assessment – within the framework of e.g. the SMSCI methodology – by critical entities are standards or technical specifications, such as:

- *PN-EN IEC 31010:2020-01 Risk management – Risk assessment techniques,*
- *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience,*
- *ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management.*

The critical entity's ability to anticipate, prepare for and respond to different circumstances should be the most important requirement for effective risk management. The critical entity should¹², among other things:

- optimise communication inside and outside the organisation,
- establish an effective way of gathering up-to-date information on emerging risks,
- counteract disinformation,
- develop a way for those responsible for risk management to influence management,
- build trust within the organisation and with collaborators, including government,
- encourage and empower relevant people in the organisation to report what they consider to be significant signals related to the potential occurrence of new risks.

The risk identification process requires the critical entity to be aware of the dynamic changes taking place in the environment in which it operates. Despite the implementation of a risk identification structure (based on the above-mentioned standards or other documents, e.g. relating to terrorist threats¹³), it should also use non-standardised, unstructured

¹² *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience.*

¹³ Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on the combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (Official Journal of the UE L 88/6 of 31 III 2017).

identification methods, as this will provide a more complementary approach to the problem and increase the effectiveness of identification. According to the *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience*, the organisation should, among other things:

- regularly, comprehensively and from multiple perspectives analyse the environment in which it operates, or use appropriate methods or techniques to identify emerging changes that may give rise to *emerging risks*,
- analyse trends and circumstances that may lead to *emerging risks*,
- analyse sources of risk and possible scenarios of events,
- update descriptions of possible risks on a continuous basis.

Examples of changing circumstances that can be sources of *emerging risks*:

- natural hazards, e.g. climate, weather,
- risks from new bacteria, viruses, fungi and parasites, or from these micro-organisms becoming resistant to available drugs,
- challenges related to the uncontrolled development of the internet of things (IoT),
- challenges related to the development of artificial intelligence.

The latter are an increasingly topical problem and, in the opinion of the author of this article, will soon become a major generator of *emerging risks*. For the first time in human history, devices and systems are being designed whose operation is not fully understood. It is not clear, for example, how Chat GPT works. The developers of this tool understand machine learning algorithms, but how neural networks work (and they have a very fast pace of development) has not been understood exactly. It is also unclear to what extent artificial intelligence will become autonomous, and the delegation of decision-making capabilities to machines, the lack of transparency and understanding of the functioning of artificial intelligence as well as the lack of human oversight may result in previously unknown risks.

Emerging risks may also involve terrorist threats in a broad sense - not just those implied by the definitions in *the NATO Glossary of Terms and Definitions* and the European Parliament's 2017 Counter-Terrorism Directive cited earlier. It must be assumed that the new reality modelled by *emerging risks* will have an impact on the way terrorist crimes are prepared and executed.

In general, the results of a systematic risk assessment by critical entities should include:

- a list of suppliers (resources, services) critical to the critical entity,
- a list of processes whose disruption may cause a critical incident,
- a list of CI necessary to maintain the essential service.

The risk assessment will be the starting point for developing and implementing adequate organisational and technical solutions.

Standardisation and certification of adequate organisational and technical solutions under the CER Directive

Outline of the CI protection regime in the light of the NCIPP 2023 and the CER Directive

Within the framework of the NCIPP, there is a so-called six-pack describing the CI security system. The measures taken to ensure the security of CI include:

- 1) ensuring physical security - a set of organisational and technical actions aimed at minimising the risk of disrupting CI operations as a result of actions of persons who have attempted to enter or have entered CI in an unauthorised manner;
- 2) ensuring technical security - a set of organisational and technical measures aimed at minimising the risk of disrupting the functioning of CI as a consequence of disrupting the technological processes in progress;
- 3) ensuring personal security - a set of organisational and technical activities aiming at minimising the risk of disrupting CI operations as a result of actions of persons who have authorised access to critical infrastructure;
- 4) ensuring ICT security - a set of organisational and technical measures aimed at minimising the risk of disrupting CI operations as a result of unauthorised interference with control apparatus and ICT systems and networks;
- 5) legal assurance - a set of organisational and technical measures aimed at minimising the risk of disrupting CI operations as a result of legal actions of external entities;

- 6) business continuity and restoration plans, understood as a set of organisational and technical actions leading to the maintenance and restoration of the functions performed by CI¹⁴.

This system corresponds to Article 13 of the CER Directive *Resilience measures of critical entities*. The first paragraph of this article reads:

1. Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:
 - a) prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;
 - b) ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access control;
 - c) respond to, resist and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;
 - d) recover from incidents, duly considering business continuity measures and the identification of alternative supply chains, in order to resume the provision of the essential service;
 - e) ensure adequate employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, setting up procedures for background checks in accordance with Article 14 and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications;
 - f) raise awareness about the measures referred to in points a) to e) among relevant personnel, duly considering training courses, information materials and exercises.

For the purposes of the first subparagraph, point e), Member States shall ensure that critical entities take into account the personnel of external service providers when setting out categories of personnel who exercise critical functions.

¹⁴ The National Critical Infrastructure Protection Programme 2023...

The CER Directive, which is the standard in European legislation, allows Member States to regulate on a case-by-case basis the provisions of national law implementing its provisions in such a way that the level of resilience of critical entities is as high as possible and compatible with national specificities, but taking into account the use of standards, as referred to in Article 16 of the Directive.

A standard is a normative document adopted by a recognised standardisation body. In Poland this is the Polish Committee for Standardisation. A standard establishes principles, guidelines or characteristics for different activities and their results, is approved by consensus, is intended for widespread and repeated use, is accepted by all interested parties as a benefit to all, and introduces a code of good practice and principles of rational conduct at the current level of technology¹⁵.

The use of standards in the standardisation and subsequent certification of organisational and technical solutions is the right step in building the resilience of CI to all types of threats. It facilitates the selection of solutions, their maintenance and validation, and allows for effective oversight and enforcement, as the national authority overseeing CI - in accordance with Article 21 of the CER Directive - will inspect and make decisions based on data collected by external competent auditing and certification entities.

The range of organisational and technical solutions that should be applied to a critical entity following a risk assessment is very broad. In order to present synthetically the issue of standardisation and certification, the author of the article referred to technical measures to ensure physical security, which are a good point of reference for this topic, as well as to ensure business continuity of essential services.

Standardisation and auditing - the context of standardisation

According to the concept presented by the author of this article on 5 October 2023 at *the National Forum for Critical Infrastructure Protection*¹⁶, organisational and technical solutions implemented by critical entities should be created in accordance with standards, which makes it possible -

¹⁵ Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation (Official Journal of the UE L 316/12 of 14 XI 2012).

¹⁶ A. Tatarowski, *Standardisation and Certification of CER Directive Solutions*, 10th National Forum for Critical Infrastructure Protection, Warszawa 2023, <https://www.gov.pl/web/rcb/x-krajowe-forum-ochrony-infrastruktury-krytycznej-za-nami>.

due to the availability of legal and business solutions - to conduct audits and certifications effectively. An audit is (...) *a systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which audit criteria are met*¹⁷. An audit assesses compliance now and in the past, may have a legal and normative purpose and should meet business needs. It is based on seven principles:

- 1) reliability as a basis for professionalism,
- 2) honesty in the presentation of results,
- 3) professional due diligence,
- 4) confidentiality,
- 5) independence,
- 6) an evidence-based approach,
- 7) a risk-based approach.

There are three types of audits (Table 1).

Table 1. Types of audit according to the standard PN-EN ISO 19011:2018.

1 ST party audit	2 ND party audit	3 RD party audit
Internal audit	External provide audit	Certification and/or accreditation audit
	Other external interested party audit	Statutory, regulatory and similar audit

Source: *PN-EN ISO 19011:2018 Guidelines for auditing management systems.*

From the perspective of critical entities, the most relevant is the third-party audit, which is carried out by independent auditing organisations, such as certification bodies or government institutions. The government institution overseeing critical entities in Poland (in the legal conditions that will follow the implementation of the CER Directive) will collect data and make decisions on the basis of (...) *evidence of the effective implementation of these measures* [i.e. Article 13 measures, discussed as organisational and technical solutions], *including the results of an audit conducted at the entity's expense by an independent and qualified auditor selected by the entity*. Evidence in a third-party audit is to be understood as certificates, i.e. documents issued by a conformity assessment body (certification body), confirming

¹⁷ *PN-EN ISO 19011:2018 Guidelines for auditing management systems.*

that a product/installation/system/process/service complies with the requirements. In the case of the implementation of the CER Directive, compliant with the requirements contained in the relevant standards.

As an aside, it is worth clarifying one of the aspects that the author of this article encounters in his professional activity as the head of a certification body. Conformity assessment always refers to a document, in this case a standard. Referring to standards in legal regulations, even though they are documents for so-called voluntary application, is possible, which is confirmed by the position of the President of the Polish Committee for Standardisation¹⁸ and by court judgements¹⁹. Thus, if a standard is referred to in the provisions of a law, then referring to it (e.g. in the case of an audit or certification) is possible and justified. Such practice is present in Polish legislation, e.g. in the Act on the National Cybersecurity System. However, the citation of standards in the legislation does not facilitate insight into them. Access to these standards is chargeable.

Conformity assessment. Competence of certification bodies and auditors to carry out certification. Certificate versus declaration of conformity

A third party audit may be conducted by a conformity assessment body (certification body) accredited under the provisions of the Act on Conformity Assessment and Market Surveillance Systems²⁰ - and such a solution already exists with regard to security auditing of an information system used to provide essential service²¹ - or by a certification body authorised to certify on behalf and for the benefit of the Polish Committee for Standardisation within the meaning of the provisions of the Act on Standardisation²². Certification should be understood as the action of a conformity assessment body (certification body) demonstrating that a product/installation/system/process/service complies with

¹⁸ *Voluntary application of standards*, the Polish Committee for Standardisation, <https://wiedza.pkn.pl/web/wiedza-normalizacyjna/stanowisko-pkn-w-sprawie-dobrowolnosci-pn> [accessed: 29 XI 2023].

¹⁹ Judgement of the Supreme Court of 10 April 2019, II OSK 1486/17; Judgement of the Voivodeship Administrative Court in Kielce of 19 May 2009, II SA/Ke 183/09.

²⁰ The Act of 13 April 2016 on Conformity Assessment Systems and Market Surveillance (Journal of Laws of 2022, item 1854).

²¹ The Act on the National Cybersecurity System ("ANCS") - (Journal of Laws 2023, item 913, as amended).

²² The Standardisation Act of 12 September 2002 (Journal of Laws of 2015, item 1483).

the requirements. The empowerment of certification bodies is very strong. They function as components of an overall European system encompassing conformity assessment and market surveillance²³ and their use in auditing and certifying organisational and technical solutions implemented by critical entities will become essential.

It is worth noting that the term ‘certificate’ is often used in an unauthorised way (from the perspective of the conformity assessment system). According to a dictionary definition, a certificate is ‘an official document stating, for example, the conformity of a product with standards, the authenticity of a work of art or the completion of a course’²⁴. The Council for the Polish Language at the Presidium of the Polish Academy of Sciences has also taken a position on the concept of a certificate²⁵. In the context of the conformity assessment system - the conformity that will be decisive in the case of CI - a certificate is therefore, as already mentioned, a document issued by a conformity assessment body (certification body), confirming that a product/installation/system/process/service complies with the requirements.

This is an authorial definition, as this concept in relation to conformity assessment with non-harmonised standards has never been defined. There is no such definition in the provisions on standardisation - both in the Act in question and in the Regulation of the Council of Ministers on the method of granting and using the mark of conformity with the Polish Standard²⁶, which even indicates the template of the certificate. Moreover, there is no definition of a certificate (in the terms indicated by the author of the article) in the Act on Conformity Assessment and Market Surveillance Systems. It only defines a certificate as an attestation of conformity issued by a notified body, i.e. one that has been notified to the European Commission and is on the list of bodies notified for specific directives and therefore

²³ Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Official Journal of the UE L 218/30 of 13 VIII 2008).

²⁴ *Polish Language Dictionary PWN*, <https://sjp.pwn.pl/sjp/certyfikat;2553201.html> [accessed: 29 XI 2023].

²⁵ *Position of The Council on the use of the word certificate*, <https://rjp.pan.pl/dokumenty-rad-y?view=article&id=98:stanowisko-rady-wobec-ucyia-sowa-certyfikat&catid=45> [accessed: 29 XI 2023].

²⁶ Regulation of the Council of Ministers on the method of granting and using the mark of conformity with the Polish Standard (Journal of Laws of 2010, no. 198, item 1316).

carrying out a mandatory conformity assessment. Given the needs arising from the CER Directive, a clarification of the concept of certificate in national legislation is expected.

The declaration of conformity is defined in the Act on Conformity Assessment and Market Surveillance Systems. This declaration is to be understood as a statement by the manufacturer, installer or their authorised representative or private importer (under their sole responsibility) that the product complies with the requirements.

What attitude to the importance of such a declaration could be observed in practice? A good, model example of an industry in which, for years, there has been a small but powerful lobby promoting the idea that a declaration of conformity is sufficient and guarantees compliance with requirements and quality is the industry of technical physical security measures. Nowadays, such voices have almost disappeared - due to a completely different awareness of market participants and government representatives, which has been altered by negative experiences. Below are some examples illustrating how the market has operated - and in some areas still operates. On 7 September 2010, the ordinance was published by the Minister of Internal Affairs and Administration on the requirements to be met for the protection of monetary values stored and transported by entrepreneurs and other organisational units²⁷. In § 12 of this regulation, there is a point stating that for the storage or transport of monetary values, equipment shall be used (...) *with a certificate of conformity issued by an authorised certification body or a declaration of conformity issued by the manufacturer or importer, attesting compliance with the essential or specific requirements within the meaning of the provisions on the conformity assessment system, where such requirements have been established for the product*. These provisions are still valid. Intuitively, it is known that if an equipment supplier has the opportunity to market a device that has a declaration of conformity that he himself issues, which most often has no factual basis, he will not carry out tests in an accredited laboratory and seek certification. The investor has no scope for action in this case. A more recent example is the 2012 Waste Act²⁸. The waste holder is obliged to maintain a visual control system for the storage or disposal site. The implementing act of this

²⁷ Ordinance of the Minister of the Interior and Administration of 7 September 2010 on the requirements to be met for the protection of monetary values stored and transported by entrepreneurs and other organisational units (Journal of Laws of 2016, item 793).

²⁸ The Waste Act of 14 December 2012 (Journal of Laws of 2023, item 1587, as amended).

law²⁹ specifies that: *The parameters of the technical equipment of the control system shall meet at least the requirements of the PN-EN 62676-4: 2015-06 Video surveillance systems for use in security applications - Part 4: Guidelines for use or a standard to replace the standard in question.* Unfortunately, most waste holders (perhaps even none) do not have such a system in place. Why is this the case? Leaving aside the less than ideal wording of this provision, it lacks any indication of how to confirm compliance that an installed CCTV system meets the requirements. The designer therefore bears no risk if he designs such a system without even knowing the referenced standard (the phenomenon of low levels of competence is common in the industry, but there are legal and normative solutions that are already beginning to work, as will be described later in this article), nor does the installer who installs such a system and issues a declaration of its compliance with the standard. Such systems, if they work at all, often fail to meet the needs of the investor and the requirements of the standards, and are, of course, unreliable. This is how a large area of the market operates.

In the case of CI, which - according to the CER Directive - must develop resistance to asymmetric threats, terrorist acts and other threats, such an approach is unacceptable. The technical security system (intrusion detection system, video surveillance system, access control system) should be certified after installation. Services provided by external entities (i.e. design, installation, maintenance) to CI should meet the highest quality standards. These entities should be certified to the standard *PN-EN 16763:2017 Services for fire safety and security systems*, which fulfils the requirements of Article 13(1)(e) of the CER Directive. This directive addresses the need to sort out the requirements for service providers (including in the area of fire protection), as the author of this article has repeatedly stated at various industry events and conferences³⁰.

²⁹ Ordinance of the Minister of the Environment on a visual inspection system for the place of waste storage or disposal (Journal of Laws of 2019, item 1755).

³⁰ A. Tatarowski, *Nowe sposoby walidacji jakości usług projektantów, instalatorów i konserwatorów systemów ochrony przeciwpożarowej i systemów zabezpieczeń technicznych w procesie budowlanym*, IV Międzynarodowa Konferencja N-T "Problemy Inżynierii Bezpieczeństwa Obiektów Antropogenicznych" (Eng. New ways to validate the quality of services of designers, installers and maintainers of fire protection and technical security systems in the construction process, 4th International Conference "Problems of Safety Engineering of Anthropogenic Facilities"), Warszawa 2021, <https://psribs.pl/conferences/iv-miedzynarodowa-konferencja-n-t-problemy-inzynierii-bezpieczenstwa-obiektow-antropogenicznych-wiosna-2021/> [accessed: 29 XI 2023]; A. Tatarowski, *Nowe*

The aforementioned standard has already been cited as relevant for assessing the competence and qualification of operators in this industry in Annex 1 *Standards for ensuring the efficient functioning of critical infrastructure - good practices and recommendations* to the NCIPP 2023.

Implementation, maintenance and certification of essential service business continuity management system

A critical entity that has carried out a risk assessment and is implementing (or has implemented) adequate organisational and technical measures should implement essential service continuity management system in accordance with the standard *PN-EN ISO 22301:2019 Security and resilience. Business continuity management systems. Requirements*. A business continuity management system based on the aforementioned standard consists of the following elements:

- a) a policy,
- b) competent people with defined responsibilities,
- c) management processes relating to:
 - 1) policy,
 - 2) planning,
 - 3) implementation and operation,
 - 4) performance assessment,
 - 5) management review,
 - 6) continual improvement,
- d) documented information supporting operational control and enabling performance evaluation.

Essential services are usually not provided by a single operator - it is most often a collection of several services that operate independently of each other and are provided by different operators. A good example of essential service - as the authors of the publication *Managing Critical Infrastructure Security and Continuity of State Essential Services* point out - is withdrawing money from an ATM. In order to be able to withdraw cash, the component services must be available in the form of:

sposoby walidacji jakości usług projektantów, instalatorów i konserwatorów systemów ochrony przeciwpożarowej, XXIX Ogólnopolskie Warsztaty – Sygnalizacja i Automatyka Pożarowa SAP '2023, Żnin 2023 (Eng. New ways to validate the service quality of designers, installers and maintainers of fire protection systems, 29th All-Poland Workshop - Fire Signalling and Automation SAP '2023, Żnin 2023), <https://www.polon-alfa.pl/pl/aktualnosci/polon-alfa-w-cukrowni-%C5%BCnin> [accessed: 29 XI 2023].

- 1) availability of power supply to the ATM,
- 2) availability of the Internet network providing connectivity to the billing system,
- 3) availability of the billing system of the bank from which the money is withdrawn,
- 4) the provision of cash at the ATM, which is currently mainly the responsibility of ATM network operators.

Thus (...) *the possibility of withdrawing money from an ATM is in fact a set of relations that exist between the said component services and can only occur as a result of the simultaneous availability of all component services. Consequently, the unavailability of one of the component services of essential service is sufficient for it also to be unavailable*³¹.

Given the complexity of essential services, the use of IM-SCI supplemented by standards may be helpful. Several ways to ensure uninterrupted access to the service have been described in the literature. These include:

- structural redundancy, which involves the duplication of elements deemed critical,
- functional redundancy, which consists in adapting selected elements of the system to perform additional functions,
- parametric redundancy, which consists in standardising the system to a degree that exceeds ensuring its usefulness³².

It is worth noting the way called functional redundancy. Using IM-SCI:

(...) a governmental institution, e.g. the Government Centre for Security, can, using the list of essential services, identify the entities that provide the constituent services for the essential services. The constituent services can then be treated as functionalities of the CI facilities under consideration. In the event of an incident limiting

³¹ M. Kisilowski et al., *Zarządzanie bezpieczeństwem infrastruktury krytycznej...*, p. 106.

³² K. Szwarz, *Modelowanie ciągłości działania systemów zarządzania kryzysowego i ocena przydatności rozwiązań na szczeblu lokalnym*, rozprawa doktorska (Eng. Modelling business continuity of crisis management systems and assessing the usability of solutions at local level, PhD thesis), Warszawa 2019, <https://repo.bg.wat.edu.pl/info/phd/WATefc9a9340f3e47cb8141566cdf6e0e53/Record+details+%25E2%2580%2593+Modeling+of+the+continuity+of+crisis+management+systems+and+the+assessment+of+suitability+at+the+local+level+%25E2%2580%2593+Military+Technical+Academy+them.+Jaroslaw+Dabrowski+title?aq=%40status%3Apracownik%2Cauthorprofile%2F%40positionPL%21%3Aadiunkt%2Cauthorprofile%2F%40positionPL%21%3Aprofesor%2C%40active%3D%27true%27%2C.%3AWUT84b1c97cce2d442fab1acd-c256a5d487&r=author&ps=20&lang=en&pn=1&cid=157628>.

or eliminating the availability of CI functionality, it is possible to identify CI facilities with similar functionality and, as part of the BCP (i.e. Business Continuity Plan), complement the missing component essential service with functionality provided by another CI facility³³.

The issue of developing, implementing and certifying a business continuity management system is vast and unique to each critical entity. The quoted excerpts taken from the literature are intended - by the author of this article - to encourage readers to expand their knowledge in this area, as this issue is the most relevant part in the overall view of the CI security management system.

In summary, from the perspective of the critical entity, an important activity will be the continuous improvement of the business continuity system through the use of effectiveness measurement, including simulation, monitoring, systematic review, incident assessment and effective removal in accordance with the security policy. One of the measurement tools will be to conduct systematic and independent audits, including those culminating in certification, but to the extent necessary to maintain the provision of the essential service.

Summary

The year 2024 will be a breakthrough year for CI. The pressing deadlines, obliging member states to enact national legislation implementing the CER Directive, require the preparation of an appropriate environment for effective legislative work. The Government Centre for Security, which for many years has been creating conditions conducive to improving the security of CI and has built an approach to security management in the sector that is unique in the EU, based on the aforementioned so-called 'six-pack', is now facing a major challenge in developing the implementation of the CER Directive in Poland. This article presents the legislative trends related to this implementation in terms of standardisation and certification of organisational and technical solutions. Standardisation and certification of these solutions based on standards will allow for the replacement of direct control by government, enable faster, more effective and optimal

³³ M. Kisilowski et al., *Zarządzanie bezpieczeństwem...*, p. 108.

adaptation of the resilience of critical entities to asymmetric, terrorist and those arising from or involving emerging risks.

In 2024, hybrid activities originating in the East, but also in other regions of the world, are expected to intensify. This makes the need for legislative regularisation not only in relation to CI, but also in the broader legal area, including: *the Act of 22 August 1997 on the Protection of Persons and Property, the Act of 26 April 2007 on Crisis Management, the Act of 10 June 2016 on Anti-Terrorist Activities and the Act of 11 March 2022 on the Defence of the Homeland.*

Adam Tatarowski

Director of the Technical Property Protection Development Institute TECHOM - a specialised certification body and a continuing education institution. It trains, among others, functionaries involved in the protection of persons and objects in the uniformed services, CI employees responsible for security and service providers carrying out projects, installations and maintenance of fire protection systems and technical means of ensuring physical security. The author is a specialist in assessment of compliance of technical means ensuring physical security (and services in this area), an expert of Technical Committees no. 52, 264, 306 and 323 of the Polish Committee for Standardisation.

Contact: tatarowski@techom.com

APPRAISE project

Building a security system for public spaces

Jarosław Przyjemczak

The Faculty of Law and Administration
of University of Business and Administration in Gdynia

 <https://orcid.org/0000-0003-3923-8078>

Nina Czyżewska

The Polish Platform for Homeland Security

 <https://orcid.org/0009-0004-0483-7577>

Open access public space, encompassing various areas and facilities, remains, especially in the case of large urban areas, a relatively free operating area for criminals, including those planning terrorist attacks. Their activity is encouraged by a number of factors, including the high accessibility of this type of space, the multiplicity and diversity of people in it, the variability of circumstances and the randomness of events and situations that may occur.

Work to develop an appropriate surveillance system for areas and facilities in public spaces has been ongoing for many years. It is assumed that such a system should not be easily noticeable and should not cause inconvenience to people in the area. Despite many efforts, it has not been possible to create a perfect instrument that, on the one hand, can effectively prevent the actions of criminals and, on the other hand, is indifferent to other participants. Past incidents such as attacks on shopping centres

(e.g. Munich, 2016), airports (e.g. Brussels, 2016), the public transport system (e.g. Madrid, 2004; London, 2005; Brussels, 2016), city squares and streets (e.g. Paris, 2015; Berlin, 2016; Nice, 2016; Stockholm, 2017) and performance halls (e.g. Paris, 2015; Manchester, 2017), highlighted the vulnerability of soft targets to attacks, and made entities responsible for security aware of the efforts that need to be made to protect such facilities¹.

One of the activities aimed at the rapid identification and implementation of appropriate countermeasures to prevent an attack from taking place or to stop it from spreading is the European Commission's APPRAISE² project. Its basic idea is to ensure security in public spaces without necessarily restricting the freedom of citizens by reducing or completely eliminating the threat of attacks.

Through the APPRAISE project, entirely new solutions are to be implemented to more effectively anticipate and identify criminal and terrorist acts and to strengthen operational cooperation between security entities - before, during and after an attack³. Based on the achievements of modern technologies, which allow the increasing use of tools such as artificial intelligence, advanced visualisation or the speed of information transmission, it is possible to significantly increase the level of security, also in public areas. The rapid detection of threats and the real-time transmission of information about abnormal or dangerous situations is of the utmost importance for uniformed or intervention services, as time is the main determinant of properly dealing with threats. The APPRAISE project, which is coming to an end as part of the development of a common anti-threat system for European Union countries, including related

¹ N. Czyżewska, J. Przyjemczak, *Wsparcie technologiczne nowoczesnych systemów bezpieczeństwa – projekt Komisji Europejskiej APPRAISE* (Eng. Technological support for modern security systems – European Commission's project APPRAISE), in: W. Zubrzycki, J. Przyjemczak, *Bezpieczeństwo w praktyce. Zagrożenia, podmioty bezpieczeństwa, działania pomocowe i ratownicze* (Eng. Safety in practice. Threats, security actors, relief and rescue operations), Kraków 2023 (in print).

² The project is about perspective of H2020 SU-FCT03-2018-2019-2020: *Zarządzanie przepływem informacji i danych w celu zwalczania cyberprzestępczości i terroryzmu* (Eng. Managing the flow of information and data to combat cybercrime and terrorism).

³ APPRAISE – *facilitating private and public security operators to combat terrorism scenarios against soft targets*, <https://ppbw.pl/pl/projekt-appraise/> [accessed: 10 XI 2023].

projects such as: Safe-Cities⁴, Lago⁵, S4AllCities⁶, Starlight⁷, Aida⁸, provides new solutions in the security sphere. The aim of all the above-mentioned projects is to achieve the ability to anticipate and deal with threats in the event of their occurrence, as well as the systemic implementation of unified procedures and standards in the operation of public and non-public entities at the time of terrorist events.

During the APPRAISE project, a number of initiatives were taken to adapt existing or develop new technologies, and the results were tested under near-real conditions. As part of the tests, study visits and so-called pilots were carried out (in Ljubljana, Bilbao, Gdańsk and Turin) to check the correct functioning of individual systems and technologies and to continuously improve them. The end of this project does not mean the end of the development.

On the contrary, it is only the beginning of building a unified, compact warning and analysis system, the task of which is to supervise public spaces and alert the competent intervention services in the event of the emergence of a threat or the detection of anomalies in people's behaviour. The overarching goal is to achieve the highest possible degree of situational awareness building in the crisis management process.

Attack on the Atlantis water park – pilot 3

For the first time, the teams working on developing the appropriate tools and technologies for the APPRAISE project met on 11 May 2023 in Slovenia. Pilot 3 took place at the Atlantis Water City located at the BTC City shopping complex in Ljubljana and was combined with the annual exercise of the Slovenian police in which local partners participated, together with the national police, the Slovenian SWAT team, stakeholders

⁴ *Project in a Nutshell*, <https://safe-cities.eu/> [accessed: 10 XI 2023].

⁵ *LAGO: Lessen Data Access and Governance Obstacles*, <https://lago-europe.eu/> [accessed: 10 XI 2023].

⁶ *Smart Spaces Safety and Security for All Cities*, <https://www.s4allcities.eu/> [accessed: 10 XI 2023].

⁷ *STARLIGHT. Enhancing the EU's strategic autonomy in the field of artificial intelligence (AI) for law enforcement agencies (LEAs)*, <https://www.starlight-h2020.eu/> [accessed: 10 XI 2023].

⁸ *AIDA project. Research project to develop a Big Data Analysis and Analytics framework*, <https://www.project-aida.eu/> [accessed: 10 XI 2023].

and APPRAISE partners. The leadership role was played by the Institut za korporativne varnostne študije (Institute for Corporate Security Studies), which prepared the exercise in cooperation with the Slovenian Ministry of the Interior, the BTC City shopping complex and its security agency⁹. The initial stage of the pilot scenario involved the analysis of content posted on social media and the Darknet. On this basis, threatening posts directed at the managers of the Atlantis complex were detected. APPRAISE computer programmes also helped detect an attempted cyber-attack on the water park's security systems to increase the amount of chlorine in the water, as well as an attack on the facility's monitoring system to disrupt the transmission of its recordings. The scenario also included a firearms attack on people in the water park. In the first phase of the attack, the perpetrator fired several shots in the outdoor pool area. This triggered the APPRAISE technology, which identified suspicious sounds and located the place of the attack. Monitoring analysis detected panic among those in the pool area and injured people lying on the ground. In the next phase of the scenario, the shooter moved inside the pool complex, where he fired further shots. Re-applied technologies used to recognise sound, identify objects from audiovisual recordings (in this case the handgun) and analyse crowd behaviour worked correctly and alerted to the threat. The adopted scenario also included the taking of a hostage with whom the perpetrator had locked himself in the basement, as well as police negotiations and the neutralisation of the terrorist¹⁰. A report from the exercise is available on YouTube¹¹.

A number of public and private security stakeholders and volunteers were involved in the implementation of this pilot. The tools developed for APPRAISE were presented to 20 Slovenian and foreign stakeholders, including representatives from the police, the post office and Plus Orbita, a company dealing with security systems and services. The exercise confirmed the usefulness of the system and technological solutions used in the tools developed for the APPRAISE project and provided a good basis for their further development and testing during subsequent pilots. The involvement of the Slovenian police enabled them to test their

⁹ *Pilot 3: Ljubljana*, <https://appraise-h2020.eu/node/103> [accessed: 29 XI 2023].

¹⁰ N. Czyżewska, J. Przyjemczak, *Wsparcie technologiczne nowoczesnych systemów bezpieczeństwa...*

¹¹ *APPRAISE First Pilot: BTC City – Ljubljana*, YouTube, 12 IX 2023, <https://www.youtube.com/watch?v=zWAJj2qHVbs>.

equipment, organisation, tactics and effectiveness in dealing with such or similar security incidents. In addition, through the APPRAISE tools, cooperation between public and private security entities was tested and new possibilities for information exchange between them were assessed.

International cycling race Itzulia Basque Country – pilot 1

Another study visit took place on 20 July 2023 in Iurreta, Spain, at a training centre of the Basque police. The scenario for this event included a cycling race, which was staged on the premises of the aforementioned centre (organisational considerations did not allow APPRAISE technology to participate in the real event). The objectives included holding of the Itzulia Basque Country cycling race starting in San Sebastian, Spain, and finishing in Bayonne, France.

The pilot was organised by Ertzaintza, the autonomous police force of the Basque Country, the Oceta company, the race organiser, the security company Alse and RAID, the elite tactical unit of the French National Police. The scenario involved a coordinated attack carried out on both sides of the border and cooperation between the Spanish and French services. In the first phase of the planned action, even before the start of the race, APPRAISE's web content analysis tools detected threatening posts targeting one of the race sponsors. During the next phase of the exercise, on the day of the event, a post containing direct threats to attack the race organiser was detected. By this time, the public had gathered at the start and finish areas. As planned, much of the area was a restricted-access zone, including a ban on vehicle traffic and allowing entry only for pedestrians and authorised personnel. The scenario provided the occurrence of a violent protest at the start of the race undertaken to block the start of the event. During the course of these incidents, a person with a suspicious package (backpack) entered the restricted area. When this offense was detected by APPRAISE tools, combined with facility surveillance cameras conducted with a drone, the person was detained by a security officer. After analysing the video footage, it became clear that a few minutes after the start of the race, the detained person was seen in the car park in the company of two people. Security failed to detain the other suspects, so the French police were alerted to the potential threat of an attack. On the French side, at the finish line of the race, there was surveillance using drones that

worked with APPRAISE tools. These systems detected a fight near the finish line and sent reports to the organisers using a *crowdsensing*¹² application. Additionally, the scenario involved a violation of the air zone above the race finish line by an unidentified drone and its neutralisation by the police using the APPRAISE anti-drone system. During the implementation of this pilot, both the intervention of the French police and their other actions were simulated, as at the time the RAID unit was carrying out important tasks in France (related to the Paris riots and the high terrorist threat). The actions carried out by the French police would be as follows: after indicating the address of the drone pilot, the police is dispatched, but the suspect does not open the door and threatens to attack the crowd. A special RAID unit is called to the scene. While arriving, RAID carefully analyses the web content in order to obtain as much information as possible about the alleged terrorist. RAID police officers storm, enter the terrorist's apartment and neutralise him¹³.

Also this time, all APPRAISE tools used during the pilot were demonstrated to representatives of public and private security services. During the open demonstration session, they had the opportunity to contact the project's technology partners directly and ask questions about the technologies used. Pilot 1 tested APPRAISE's tools for the rapid exchange of information between police forces from two different European countries and race organisers.

Knife attack at Międzynarodowe Targi Gdańskie SA (MTG SA Gdańsk International Fair Co.) – pilot 4

On 21 September 2023, the APPRAISE consortium conducted its fourth pilot to test once again the technologies developed by the project partners. The exercises took place at the Gdańsk International Fair (MTG) – AMBEREXPO during the 15. International Railway Fair TRAKO 2023. The Polish Platform for Homeland Security (leader of the pilot), the Gdańsk International Fair and the Provincial Police Headquarters in Gdańsk were

¹² *Crowdsensing* - an application-based programme designed for communication between the crowd and the system administrator, whose task is to collect information from people in danger and send it to the relevant services.

¹³ N. Czyżewska, J. Przyjemczak, *Wsparcie technologiczne nowoczesnych systemów bezpieczeństwa...*

involved in the organisation of these exercises. Employees of the TAURUS security office and students of the Polish Naval Academy of the Heroes of Westerplatte in Gdynia who played the role of fair participants also took part in the fair¹⁴.

The scenario of this pilot was based on a knife attack on the participants of the fair. Phase one involved constant observation of social media and content posted in the Darknet. In this way, increased activity related to the fair and a post containing threats addressed to the organisers were detected. Using tools designed to analyse web content and detect online threats, information was collected on suspicious individuals who may have directed these threats. In addition, the police received information that the day before the start of the fair, one of the suspects purchased a knife from a nearby shopping centre. On the opening day of the event, a cyber-attack on the TRAKO website was carried out, which was detected using APPRAISE tools. On the same day, the suspect entered the MTG area, where he was recognised by one of the security guards. The monitoring system that was activated tracked the suspect with a tool using technology based on so-called non-biometric features. Initially, the observed person behaved normally, calmly walking around the exhibition area. At one point, the monitoring system spotted a suspect with a backpack he didn't have before. APPRAISE video analysis tools allow you to search for items on CCTV recordings. Thanks to this, the suspect's helper who had dropped the backpack was also identified. To make it easier to find him, one of the security guards was equipped with HoloLens goggles with the image of the helper displayed on them. During this time, the suspect made his way to the restricted access area. At the entrance to the conference room, he wounded a security guard with a knife, then entered the room and continued the attack. As a result of the incidents, several fair participants were injured. The attacker then took the victims hostage and locked himself in a conference room with them. APPRAISE tools overseeing the incident triggered alerts about the attack, which were sent to both MTG security and the police. The audio analysis tools detected screams and panic, while the video analysis tools detected a running crowd, injured people lying on the ground, and a knife.

¹⁴ *Update and video for Pilot 4 in Gdansk*, <https://appraise-h2020.eu/node/107> [accessed: 10 XI 2023].

Countering the effects of panic required effective crowd management and evacuation to avoid additional casualties. Using a *crowdsensing* application, evacuation instructions were sent to those attending the fair. Additional police forces, including the Independent Counter-terrorist Sub-division of the Police and police negotiators, were called to the event area and managed to neutralise the terrorist and free the hostages. The negotiators' conversations were recorded and were transcribed using speech-to-text conversion tools. The pilot also included drone surveillance of the area. This allowed the detection of a vehicle moving through the MTG area in a suspicious manner (zigzag driving). This scenario also introduced elements of communication via a *crowdsensing* application, allowing participants in the event to inform security staff of potential danger and send information about where the injured or people who had taken cover after the attack were located¹⁵. The event can also be viewed on YouTube¹⁶.

The tools used in this pilot were demonstrated to more than 20 stakeholders, including representatives of the Police, the Armed Forces, government agencies, the Fire Brigade, operators of sports facilities, representatives of seaports and academia. As during previous meetings, there was an opportunity to contact the technology partners directly and ask questions about the tools developed for the project.

The pilot scenario 4 was the most comprehensive of all those prepared. It was the first and only one to be carried out during the actual ongoing event – a large event such as the TRAKO 2023 fair. It also used the largest number of tools developed by the APPRAISE project. This posed many - sometimes unforeseen - challenges for the preparation and organisation of the pilot, but at the same time provided the consortium with a unique opportunity to test new solutions in a real-world setting. Pilot 4 proved that they are effective. The exercise was also an opportunity to develop better cooperation between public and private entities involved in providing security in public spaces in case of attacks.

¹⁵ N. Czyżewska, J. Przyjemczak, *Wsparcie technologiczne nowoczesnych systemów bezpieczeństwa...*

¹⁶ APPRAISE Pilot in Gdańsk, YouTube, 17 XI 2023, <https://www.youtube.com/watch?v=8-7inzQ1grE>.

Kappa FuturFestival – pilot 2

The most recent verification of technologies developed under the APPRAISE project took place on 30 November 2023 in Turin, Italy. Originally, the plan was for the tests to take place from 13 to 17 November, 2023, during the ATP Finals 2023 tennis tournament. Unfortunately, it was necessary to change the date and place. Finally, the pilot was carried out as part of the Kappa FuturFestival – one of Italy's most popular summer festivals of urban electronic music. During this pilot, the organisers wanted to test elements such as: online content tracking and control, real-time video analysis, surveillance of areas and facilities with drones and cameras, elements of crowd communication.

The course of this exercise was as follows. As in previous pilots, hateful tweets against Kappa FuturFestival appeared online prior to the start of the event, so additional forces in the form of public and private security and rescue teams were prepared on the day of the event. At one point, an unidentified car passed the access barrier, drove into the pedestrian area and headed at full speed towards people queuing and waiting to enter the festival. It moved in such a way as to injure as many people as possible. Some people managed to escape, others were injured. The terrorist got out of his car and tried to enter the roofed area of Parco Dora Park. Spectators staying there were alerted via the APPRAISE application that an attack was taking place nearby and they should hide. Some of them did so, but some panicked. As they fled, they fell over and suffered injuries. Information about the dead and injured was given over the radio, social networks and a crowd detection application. Police sent a drone to the premises to check the damage caused by the incidents and whether the area was safe for rescuers to provide first aid to the injured. Online content related to the incident was monitored to find out the perpetrator's motives. A special tool searched web browsers sites, social media, analysed texts, as well as assessed risks and estimated the threats that arose. Given the large flow of people after the attack, it was extremely important to monitor the situation constantly. It was also important to collect evidence that law enforcement authorities would be able to use during the detection process. The monitoring system has been enriched with a tool that analyses the collected data (e.g. panic situations, beatings, etc.). During the implementation of the scenario, individual services were kept informed about the next steps and tasks.

This exercise, once again, proved the usefulness of the tools and technologies developed by the APPRAISE project. As before, a stakeholder meeting was organised after the pilot to discuss the possibilities of these tools and exchange comments.

Summary

The European Commission's APPRAISE project within the H2020 SU-FCT03-2018-2019-2020 Perspective: Management of information and data flow to combat cybercrime and terrorism is an initiative that has indicated the appropriate direction of development in the field of security surveillance and monitoring of open access public spaces. It has tested the functioning of tools and technologies in challenging, difficult and problematic situations in order to effectively counteract threats, avoid them and act appropriately when they arise. The level of advancements of the technologies developed and produced allows us to conclude that the tools that make use of them will interact efficiently with those already existing and will contribute to a faster and more effective response by the services to arising threats. Thanks to the efforts of the people involved in the APPRAISE project, the activities made in the project to improve safety will continue and be developed through various initiatives.

Jarosław Przyjemczak, PhD

Doctor of social sciences in the discipline of security sciences, assistant professor at the Faculty of Law and Administration of the E. Kwiatkowski University of Business and Administration in Gdynia. Retired major, for many years served in the Independent Counter-terrorist Sub-division of the Police in Gdańsk. Participant in numerous national and international courses and trainings related to counter-terrorism. He completed, among other things, a strategic counter-terrorism and terrorist threats course in Bramshill, United Kingdom organised by the Police College (CEPOL) within the Europol framework. Member of the Polish Association for National Security, security expert of the Polish Platform for Homeland Security. Scientific editor of the cyclical publication

Zadanie specjalne – człowiek, technologia, instytucja (Special task - man, technology, institution).

Contact: jarek.przyjemczak@wp.pl

Nina Czyżewska

Project Manager at the Polish Platform for Homeland Security. She completed a master's degree in political science with a specialisation in international organisations at Leiden University in the Netherlands and a bachelor's degree in international relations at the Jagiellonian University in Kraków. In the PPHS, she is responsible for the implementation and execution of public space security and counter-radicalisation projects funded by European Union programmes.

I believe we can handle the new threats!

Interview with Col. (Ret.) Christopher P. Costa, former counterterrorism advisor to the US president and director of the International Spy Museum in Washington, DC

The world is changing at a rapid pace. The nature of modern threats is also changing. The unstable geopolitical situation, the rapid development of new technologies, the emergence of cryptocurrencies and artificial intelligence are causing security services to face new challenges. How can they prepare for them to more effectively counter emerging threats? Colonel (Ret.) **CHRISTOPHER P. COSTA**, a long-time US intelligence officer, answers this question by referring both to his own extensive experience and to the history of global espionage and terrorism. He points out both the need to critically analyze the lessons of the past and the services' ability to take advantage of new technological opportunities. He stresses the importance of exchanging information and developing cooperation at the international level, and emphasizes the role that public education plays in prevention efforts. He sees the promotion of knowledge as the mission of the International Spy Museum in Washington, which he directs. The interview was conducted during Director Costa's visit to Poland, and the conversation is accompanied by reflections on the current situation in Central and Eastern Europe.

Damian Szlachter: The interview will be published on the 20th anniversary of the attacks on Madrid's commuter transport system, widely accepted as a European awakening in the fight against terrorism. However, I would like to start this conversation with another event, a symbol of the end of the 20th century. If I may ask, where were you on September 11, 2001, where did you find information about the attacks on the WTC and the Pentagon, and what were the immediate consequences for you?

Christopher P. Costa: When 9-11 happened, I had just moved to New York State, which is located just up the river from New York City in Albany. At the time, I was taking command of a recruiting battalion, a role that involves overseeing the enlistment of young individuals into the Army. Before this, I had spent my career as an intelligence officer in combat zones even prior to 9-11. However, the Army decided to assign me to a recruiting battalion, which was not where I wanted to be when the terrorist attacks occurred.

Initially, I felt bad that I wasn't with my colleagues who were fighting in Afghanistan. I had to spend the next two years learning about the Army and its mission. However, I decided to use this opportunity to study terrorism. I taught a class on terrorism in the evenings while also managing my other responsibilities. I spent a year and a half studying terrorism, almost obsessively, to understand this dynamic better.

Although I wasn't overseas, I kept waiting for the call to deploy. I wanted to use my skills and knowledge to help in the fight against terrorism. Eventually, before I changed command, a general officer called me and asked for my help with human intelligence in Afghanistan. I eagerly accepted the opportunity without hesitation.

When 9-11 occurred, I was in New York State, and just like most everyone else in the world, I was appalled by it. However, I also felt a little sorry for myself at the time because I wasn't in a position to use my skills and training overseas. Looking back, I realized that this experience was positive for my personal development since it allowed me to take the time to study and prepare for the counterterrorism fight. Thank you for that question.

When reading your biography, you can proudly say that you have worked in every area of the US counterterrorism system, from operational work, through the tactical level, to the strategic level, headed by the President of the United States. In each of them, the coordination of many entities participating in anti-terrorist activities is extremely important. My question is how to maintain a high degree of coordination at each of the three levels, what is your personal experience with this?

Ch. C.: Just how to coordinate all those entities on the operational, tactical, and strategic levels is more art than science. So that's an important question. And I will tell you that although I worked at the operational and tactical levels, on multiple deployments for many years, when 9-11 happened, I had not, as of yet, served at a strategic level. I have always served in operational and tactical levels. I had certainly been conducting operations that I knew the chairman of the Joint Chiefs staff, for example, would have visibility on to brief the President on if required, but I had never seen the complete strategic-operational-tactical cycle until I had the benefit of serving at the White House. And on the point of the White House, please allow me to digress for a second. I love that you produce a journal such as this ABW journal, because I'm a lifelong learner. And I've already suggested to you that my studying terrorism and teaching in the aftermath of 9-11 helped me get my head around these problems. I had read about national security decision-making. I was fascinated by how powerful government figures make decisions, and how leaders on a battlefield make decisions. So, when I had the opportunity to go to the White House, and I had the opportunity also to see how we worked together with foreign partners, and how we built a counterterrorism enterprise to focus on a global fight on counterterrorism, those experiences came together for me when I served on the National Security Council at the White House. And that's when I was the convening authority for the interagency, meaning I was roughly a three-star general officer equivalent, assistant secretary level in our system. There, I was able to pull together the interagency to focus on strategic threats. And the secret to my success, if I had success at all, was having the humility to know that I didn't have all the answers, having the humility and experience to know that I have to represent and let others offer their opposing views. I knew not to 'fall in love' with my recommendations on policy and

courses of action for the President to decide on. I learned all of that on the battlefield. So those experiences helped me serve at the White House. But I never saw the strategic, operational, and tactical come together until I served at the National Security Council. And what a tremendous experience that was.

The 2018 National Strategy for Counterterrorism of the USA is a pillar of the US counterterrorism system. At that time, Poland had a National Anti-Terrorist Programme which performed a similar function. How to effectively supervise the implementation of such a strategy by state authorities? In other words, how to assess the timeliness and quality of implementation of strategy tasks by area leaders and their supporting institutions? How was it solved in the US?

Ch. C.: We began shaping the 2018 National Counterterrorism Strategy the day I came into the White House by operationalizing counterterrorism ideas. And frankly, most of our efforts were focused on kinetically going after terrorists in places like Afghanistan, and on the ground in Syria and Iraq. So while we were implementing strategies, while we were accelerating our approach, we were also framing what our strategy looks like. There was a time that I believed our strategy should almost singularly focus on the jihadi threat because we were so focused on Islamist terrorism. But then my team concluded that there are other threats, too, and built in the far-right threat, and other extremist threats to include, in the 2018 strategy, you'll see the word Nazi used or the organization Nazis used because we recognized that we had to go beyond the jihadi threat. So the wisdom of the interagency coming together with a feedback loop, hearing from all of the agencies responsible for terrorism, we recognized that we needed to build in words and framing on domestic violent extremism, on counter-radicalization, on the far right, and any kind of extremism that could lead to political violence. So for the first time in the nation's history from a policy standpoint, the United States talked about domestic terrorism. And remember, we had our terrorism domestically in Oklahoma City in 1995, but we had the wisdom in 2017-18 to recognize a changing terrorism landscape. Despite the focus on ISIS, Al-Qaeda, Afghanistan, Iraq, and Syria, we knew that we needed to focus on domestic terrorism,

too. That said, it's now 2023 (the interview was conducted in August 2023 - editor's note), and there's been an evolution of thinking on terrorism threats, and the current Biden administration did what I think is right, and that is to say, they focused a strategy on domestic violent extremism, and they published that soon after the new administration came on board.

Indeed, the threat evolves. I didn't expect the 2018 strategy to last forever, but I'm really happy that it lasted until this year because that represents a solid strategy that helped the last administration and the current administration. And just one other focus on how do you assess implementation? So that is the mechanics of, as we say, sausage making. The interagency is responsible for identifying specific measures of effectiveness and performance, and they go back to the National Security Council and find out how many attacks were disrupted, and how many intelligence agreements with partners across the world were impacted, for example. The interagency takes those lofty words in a strategy and turns them into measurable and implementation instructions because it's easy to write an overarching strategy, but the challenge is implementation and measuring performance and success. What's much more challenging is implementing that strategy and assessing the implementation of that strategy.

Currently, on the eastern flank of NATO, we have an unprecedented situation related to the internal security of countries bordering the Russian Federation and Belarus. In the opinion of national and EU experts, in the next three years, terrorist activities should be expected to be used for hybrid activities carried out with the support of state entities. These activities will focus on attacks disrupting the continuity of operation of critical infrastructure (e.g. transport, energy, telecommunications). How to work on increasing the resilience of such facilities strategically for state security?

Ch. C.: Currently, in our eastern flank of the NATO, we have an unprecedented situation related of course to the internal security of countries bordering Russia and Belarus. According to national EU experts, in the next few years, this activity should be expected to be used by private activities carried out with the support of those

states. Those activities will focus on attacks disrupting the continuity of operational or critical infrastructure, of course. How to work on increasing the resilience of such facilities as critical infrastructure? So this gets to the heart of what I think the challenges are. I think Putin is going to become increasingly unhappy with his ability to wage conventional warfare. So he is going to revert more deliberately to infrastructure attacks. As such, the heart of your question is really important. And we know Russia has a history of, as somebody from the Internal Security Agency (ABW) has pointed out, of maskirovka, and not only disruption but disinformation, subversion, covert actions, assassinations, all things we talk about at the Spy Museum from the lens of history. But those activities are going to begin to happen outside of Ukraine to increasingly put stress on the alliance of NATO and other partnerships. So critical infrastructure, not only from a cyber-standpoint but also physical infrastructure is crucial because it's vulnerable to sabotage. We've seen dams that have been disrupted. We've seen bridges that have gone down in Ukraine, railways, and other infrastructure at risk. Again, from a special operations standpoint, we know history is a great guide to the way nations have handled special operations and counter-subversion. As such, I think the importance of the ABW, the importance of lessons learned, and sharing those lessons learned, are crucial. And I've said this elsewhere, this isn't just for you. I say this to my friends at the FBI, and to generals at Special Operations Command, the 'coin of the realm', so to speak, is counterintelligence going forward, because the threats are going to be hybridized, meaning intelligence services are going to behave increasingly more like terrorists. We see that from Iran in their employment of proxies. We see that in Russia. Proxies are going to be mobilized to do more increasingly lethal and dangerous things. I think, then, that the heart of your question is important, but I also have faith in the Polish security services, and you're asking all the right questions. I do. I read Polish history. I'm very impressed by it. I mean, I've always been a fan of Polish military and security capabilities. Unfortunately, as you all know, historically, Soviet-German disinformation in past years has tried to propagandize a false narrative about your impressive nation. We know that Poland has been a strong military power throughout history, but you have also fallen victim to some of your geography.



Photo: Christopher P. Costa, Director of the International Spy Museum in Washington (left), and Damian Szlachter, Editor-in-Chief of the magazine “Terrorism – Studies, Analyses, Prevention”, during the meeting at the Central Training and Education Centre of the Internal Security Agency in Emów.

Source: own materials.

What are the challenges faced by Western secret services and law enforcement agencies that carry out tasks to combat terrorism in this decade of the 21st century? How to improve their structures, personal potential, or technical resources against terrorists using unmanned systems, 3D printing, cryptocurrency payments, and professionally encrypted instant messengers or hidden forums on gaming platforms?

Ch. C.: The first step for an intelligence service is to be prepared to vigorously study lessons learned. You’re doing that. I’m seeing that. You have to be introspective. You have to encourage reflection. You have to encourage, even if it’s never published, people to write internally, and to share their perspectives and lessons learned. That’s the first step, to recognize that the world is changing and intelligence services have to be far more adaptive. And I’ll give you an example. The United States, much to the chagrin and anger, if you will, of some of my former colleagues, don’t like the fact that intelligence sharing has been so dramatically changed as a result of the war in Ukraine. In other words, we have declassified in the United States a lot of sensitive intelligence. I think it’s brilliant. I think it’s inspired. And I think it is an important evolution of information and the use of social media to get ahead of our adversaries. For example,

according to media reports, the United States seemed to know that Russia was going to conduct some kind of act that would be a pretext to suggest that Ukrainians employed chemical weapons. According to the media, the United States seemed to understand that a ruse by Russia was to be implemented. As a consequence, the United States shared that intelligence, so if it happened, everybody knew that it was a Russian disinformation operation. That's staying ahead of the speed of information. And that's just one example. How do we reconcile social media? How do we use social media? Well, the United States, and at least the United Kingdom, because I'm not tracking Polish media, are now publishing and advertising openly, hey, if you're not happy with Putin, reach out to CIA, and here's the number, and here's how you can do it securely. Brits are doing the same thing. We know there are a lot of dissatisfied Russians, both of us, you and I understand that. How do we tap into that? If you can use X (former Twitter) accounts for bad purposes, or malign purposes, you can use social media for good or to benefit security services.

Security professionals have to reconcile everything from 3D printing, cryptocurrency, and all of these new-century dynamics, to quickly come together in order to better understand the threats. Artificial intelligence is another looming problem, and the United States has to do so, along with the world community, and it can't be a U.S. only solution, especially staying ahead of artificial intelligence. I have just participated in a brief conference, where I heard from former senators about the challenges with policy on how to stay ahead of AI. There is no universal policy for artificial intelligence, but we have to work with the international community in ways we never have before. The United States certainly did that with Huawei. I don't know what Poland's use of Huawei was, but I know that media reported that the United States recognized the serious implications of Huawei in China having a 'backdoor' for collecting data, it wasn't heavy-handed, but the United States shared their concerns with partners, and many partners recognized threats to privacy. We have to do the same with artificial intelligence. We have to understand what the risks are, and what the opportunities are, but what are our vulnerabilities, too? And the other thing I want to say is the United States produces unclassified intelligence on the kinds of the threat we're seeing from the world, and we publish that for the public. The Director for National Intelligence publishes

a worldwide threat assessment. These ideas of threats from AI misuse, the idea of global pandemics, maybe more dangerous than COVID, the idea of dissatisfied populations, the idea of not just more far-right extremist or populist views, but also those views that are manipulated by intelligence services, will make more nations vulnerable to anti-government action against them. In other words, there is a trend that is coming into sharper focus that governments are going to be more vulnerable. For example, people believe that the government can't protect them from COVID; the government can't protect them from losing their life savings from hacking. With all of these things and technologies, people being unable to keep up with all the technological change, and artificial intelligence, nations are more vulnerable than ever. So, it's intelligence and security services that are the first line of defense. I'm glad that when I exercised my tradecraft overseas, it was 'old school'. The Russians used the same kind of tradecraft I did. It was universal. And so did Poland. Life was simpler.

The world has changed dramatically because of technology. It is very challenging. But I do have faith, especially when I looked at the people that were in the auditorium today and heard their questions, it's no different when I talk to the FBI and other agencies. In short, I'm confident that this generation will figure it out.

The last question is that you are the Director of the famous International Spy Museum in Washington, are there exhibits directly related to the history of operational activities carried out as part of the war on terror?

Ch. C.: Well, unfortunately, we show the public the consequences of strategic surprise of 9-11 in particular, and it's related to what you said, the exigency and the circumstances of 9-11 changed the United States' focus on counterterrorism. And it forced the interagency to communicate in ways they never did before. Unfortunately, we don't want to wait for a crisis to cause necessary change, but it does. So at the Spy Museum, we talk not just about 9-11, we compare that strategic surprise to Pearl Harbor, and we demonstrate interactives on cyber vulnerabilities, too. We show the public national security decision-making in the decision to launch a raid against Bin Laden. We show briefly how the operation was executed, that's important,

but what's more important to educate the public, is how was that the decision made to launch a raid. And how do you red team-challenge- your own intelligence judgments? And who were those faceless, nameless analysts? How did they do their work long before we executed the operation?

The Spy Museum tells those stories. Also, when you go into our fourth floor, which is why nations spy, our stories include strategic warnings. The Museum does not just focus on jihadists and post-9-11 terrorism, we tell stories about anarchists and militia threats in the United States. The red scare and anarchist fears in 1919, for example. The birth of the FBI came out of J. Edgar Hoover investigating anarchists, right? We address the Oklahoma City attack. The International Spy Museum focuses on a wide array of stories. And of course, one of my favorite and deeply personal stories is 1972 Munich. I was 10 years old when the attacks at the Munich games took place, so you now know how old I was, if you already didn't know. I watched that live. So did 900 million other people across the world. That got my attention as a 10-year-old. That ushered in a whole new era of terrorism, but also slowly shaped into the wave we're still dealing with, which is jihadi-inspired terrorism. The Museum tells all of those narratives at a very macro level. And we have artifacts that highlight those periods in terrorism history. And also, we show the public interrogation through history. And I don't mind saying that we tackled the controversial subject of enhanced interrogation. I won't talk a lot about that here, because I want your readers to come visit and see how we handle that in the Museum.

Can I offer another comment? I want to make another important point. I want to again stress that, I went to the uprising museum here in Warsaw. The story of Polish resistance, the story of tradecraft, and you used the word resilience in the second world war, is an extraordinary model of courage. And I tell anyone that will listen about Polish courage and resilience. It's crucial still to understand the importance of unconventional warfare. We didn't talk a lot about that today. But much of my career was focused on understanding resistance and unconventional warfare. And working with people that studied it and practiced it. So, I believe strongly that Poland is an extraordinary example to study in terms of resilience, resistance and irregular warfare. In light of Russia's malign behavior those lessons are enduring and are worth thinking about.

We also tell a human intelligence story of an individual that was from Denmark and volunteered his services, and was recruited as a spy. His name is Morten Storm. He knew Anwar al-Awlaki, a propagandist for AQ. That's one of the first stories we tell on counter-terrorism. But through the lens of human intelligence. The Museum also, in that same gallery on human intelligence, tells the story of an Israeli Shin Bet officer, and a Palestinian that was associated with Hamas (it is about Mosab Hassan Yousef- editor's note). The Museum shows the dynamics of the clandestine relationship between source and handler. I appreciate how the Museum tells that story, as somebody who's handled sources. The *Green Prince* was a book written about that particular story.

And then the next story on counter-terrorism is about analysis. And how prior to 9-11, mostly women analysts at CIA and elsewhere in the U.S. intelligence community, were tracking Bin Laden, before, during, and after 9-11. And those women talk about some of their analytical tools. We tell that important story. And there are some great interactives. And that transitions into a red-teaming exercise that shows the Bin Laden compound. And shows the public examples of national security decision-making. I've talked about my White House experience working terrorism. There, I wouldn't have been the ultimate decision-maker for the Bin Laden raid. In that case, the President of the United States was the decision maker.

The Museum also compares the dynamics of 9-11 to Pearl Harbor. And the dynamics are almost the same. Everything from mirror imaging to noise versus signals. Here again, we tell that story from the lens of history. As noted already, the Museum transitions to anarchists in places like Washington, D.C. in 1919. We have artifacts from the Oklahoma City federal building attack. And then, lastly, as I already shared my personal recollections of 1972 Munich, we tell that story, too.

The Museum permanent exhibition shows the history of espionage and tradecraft during the Cold War, and how similar some of the things are for providing important context for what we're seeing in Ukraine today. We talked about the idea of resistance and unconventional warfare, and irregular warfare, the Museum has artifacts for those efforts during WW 2, that by the way, Poland practiced and executed so well. It's important to note that we're seeing Ukraine exercises some excellent examples of unconventional warfare

against Russia. Those past lessons must be considered instructional and worth reconsideration as the West must counter the subversive work of Russia.

The International Spy Museum does not take a position. We don't tell people what to think. They decide. And I think that's important. These are really important questions, thank you.

He was talking: Damian Szlachter

Colonel (Ret.) Christopher P. Costa

Retired intelligence officer. He served in the Department of Defense for 34 years, during which he spent 25 years as an intelligence officer with Special Operations Forces (SOF). He was recognized for his sensitive human intelligence work in Afghanistan with two Bronze Stars. After retiring from the military, he continued to serve at the Naval Special Warfare Development Group as a civilian and was later inducted into the United States Special Operations Command Hall of Honor for his lifetime service to US Special Operations. Colonel Costa's most recent role was as the Special Assistant to the President and Senior Director for Counterterrorism at the White House. He is now the Executive Director at the International Spy Museum.

