Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 237–262

https://doi.org/10.4467/27204383TER.25.009.21512

Artykuł

Cyberzagrożenia jako działalność hybrydowa przeciwko Unii Europejskiej w świetle obecnej sytuacji geopolitycznej

Cyber threats as hybrid activity against the European Union in light of the current geopolitical situation

MONIKA STODOLNIK

https://orcid.org/0009-0000-5319-7968

Agencja Bezpieczeństwa Wewnętrznego

Abstrakt

W artykule została przedstawiona analiza cyberzagrożeń jako przejawu zagrożeń hybrydowych, z którymi zmaga się Europa. Autorka przeanalizowała raporty państw Unii Europejskiej i NATO pod kątem tego, w jaki sposób wskazane zagrożenia są prezentowane przez służby wywiadowcze, rządy oraz krajowe zespoły CERT (Computer Emergency Response Team) i CSIRT (Computer Security Incident Response Team). Omówiła również kategoryzację cyberzagrożeń na podstawie ich źródła pochodzenia oraz celu działania, z uwzględnieniem grup sponsorowanych przez państwa, haktywistycznych oraz cyberprzestępczych. Wskazała na wzrastającą częstość cyberataków, prowadzonych zwłaszcza z Rosji i Chin, oraz omówiła ich wpływ na infrastrukturę krytyczną i stabilność polityczną państw. Zaprezentowała zmieniający się krajobraz cyberzagrożeń w Europie, podała przykłady cyberataków oraz opisała sposoby raportowania o tych zdarzeniach przyjęte w Danii, Niemczech, Estonii, Litwie, Łotwie oraz Polsce.

Słowa kluczowe

zagrożenia hybrydowe, cyberatak, cyberbezpieczeństwo, dezinformacja, operacje informacyjne

Abstract

The article presents analysis of cyber threats as a manifestation of the hybrid threats facing Europe. The author analysed reports from European Union and NATO countries in terms of how the identified threats are presented by intelligence services, governments and national CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams). She also discussed the categorisation of cyber threats based on their source of origin and their purpose, including state-sponsored, hacktivist and cybercriminal groups. She pointed to the increasing frequency of cyber attacks, especially those conducted from Russia and China, and discussed their impact on the critical infrastructure (CI) and political stability of states. She presented the changing landscape of cyber threats in Europe, gave examples of cyber attacks and described the methods of reporting these incidents adopted in Denmark, Germany, Estonia, Lithuania, Latvia and Poland.

Keywords

hybrid threats, cyber attack, cyber security, disinformation, information operations

Wprowadzenie

Współczesna sytuacja geopolityczna sprawia, że zagrożenia hybrydowe stają się jednym z najpoważniejszych wyzwań dla bezpieczeństwa i stabilności Europy. Zagrożenia hybrydowe stanowią połączenie taktyk konwencjonalnych oraz niekonwencjonalnych i mają na celu m.in. destabilizację państwa, jego demokracji oraz podważenie zaufania społecznego. Odwołując się do definicji Francisa Fukuyamy, którego zdaniem (...) *zaufanie to mechanizm oparty na założeniu, że innych członków danej społeczności cechuje uczciwe i kooperatywne zachowanie oparte na wyznawanych normach*[1], można zauważyć, że manipulacyjne działania psychologiczne, dezinformacyjne naruszają ten

[1] F. Fukuyama, *Zaufanie. Kapitał społeczny a droga do dobrobytu*, Warszawa 1997, s. 38.

właśnie mechanizm i pogłębiają podziały w społeczeństwie. W 2025 r. Europa jest szczególnie narażona na tego rodzaju zagrożenia ze względu na bliskie sąsiedztwo z możliwym przeciwnikiem, a także rozwój technologiczny, którego potencjał może być wykorzystany zarówno do obrony, jak i ataku. Obserwacje i lekcje wynoszone z wojny w Ukrainie wskazują prawdopodobne wektory działalności Federacji Rosyjskiej (FR) w sytuacji rozszerzenia konfliktu na inne państwa europejskie. Dynamiczny rozwój sztucznej inteligencji w ostatnich latach wspiera wrogą działalność w cyberprzestrzeni, pod kątem generowania treści dezinformacyjnych oraz rozwoju narzędzi służących do ataków na infrastrukturę teleinformatyczną.

Standard życia rośnie wraz z postępem technologicznym. Rozwój technologii informacyjno-telekomunikacyjnych (ang. *information and communication technologies*, ICT) oraz rosnąca zależność od automatyzacji różnych sektorów, zwłaszcza systemów kontroli przemysłowej (ang. *industrial control systems*, ICS), powodują, że ryzyko narażenia społeczeństwa na zagrożenia pochodzące z cyberprzestrzeni się zwiększyło. Destrukcyjne działania są kierowane zwłaszcza na sektor energetyczny, będący kluczowym filarem gospodarki każdego nowoczesnego państwa[2]. Jak wskazuje EnergiCERT, duński zespół reagowania na incydenty komputerowe sektora energii, liczba ataków na ten sektor w Europie stale wzrastała w latach 2015–2022[3]. Ataki na podmioty sektora energii mogą doprowadzić do paraliżu kraju – niezależnie od tego, czy sprawcy kierują się pobudkami finansowymi, ideologicznymi czy politycznymi. Jednocześnie liczba oraz charakter oficjalnych dokumentów i korespondencji tworzonych i przetwarzanych w formie elektronicznej sprawiają, że jest to główny cel operacji szpiegowskich stwarzających zagrożenie bezpieczeństwa narodowego.

W artykule został przeanalizowany wielowymiarowy charakter zagrożeń hybrydowych, przed którymi stoi Europa. Dokonano tego na podstawie przeglądu raportów dotyczących cyberzagrożeń oraz cyberataków jako przejawów działalności hybrydowej, sporządzonych w wybranych krajach Unii Europejskiej i NATO. Przedmiotem analizy był sposób, w jaki te zagrożenia są przedstawiane przez służby wywiadowcze, rządy oraz

[2] *Cybersecurity of Critical Sectors – Energy*, ENISA, https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/energy [dostęp: 8.04.2025].

[3] *Cyber attacks against European energy & utility companies*, EnergiCERT, wrzesień 2022, https://sektorcert.dk/wp-content/uploads/2022/09/Attacks-against-European-energy-and-utility-companies-2020-09-05-v3.pdf [dostęp: 8.04.2025].

zespoły CERT i CSIRT Danii, Niemiec, Estonii, Litwy, Łotwy i Polski – państw zlokalizowanych w niedużej odległości od FR i będących w zainteresowaniu rosyjskich grup cyberofensywnych.

Krajobraz cyberzagrożeń jako zagrożeń hybrydowych

Zgodnie z definicją NATO: *Zagrożenia hybrydowe łączą środki wojskowe i niewojskowe, jawne i niejawne, w tym dezinformację, cyberataki, presję ekonomiczną, użycie nieregularnych formacji zbrojnych i wojsk regularnych. Metody hybrydowe służą do zacierania granic między wojną a pokojem oraz mają na celu sianie wątpliwości w umysłach ludzi będących grupą docelową. Ich celem jest destabilizacja i podważanie fundamentów społeczeństw*[4]. Unia Europejska w dokumencie opracowanym przez Komisję Europejską, zatytułowanym *Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej* (*Joint framework on countering hybrid threats – a European Union response*), podkreśla, że (...) *zagrożenia hybrydowe są różnie definiowane i definicje te należy formułować w sposób elastyczny, tak by uwzględniały one zmienny charakter tego rodzaju zagrożeń*[5]. Z kolei Europejskie Centrum Doskonalenia ds. Przeciwdziałania Zagrożeniom Hybrydowym (European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE) przedstawia zagrożenia hybrydowe jako (...) *działania podejmowane przez państwa autorytarne oraz podmioty niepaństwowe, które często działają jako pełnomocnicy reżimów autorytarnych. Przykładami aktorów stwarzających zagrożenia hybrydowe są Rosja, Chiny i Iran. Podmioty niepaństwowe mogą obejmować grupy, ruchy lub inne jednostki wykorzystywane lub podporządkowane w celu realizacji określonych celów strategicznych*[6].

[4] *Countering hybrid threats*, NATO, 7.05.2024, https://www.nato.int/cps/en/natohq/topics_156338.htm? [dostęp: 19.03.2025]. Tłumaczenia w artykule pochodzą od redakcji (dop. red.).

[5] *Wspólny komunikat do Parlamentu Europejskiego i Rady. Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej*, Bruksela, 6.04.2016, JOIN(2016) 18 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52016JC0018, s. 2 [dostęp: 19.03.2025].

[6] *Frequently asked questions on hybrid threats*, Hybrid CoE, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [dostęp: 19.03.2025].

Rozważając cyberzagrożenia w tym kontekście, można je podzielić na ogólne kategorie w zależności od tego, kto jest ich źródłem oraz jakimi metodami posługuje się do osiągnięcia obranego celu:

- Podmioty państwowe (aktorzy państwowi), często wysoce zaawansowane technologicznie i operacyjnie:
  - cyberszpiegostwo,
  - cybersabotaż,
  - operacje informacyjne w cyberprzestrzeni.
- Grupy hakerskie (haktywiści) motywowane ideologicznie:
  - zakłócanie funkcjonowania systemów i usług IT (ataki typu DDoS),
  - cybersabotaż (ataki zmieniające parametry, niszczące, wpływające na świadczenie usługi w sposób inny niż przez niedostępność),
  - podmiana zawartości strony (ang. *defacement*),
  - ataki typu *hack-and-leak* (włamanie i wyciek danych).
- Cyberprzestępcy działający dla korzyści finansowych:
  - wymuszenia finansowe z wykorzystaniem oprogramowania ransomware,
  - wymuszenia finansowe przez groźbę ujawnienia danych.

Podmioty państwowe, nazywane również grupami sponsorowanymi przez państwo, często utożsamiane z grupami APT (ang. *advanced persistent threat*)[7], to jednostki wspierane przez rząd, często będące częścią służb specjalnych prowadzące ofensywne działania cybernetyczne w interesie państwa[8]. Cyberszpiegostwo, będące naturalnym rozszerzeniem tradycyjnych metod wywiadowczych, stanowi trzon ich działalności – zarówno jako cel sam w sobie, jak i środek do przeprowadzania rozpoznania, niezbędnego do pozostania niezauważonym. Cyberszpiegostwo jest najczęściej realizowane za pomocą ataków phishingowych lub spearphishingowych, czyli wykorzystujących techniki inżynierii społecznej do manipulowania za pośrednictwem poczty e-mail w celu pozyskania określonych informacji lub infekowania stacji roboczych złośliwym oprogramowaniem. Cyberszpiegostwo oprócz phishingu może obejmować również naruszenie bezpieczeństwa urządzenia lub sieci przez wykorzystanie luki w zabezpieczeniach, czyli słabości systemu IT (może to być

[7] Grupy APT – zorganizowane jednostki realizujące wyrafinowane i długo trwające ataki w cyberprzestrzeni.

[8] J. Kose, *Cyber Warfare: An Era of Nation-State Actors And Global Corporate Espionage*, „ISSA Journal" 2021, t. 19, nr 4, s. 12–15.

zarejestrowana, dobrze znana podatność, luka typu zero-day, nadużycie funkcji systemu lub błąd użytkownika). Tego rodzaju ataki podważają jeden z 3 kluczowych filarów cyberbezpieczeństwa – poufność[9]. W odniesieniu do integralności danych takie ataki są uznawane za cybersabotaż – mają charakter destrukcyjny i niosą ze sobą znacznie poważniejsze konsekwencje. Mogą zakłócić życie codzienne obywateli, np. przez przerwanie dostaw energii elektrycznej czy opóźnienia w transporcie, gdy zostaną wymierzone w infrastrukturę krytyczną. Mogą nawet spowodować ofiary śmiertelne, zwłaszcza gdy celem staną się systemy nawigacyjne lub systemy ochrony zdrowia.

Operacje informacyjne to (...) *działania podejmowane w celu wpływania na informacje i systemy informacyjne przeciwnika przy jednoczesnej ochronie własnych zasobów informacyjnych i systemów*[10]. Operacje informacyjne wspomagane cyberatakami, znane również jako kampanie wpływu – terminy te są stosowane zamiennie – (...) *znajdują się na styku oszustw opartych na danych wywiadowczych i efektów wywołanych z myślą o strategii*[11]. Polegają na (...) *celowym wykorzystaniu informacji przez jedną stronę, aby zdezorientować przeciwnika, wprowadzić w błąd i ostatecznie wpłynąć na dokonywane przez niego wybory oraz podejmowane decyzje*[12]. Tego rodzaju działalność może obejmować naruszanie systemów IT mediów informacyjnych w celu publikowania spreparowanych treści w renomowanych źródłach, tworzenie własnych stron internetowych i profili w mediach społecznościowych oraz masowe wysyłanie wiadomości e-mail czy SMS.

Słowo haktywizm powstało z połączenia słów *hacking* i *activism*. Oznacza ono (...) *połączenie oddolnego protestu politycznego z hakowaniem komputerowym*[13]. W ostatnim czasie na czele haktywistów znajdują się grupy prorosyjskie i propalestyńskie, organizujące się i komunikujące przez

[9] Triada CIA: poufność, integralność, dostępność (ang. *confidentiality, integrity, availability*).

[10] D.T. Kuehl, *Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age*, „International Law Studies" 2022, t. 76, s. 36.

[11] J. Vićić, R. Harknett, *Identification-imitation-amplification: understanding divisive influence campaigns through cyberspac*e, „Intelligence and National Security" 2024, t. 39, nr 5, s. 897–914. https://doi.org/10.1080/02684527.2023.2300933.

[12] H. Lin, J. Kerr, *On Cyber-Enabled Information/Influence Warfare and Manipulation*, w: *The Oxford Handbook of Cyber Security*, P. Cornish (red.), Oxford University Press 2021, s. 251–272. https://doi.org/10.1093/oxfordhb/9780198800682.013.15.

[13] T. Jordan, P. Taylor, *Hacktivism and Cyberwars. Rebels with a cause?*, London 2004, s. 1.

aplikację Telegram oraz przeprowadzające różnego rodzaju cyberataki o różnej skuteczności. Oddolny charakter tych działań bywa kwestionowany. Niektórzy eksperci uważają, że grupy takie jak XakNet Team, Infoccentr, Solntsepek i Cyber Army of Russia Reborn współpracują z rosyjskim Głównym Zarządem Wywiadowczym (GRU) oraz z powiązanymi z nim grupami cyberzagrożeń, takimi jak APT28[14] i APT44[15].

Najbardziej znane grupy haktywistyczne stosują głównie ataki typu *distributed denial-of-service* (DDoS), których celem jest uniemożliwienie dostępu do wybranych stron internetowych lub usług dla ogółu użytkowników. Grupy te naruszają również infrastrukturę przez nieautoryzowany dostęp. Często nie chodzi im przy tym o osiągnięcie jakiegoś złożonego celu, a jedynie o zademonstrowanie swoich możliwości technicznych. Narzędzia wykorzystywane przez te grupy do rozpowszechniania swoich przekazów to również *defacement* stron internetowych oraz ataki typu *hack-and-leak*. Pierwsze działanie polega na zastąpieniu treści strony internetowej wiadomością od hakera, drugie na upublicznieniu danych wykradzionych z sieci i serwerów zaatakowanego podmiotu[16].

Podobnie jak haktywizm jest aktywizmem w cyberprzestrzeni, tak cyberprzestępczość (...) *składa się z czynów przestępczych popełnianych online przy użyciu sieci łączności elektronicznej i systemów informatycznych*[17]. Takimi czynami są np. ataki na systemy informatyczne jako najbardziej krytyczne dla państwa, a nie dla samych obywateli. Najczęściej zgłaszane incydenty związane z cyberprzestępczością dotyczą oprogramowania ransomware, które (...) *stało się dominującym zagrożeniem dla cyberbezpieczeństwa*[18]. Ransomware to rodzaj złośliwego oprogramowania, które jest

[14] Mandiant Intelligence, *Hacktivists Collaborate with GRU-sponsored APT28*, Mandiant, 23.09.2022, https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions [dostęp: 19.03.2025].

[15] G. Roncone i in., *APT44: Unearthing Sandworm*, Mandiant, 17.04.2024, https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf [dostęp: 19.03.2025].

[16] D. Sancho, *Understanding Hacktivists. The Overlap of Ideology and Cybercrime*, Trend Micro, 4.02.2025, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/understanding-hacktivists-the-overlap-of-ideology-and-cybercrime [dostęp: 19.03.2025].

[17] *Cybercrime*, European Commission, 31.10.2024, https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en [dostęp: 19.03.2025].

[18] T. McIntosh i in., *Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration*, „ACM Computing Surveys" 2024, t. 57, nr 1, s. 1. https://doi.org/10.1145/3691340.

wykorzystywane po to, aby wymusić od zaatakowanego okup przez odmowę dostępu do systemów i danych. Większość obecnie dokonywanych ataków ransomware to ataki podwójnego wymuszenia, w których atakujący szyfruje dane i je kradnie. Żąda przy tym okupu nie tylko za odszyfrowanie, lecz także za uniemożliwienie ich sprzedaży czy publikacji[19]. Takie oprogramowanie może zakłócać operacyjność podmiotu, a ze względu na skutki w postaci przerwy w świadczeniu usług oraz wycieku danych, w tym klientów, może powodować utratę zaufania ze strony potencjalnych partnerów do współpracy.

W latach 2014–2024 częstość ataków hybrydowych, zwłaszcza w cyberprzestrzeni, rosła. Federacja Rosyjska jest jak dotąd największym sprawcą sponsorowanych przez państwo cyberataków – włączając w to ataki prorosyjskich haktywistów – przeciwko krajom europejskim[20]. Były one wymierzone głównie w systemy rządowe i strony internetowe, infrastrukturę krytyczną, firmy państwowe i prywatne, think tanki, organizacje pozarządowe, dziennikarzy i polityków. W 2022 r. grupy haktywistów działających na rzecz Rosji przeprowadziły 61% cyberataków na świecie[21]. Największym katalizatorem takiej aktywności jest wojna w Ukrainie. Od początku 2022 r. różne podmioty deklarują wsparcie dla Rosji i działają w jej interesie, prowadząc cyberszpiegostwo, cybersabotaż i operacje informacyjne przeciwko krajom UE i NATO[22]. Powiązani z Rosją cyberprzestępcy dokonujący ataków na Europę i USA działają nie tylko z pobudek politycznych. Niektórzy z nich to Hunters International[23],

[19] *What is data exfiltration?*, IBM, https://www.ibm.com/think/topics/data-exfiltration [dostęp: 19.03.2025].

[20] *Microsoft Digital Defense Report 2024, The foundations and new frontiers of cybersecurity*, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024, s. 13 [dostęp: 19.03.2025].

[21] Thales Cyber Threat Intelligence, *From Ukraine to the whole of Europe: cyber conflict reaches a turning point*, Thales, 29.03.2023, https://www.thalesgroup.com/en/worldwide/security/press_release/ukraine-whole-europecyber-conflict-reaches-turning-point [dostęp: 8.04.2025].

[22] S.G. Jones, *Russia's Shadow War Against the West*, Center for Strategic & International Studies, 18.03.2025, https://www.csis.org/analysis/russias-shadow-war-against-west [dostęp: 19.03.2025].

[23] R. Wolert, *RaaS group profile Hunters International*, CERT Orange, 28.10.2024, https://cert.orange.pl/wp-content/uploads/2024/11/CERTOPL_CTI_Hunters_International_en.pdf [dostęp: 19.03.2025].

Hive[24] czy Conti[25]. Niezależnie od przypisania haktywisty czy grupy cyberprzestępczej do APT, w przypadku rosyjskiej aktywności w cyberprzestrzeni należy również rozważyć działania pod obcą flagą. Jeśli uwzględni się takie przykłady jak aktywność grupy identyfikującej się jako Cyber Berkut w 2014 r., działania Cyber Caliphate w 2015 r. i ataki ransomware w 2016 r. i 2017 r., wszystkie przypisywane rosyjskiemu wywiadowi wojskowemu GRU[26], to zasięg działania rosyjskich służb specjalnych może być szerszy niż można było początkowo przypuszczać.

Kolejnym poważnym źródłem cyberzagrożeń są Chiny, które realizują swoje cele polityczne i ideologiczne, m.in. dążą do uzyskania statusu supermocarstwa[27]. Działania hakerskie, które prowadzą, służą strategicznym celom ekonomicznym. Zgodnie z chińską strategią wojskową (...) *cyberprzestrzeń stała się nowym filarem rozwoju gospodarczego i społecznego*[28]. W ocenie ekspertów NATO (...) *Części chińskiego wojska stały się dla rządu użytecznymi narzędziami do prowadzenia politycznego i gospodarczego cyberszpiegostwa, a także do pomocy w zmniejszeniu technologicznych i strategicznych braków ChALW* [Chińskiej Armii Ludowo-Wyzwoleńczej] *w stosunku do konkurentów*[29]. Sektory gospodarki państw europejskich najbardziej narażone na ataki to: energetyka, telekomunikacja i transport[30].

---

[24] *Russian National Charged with Ransomware Attacks Against Critical Infrastructure*, U.S. Department of Justice, 16.05.2023, https://www.justice.gov/archives/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure [dostęp: 19.03.2025].

[25] *Multiple Foreign Nationals Charged in Connection with Trickbot Malware and Conti Ransomware Conspiracies*, U.S. Department of Justice, 7.09.2023, https://www.justice.gov/archives/opa/pr/multiple-foreign-nationals-charged-connection-trickbot-malware-and-conti-ransomware [dostęp: 19.03.2025].

[26] A. Greenberg, *A Brief History of Russian Hackers' Evolving False Flags*, Wired, 21.10.2019, https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/ [dostęp: 19.03.2025].

[27] A.H. Cordesman, *China's Emergence as a Superpower*, Center for Strategic & International Studies, 15.08.2023, https://www.csis.org/analysis/chinas-emergence-superpower [dostęp: 19.03.2025].

[28] *China's Military Strategy*, Ministry of National Defense of the People's Republic of China, 23.06.2021, http://eng.mod.gov.cn/xb/Publications/WhitePapers/4887928.html [dostęp: 19.03.2025].

[29] M. Raud, *China and Cyber: Attitudes, Strategies, Organization*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2016, https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf, s. 21 [dostęp: 19.03.2025].

[30] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*, w przygotowaniu.

Dania

Do jednego z największych cyberataków na duńską IK doszło w maju 2023 r. Aktor, którego nie wiąże się otwarcie z GRU, ale SektorCERT podejrzewa, że jest powiązany z grupą Sandworm[31], przeprowadził dokładny rekonesans przed atakiem. Mógł on obejmować, oprócz cyberszpiegostwa, również tradycyjne sposoby gromadzenia danych wywiadowczych. W raporcie SektorCERT poinformował, że w czasie ataku informacje o podatnych urządzeniach nie były dostępne w serwisach publicznych (takich jak Censys lub Shodan), co dowodzi, że atakujący uzyskali je w inny sposób[32]. Luka oprogramowania urządzenia brzegowego firmy Zyxel, która została wykorzystana podczas tego ataku (CVE-2023-28771), otrzymała ocenę 9,8 na 10. Czyni to z niej lukę krytyczną – łatwą do wykorzystania i pozwalającą na naruszenie bezpieczeństwa, które ma poważne konsekwencje. Podatne na ataki urządzenia wyprodukowane przez Zyxel były używane w tym czasie w dużej mierze przez niewielkich duńskich operatorów IK w ich środowiskach OT[33]. W sumie udało się zagrozić bezpieczeństwu 22 firm energetycznych, a kilka z nich odnotowało zakłócenia w działalności.

Najnowsza ocena Danii dotycząca zagrożeń hybrydowych ze strony Rosji jest taka, że (...) *wykorzystuje ona środki hybrydowe zarówno w okresie poprzedzającym bezpośredni konflikt zbrojny, jak i w jego trakcie* (...) *środki hybrydowe obejmują narzędzia polityczne, gospodarcze, informacyjne i wojskowe, które mogą być wykorzystywane w sposób skoordynowany w celu maksymalizacji ich wpływu*[34]. Duńska Służba Wywiadu Obronnego (dun. Forsvarets Efterretningstjeneste) wskazuje, że w rosyjskie operacje hybrydowe są angażowane zarówno władze państwowe, jak i podmioty prywatne, przy czym te pierwsze koordynują działania. W przypadku tego rodzaju operacji często jest ukrywane, kto za nimi stoi[35]. Duńskie Centrum Cyberbezpieczeństwa (dun. Center

[31] *The attack against Danish, critical infrastructure*, SektorCERT, listopad 2023, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf, s. 15 [dostęp: 19.03.2025].

[32] Tamże, s. 10.

[33] Operational technology – systemy i urządzenia wykorzystywane do monitorowania, kontrolowania i zarządzania procesami technologicznymi, takimi jak maszyny produkcyjne, pompy, urządzenia pomiarowe czy systemy zarządzania ruchem.

[34] *Intelligence Outlook 2024*, Danish Defence Intelligence Service, 22.01.2025, https://www.fe-ddis.dk/en/produkter/Risk_assessment/riskassessment/Intelligenceoutlook2024/, s. 26 [dostęp: 19.03.2025].

[35] Tamże.

for Cybersikkerhed), które obecny poziom zagrożenia i cele Rosji ocenia podobnie jak wywiad, wskazuje, że (...) *jest prawdopodobne, że sponsorowani przez państwo rosyjscy hakerzy prowadzą cyberszpiegostwo przeciwko duńskiej infrastrukturze krytycznej w ramach przygotowań do destrukcyjnych cyberataków w przyszłości*[36]. Jednocześnie podejrzewa się, że cyberszpiegostwo w celu uzyskania informacji na temat technologii i polityki prowadzą również Chiny. Centrum to jest zdania, że największe ryzyko cyberataków, które skutkują ofiarami śmiertelnymi lub rannymi, znacznymi szkodami materialnymi, zniszczeniem informacji, danych, oprogramowania czy manipulacją nimi, wiąże się z Rosją, a głównie z grupami sponsorowanymi przez państwo.

Niemcy

W maju 2023 r. niemiecka federalna minister spraw wewnętrznych stwierdziła: *Absolutnie nie damy się zastraszyć rosyjskiemu reżimowi*[37]. Słowa te padły w odniesieniu do cyberataków przeprowadzanych przez FR. Przyczyną takiej reakcji było podanie do wiadomości, że GRU i jego grupa zagrożeń APT28 stały za cyberatakami ze stycznia 2023 r. Celem tych ataków były systemy partii SPD oraz firm z sektora logistyki, obronności, lotnictwa i IT. Atak był możliwy ze względu na lukę w zabezpieczeniach programu Microsoft Outlook, która spowodowała, że nieautoryzowany aktor mógł uzyskać dostęp do kont e-mail tych podmiotów. Niemcy podtrzymały opinię, że ten atak był (...) *poważną ingerencją w struktury demokratyczne*[38]. Federalne Ministerstwo Spraw Wewnętrznych i Ojczyzny (niem. Bundesministerium des Innern und für Heimat) ocenia, że wojna w Ukrainie zmieniła sytuację bezpieczeństwa w Niemczech w taki sposób, że kraj ten potrzebuje lepszej ochrony i większej świadomości na temat podatności na cyberataki i rosyjską dezinformację[39].

[36] *Threat assessment: the cyber Threat against Denmark 2024*, Centre for Cyber Security, wrzesień 2024, https://www.cfcs.dk/link/472c3cc8872446e59fa59eaf0f7ad945.aspx, s. 8 [dostęp: 19.03.2025].

[37] *Cyber attacks traced to Russian military intelligence agency*, Federal Ministry of the Interior and Community, 3.05.2024, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html [dostęp: 19.03.2025].

[38] Tamże.

[39] *Heightened security situation in Germany*, Federal Ministry of the Interior and Community, https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/ukrain/security_meldung.html [dostęp: 19.03.2025].

Niemieckie służby wywiadowcze twierdzą, że rosyjskie działania szpiegowskie dotyczą rządu i administracji, a także wojska, technologii, badań, biznesu i przemysłu. *Rosyjskie cyberataki, niezależnie od tego, czy są skierowane na osoby fizyczne, organizacje czy instytucje rządowe, mają przede wszystkim na celu zdobycie stałego źródła informacji wywiadowczych. Oprócz takiego szpiegostwa, ataki te mogą być również wykorzystywane do sabotażu, operacji wywierania wpływu, dezinformacji lub celów propagandowych*[40].

W kwestii cyberzagrożeń ze strony Chin Niemcy uważają, że działania służb wywiadowczych służą realizacji celu Komunistycznej Partii Chin, którym jest status Chin jako globalnego lidera i światowej potęgi[41]. Federalny Urząd Ochrony Konstytucji (niem. Bundesamt für Verfassungsschutz) bezpośrednio wskazuje na grupy APT15 i APT31 jako wymagające uwagi ze względu na złożone techniki i narzędzia, jakimi się posługują. Na początku 2023 r. celem ataku na łańcuch dostaw przeprowadzonego przez sprawcę z Chin stali się niemieccy dostawcy usług IT dla sieci rządowych[42]. W raporcie nie sprecyzowano jednak, na czym ten atak polegał.

Estonia

Pierwszy cyberatak, o którym publicznie poinformowały estońskie władze, został przeprowadzony w 2020 r. przez GRU, a konkretnie Jednostkę 29155. Zespół CERT-EE, zajmujący się obsługą incydentów w estońskim Urzędzie ds. Systemów Informacyjnych, poinformował, że systemy komputerowe Ministerstwa Gospodarki i Komunikacji zostały naruszone za pomocą złośliwego oprogramowania typu backdoor. Spowodowało to wyciek 350 GB danych, w tym poufnych informacji wewnętrznych – dokumentów strategicznych i roboczych, danych osobowych i korespondencji z firmami[43]. Ten sam podmiot zaatakował także Ministerstwo Spraw Zagranicznych oraz Centrum Systemów Informacyjnych o Zdrowiu i Opiece Społecznej.

[40] *Brief summary 2023 Report on the Protection of the Constitution (Facts and Trends)*, Bundesamt für Verfassungsschutz, https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/reports-on-the-protection-of-the-constitution/2024-06-brief-summary-2023-report-on-the-protection-of-the-constitution.pdf, s. 60 [dostęp: 19.03.2025].

[41] Tamże.

[42] Tamże, s. 62.

[43] *Cyber Security in Estonia 2025*, Republic of Estonia Information System Authority, https://www.ria.ee/en/cyber-security-estonia-2025 [dostęp: 19.03.2025].

Podanie tych informacji do publicznej wiadomości i przypisanie ataków nastąpiło dopiero pod koniec 2024 r. w wyniku operacji Toy Soldier przeprowadzonej przez Estonię i kilka innych krajów. Dzięki niej połączono Jednostkę 29155 z wieloma cyberatakami na Ukrainę, kraje NATO i UE. *Cele komórki cybernetycznej GRU, Jednostki 29155, obejmują gromadzenie danych wywiadowczych, naruszanie dobrego imienia przez kradzież i wyciek poufnych informacji oraz systematyczny sabotaż przez niszczenie danych i systemów komputerowych*[44].

W 2023 r. CERT-EE opublikował szczegółową analizę ataków DDoS przeprowadzonych przez haktywistów w 2022 r., których celem były strony internetowe sektora publicznego, transportowego i finansowego Estonii. Ataki nasilały się w związku z pewnymi wydarzeniami, takimi jak przeniesienie radzieckich pomników w Narwie czy oświadczenie estońskiego parlamentu Riigikogu, że rosyjski reżim jest terrorystyczny[45]. CERT-EE ogłosił, że były to działania o marginalnym znaczeniu i dał do zrozumienia, że Estonia nie uznała ich za poważne zagrożenie, lecz za utrudnienie. Co najważniejsze, CERT-EE nie przypisał tych ataków Rosji, lecz ideologicznie zmotywowanym hakerom, dla których wojna była katalizatorem. Często były one wynikiem i działań niezgodnych z oficjalną rosyjską narracją.

Prezentując ogólne postrzeganie zagrożeń sponsorowanych w cyberprzestrzeni, estońska Służba Bezpieczeństwa Wewnętrznego (eston. Kaitsepolitseiamet, KAPO) stwierdziła, że wrogie działania cyberwywiadowcze są prowadzone zwykle przez (...) *wojskowe i specjalne jednostki cyberwywiadowcze wrogich państw, które wytrwale działają na rzecz interesów swojego kraju*[46]. Według KAPO (...) *zarówno instytucje państwowe, jak i firmy świadczące usługi kluczowe muszą zdawać sobie sprawę, że ich status jako takich czyni je potencjalnymi celami ataków* [cybernetycznego sabotażu][47]. KAPO uważa za wysoce prawdopodobne, że (...) *rosyjskie służby specjalne nadal będą próbowały uzyskać nielegalny dostęp do sieci komputerowych estońskich dostawców usług kluczowych oraz najważniejszych firm transportowych*

[44] Tamże.

[45] *Cyber Security in Estonia 2023*, Republic of Estonia Information System Authority, https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf, s. 17 [dostęp: 19.03.2025].

[46] *Annual review 2023–2024*, Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2023-2024.pdf, s. 26 [dostęp: 19.03.2025].

[47] Tamże.

i logistycznych w celu zebrania informacji i przygotowania się do zakłócenia ich działalności za pomocą środków cybernetycznych, jeśli zajdzie taka potrzeba[48].

Ważnym spostrzeżeniem dotyczącym nastawienia opinii publicznej i postrzegania przez nią aktorów prezentujących się jako niepaństwowi, takich jak cyberprzestępcy czy haktywiści, jest to, że (...) *rosyjskie służby specjalne również korzystają z usług hakerów, którzy są z nimi pośrednio powiązani i wydają się działać niezależnie*[49]. KAPO ocenia, że takie ataki o niskim poziomie zaawansowania i niewielkim wpływie, w przeciwieństwie do grup APT bezpośrednio powiązanych ze służbami specjalnymi, umożliwiają Rosji tworzenie iluzji silnego wsparcia i dużych możliwości[50].

Estonia wskazuje również na zagrożenia ze strony Chin. KAPO zwraca uwagę, że produkowana tam technologia może zawierać złośliwe oprogramowanie i sprzętowe backdoory, pozwalające Chińczykom na nieautoryzowany dostęp do estońskich sieci i urządzeń[51]. Dlatego pomimo konkurencyjnych cen tych technologii należy rozpatrywać rozwiązania pochodzące z Chin jako potencjalne zagrożenie dla informacji przetwarzanych w docelowych systemach i każdorazowo przeprowadzać analizę ryzyka wynikającego z ich zastosowania.

Litwa

Przed wojną w Ukrainie Litwa była jednym z głównych celów operacji „Ghostwriter", przypisywanej grupie UNC1151, w tamtym czasie łączonej z Rosją[52]. Działalność ta, prowadzona w dalszym ciągu, chociaż na mniejszą skalę, łączy w sobie dwie sfery – cyberataki i operacje informacyjne, w których zaatakowana infrastruktura jest wykorzystywana do szerzenia w społeczeństwie dezinformacji. Wiele operacji dotyczyło stosunków między Litwą a Polską, np. operacje informacyjne pod hasłem „Wyciek odpadów radioaktywnych z litewskiej elektrowni jądrowej stanowi

[48] *Annual review 2022–2023,* Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202022-23_0.pdf, s. 22 [dostęp: 19.03.2025].

[49] *Annual review 2023–2024*..., s. 26.

[50] Tamże, s. 27.

[51] *Annual review 2022–2023*..., s. 24.

[52] Obecnie eksperci uważają, że równie prawdopodobne są powiązania tej grupy i z Rosją, i z Białorusią. Możliwe jest również, że działa ona pod obcą flagą.

zagrożenie dla Polaków mieszkających w pobliżu granicy" czy „Polska szkoliła ekstremistów w celu destabilizacji Litwy", a także między Litwą a Niemcami lub USA[53]. W oświadczeniu z 23 września 2021 r. wiceminister obrony narodowej Margiris Abukevičius stwierdził, że (...) *Litwa zdecydowanie popiera wspólną deklarację Unii Europejskiej wydaną w ramach stanowczego potępienia cyberataków informacyjnych Ghostwritera powiązanych z Rosją, które są wymierzone w procesy demokratyczne, instytucje, polityków, przedstawicieli mediów i ogólnie społeczeństwa państw członkowskich UE*[54]. W 2023 r. litewskie służby wywiadowcze – Drugi Departament Służb Operacyjnych (lit. Antrojo Operatyvinių Tarnybų Departamento, AOTD) oraz Departament Bezpieczeństwa Państwa (lit. Valstybės Saugumo Departamentas, VSD) poinformowały, że cybernetyczne operacje informacyjne przeciwko Litwie prowadzone przez grupę Ghostwriter ustały z powodu przekierowania działań na Ukrainę.

Litewskie służby wywiadowcze oceniły, że w związku z masowymi wydaleniami rosyjskich dyplomatów, a właściwie oficerów rosyjskiego wywiadu działających pod przykryciem dyplomatycznym, Rosja będzie poszukiwać innych sposobów gromadzenia informacji i uprawiać m.in. cyberszpiegostwo. AOTD i VSD odnotowały, że ataki są coraz częstsze. Ich celem są przede wszystkim organizacje rządowe i infrastruktura krytyczna.

Litwa podobnie jak Estonia wskazuje na współpracę cyberprzestępców i nienadzorowanych przez państwo hakerów z rosyjskimi służbami specjalnymi. Przestępcy osiągają dzięki niej korzyści finansowe i mają technologiczne wsparcie, a państwa zyskują na tym, że przypisanie atrybucji staje się trudniejsze[55].

W 2024 r. Litwa skoncentrowała się w swoich raportach na zagrożeniu ze strony Chin. Wskazano, że (...) *ich aktywność w litewskiej cyberprzestrzeni wzrosła, szczególnie od 2021 r., kiedy to Litwa ogłosiła otwarcie*

[53] *GhostWriter Update: Cyber Espionage Group UNC1151 Likely Conducts GhostWriter Influence Activity*, Mandiant, 28.04.2021, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf, s. 12–14 [dostęp: 19.03.2025].

[54] *Lithuania supports the EU declaration condemning Ghostwriter malicious cyber activities and calls to use more political tools*, Ministerstwo Obrony Narodowej Republiki Litwy, 23.09.2021, https://kam.lt/en/lithuania-supports-the-eu-declaration-condemning-ghostwriter-malicious-cyber-activities-and-calls-to-use-more-political-tools/ [dostęp: 8.04.2025].

[55] *National Threat Assessment 2023*, https://kam.lt/wp-content/uploads/2023/03/Assessment-of-Threats-to-National-Security-2022-published-2023.pdf, s. 55 [dostęp: 19.03.2025].

przedstawicielstwa Tajwanu na Litwie[56]. Nastąpiła zmiana celów ataków – z sektora prywatnego na instytucje rządowe zajmujące się sprawami wewnętrznymi i polityką zagraniczną. Taktyka ewoluowała w kierunku inżynierii społecznej, działania są prowadzone za pośrednictwem sieci społecznościowych.

Łotwa

Łotewski rząd niechętnie ujawnia sprawców cyberataków, chociaż wskazuje sektory, które są najbardziej narażone. W 2022 r. ci sami aktorzy stojący za atakami na infrastrukturę Ukrainy próbowali zaatakować łotewskie podmioty z sektora telekomunikacyjnego i energetycznego. Ze względów bezpieczeństwa nazwy czy też powiązania atakujących nie zostały ujawnione[57]. Zgodnie z przewidywaniami łotewskiej Służby Bezpieczeństwa Państwowego (łot. Valsts drošības dienests, VDD) z 2022 r.[58] i potwierdzonymi zdarzeniami w latach 2023[59] i 2024[60] za atakami na łańcuchy dostaw przy użyciu sprzętu lub oprogramowania zainfekowanego złośliwym kodem, a także aktualizacji oprogramowania bądź usług serwisowych, stały grupy wywodzące się z Rosji i wspierane przez to państwo. Według Biura Ochrony Konstytucji (łot. Satversmes aizsardzības birojs, SAB) tego typu ataki na łańcuch dostaw były wymierzone m.in. w satelitę telewizyjnego łotewskiego operatora telekomunikacyjnego – firmę Tet. Skutkiem tych ataków była krótka emisja rosyjskiej propagandy. Hakerzy uzyskali również dostęp do serwerów wynajętych przez operatora telekomunikacyjnego – firmę Balticom, obsługiwanych przez zewnętrznego dostawcę usług z Bułgarii,

[56] *National Threat Assessment 2024*, https://www.vsd.lt/wp-content/uploads/2024/03/GR-2024-02-15-EN-1.pdf, s. 57 [dostęp: 19.03.2025].

[57] D. Antoniuk, *Latvia's cyberspace faces new challenges amid war in Ukraine*, The Record, 28.10.2022, https://therecord.media/latvias-cyberspace-faces-new-challenges-amid-war-in-ukraine [dostęp: 19.03.2025].

[58] *Annual Report on the activities of Latvian State Security Service (VDD) in 2022*, https://vdd.gov.lv/uploads/materials/33/en/annual-report-2022.pdf, s. 13–14 [dostęp: 19.03.2025].

[59] *Annual Report on the activities of Latvian State Security Service (VDD) in 2023*, https://vdd.gov.lv/uploads/materials/37/en/annual-report-2023.pdf, s. 15 [dostęp: 19.03.2025].

[60] *Annual report on the activities of Latvian State Security Service (VDD) in 2024*, https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf, s. 17 [dostęp: 19.03.2025].

i wyemitowali nagranie z rosyjskiej parady wojskowej[61]. W żadnym z tych przypadków infrastruktura nie znajdowała się na terenie Łotwy[62]. Niemniej jednak zespół CERT.LV podkreślił, że (...) *kluczowe jest zapobieganie zaangażowaniu łotewskiej infrastruktury IT w cyberataki oraz możliwości przeprowadzania ataków z terytorium kraju, ponieważ firmy telekomunikacyjne powiązane z Rosją celowo budują swoją obecność na Łotwie i w innych państwach członkowskich UE*[63].

Ataki naruszające infrastrukturę transmisyjną w celu szerzenia propagandy zacierają granice między cyberatakiem a operacją informacyjną, w której podmiot zostaje przejęty po to, aby wykorzystać jego zasięg i zaufanie, jakim się cieszy, do rozpowszechniania dezinformacji. W porównaniu z innymi metodami wykorzystywanymi w tego typu działaniach operacje informacyjne wspierane cyberatakami mogą znacznie szybciej dotrzeć do grupy docelowej, co dla sprawców czyni je atrakcyjnym narzędziem.

Podobnie jak inne kraje europejskie Łotwa również podziela przekonanie, że prorosyjscy haktywiści są (...) *prawdopodobnie koordynowani i finansowani w celu realizowania rosyjskich operacji wpływu, zarówno w polityce wewnętrznej, jak i zagranicznej*[64]. Jednocześnie, po przeanalizowaniu wydarzeń z 2022 r., VDD zweryfikowało, że informacje publikowane przez takie grupy na ich kanałach na Telegramie często są dezinformacją, ponieważ zgłaszane przez nie szkody w rzeczywistości nie zaistniały[65].

W odniesieniu do chińskiego wywiadu VDD ocenia, że Chiny nadal postrzegają Łotwę przede wszystkim jako część NATO i UE, które uznają za głównych rywali w globalnej rywalizacji o wpływy[66]. Gdy weźmie się to pod uwagę, ich cel jest jasny – jest nim gromadzenie informacji wywiadowczych na temat strategicznych decyzji i polityki dotyczącej relacji między Chinami a krajami przeciwnymi. Łotewskie służby wywiadowcze obserwują próby nawiązywania i wzmacniania przez przedstawicieli Chin

[61] *Latvia mulls tightening security after recent TV propaganda hacks*, LSM+, 20.05.2024, https://eng.lsm.lv/article/society/crime/20.05.2024-latvia-mulls-tightening-security-after-recent-tv-propaganda-hacks.a554618/ [dostęp: 19.03.2025].

[62] *2024 Annual Report*, Republic of Latvia Constitution Protection Bureau, https://www.sab.gov.lv/files/uploads/2025/02/SAB-gada-parskats_2024_ENG.pdf, s. 36 [dostęp: 19.03.2025].

[63] *Latvian Cybersecurity and CERT.LV Technical Activities Annual Report 2023*, 26.07.2024, https://cert.lv/uploads/eng/Annual_Report_CERT-LV_2023.pdf, s. 4–5 [dostęp: 19.03.2025].

[64] Tamże, s. 6.

[65] *Annual Report on the activities of Latvian State Security Service (VDD) in 2022...*, s. 13.

[66] Tamże.

pozytywnych relacji i wpływów wśród łotewskich polityków, naukowców i badaczy, co potwierdza ich zainteresowanie nowymi technologiami, innowacjami i polityką. Zainteresowanie to dotyczy również kwestii cybernetycznych – chińskie grupy cybernetyczne prowadzą działania hakerskie.

Polska

Polskie instytucje bezpieczeństwa państwa nie udostępniają informacji w formie okresowych raportów dotyczących kwestii strategicznych czy operacyjnych (jedynie raporty poświęcone zagadnieniom technicznym), dlatego w celu oceny stanowiska rządu wobec zagrożeń hybrydowych konieczne było sięgnięcie po doraźne komunikaty rzeczników bądź publikacje ukazujące się na oficjalnej stronie rządowej gov.pl.

Pod koniec 2022 r. ukazał się komunikat Pełnomocnika Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej Rzeczypospolitej Polskiej, w którym kilka cyberataków przypisano rosyjskim hakerom: (...) *przez wrogie operacje w cyberprzestrzeni Rosja chce wywierać presję na Polskę jako kraj frontowy i kluczowego sojusznika Ukrainy na wschodniej flance NATO*[67]. Obejmowały one ataki DDoS przeprowadzone przez prorosyjską grupę haktywistów NoName057(16) w odpowiedzi na uchwałę Sejmu RP z grudnia 2022 r. uznającą Rosję za państwo sponsorujące terroryzm[68], a także tworzenie stron do zbierania danych za pomocą phishingu.

Podobnie rzecznik prasowy ministra koordynatora służb specjalnych Polski stwierdził w połowie 2022 r.: *Operacje wywiadowcze polegające na atakach hakerskich, przejmowaniu zasobów informacyjnych i wykorzystywaniu ich do manipulowania opinią publiczną są w ostatnich latach wykorzystywane przez Kreml w ramach walki z NATO*[69]. Jednoznacznie przypisał więc te działania Rosji.

---

[67] *Russian cyberattacks*, Serwis Rzeczypospolitej Polskiej, 30.12.2022, https://www.gov.pl/web/special-services/russian-cyberattacks [dostęp: 19.03.2025].

[68] *Sejm uznał Rosję za państwo wspierające terroryzm*, Sejm Rzeczypospolitej Polskiej, 14.12.2022, https://www.sejm.gov.pl/sejm9.nsf/komunikat.xsp?documentId=4774505381CECC-10C1258918007022FA [dostęp: 8.04.2025].

[69] *Ataki hakerskie na RP operacją rosyjskich służb*, Serwis Rzeczypospolitej Polskiej, 20.07.2022, https://www.gov.pl/web/sluzby-specjalne/ataki-hakerskie-na-rp-operacja-rosyjskich-sluzb [dostęp: 19.03.2025].

Rok 2024 był pierwszym, w którym sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa za poprzedni rok zostało przedstawione publicznie[70]. Wcześniej był to w pełni tajny dokument. Tym samym, wraz z corocznymi raportami CERT Polska i CSIRT GOV, stało się jednym z nielicznych oficjalnych źródeł podsumowujących rok 2023.

W miesiącach poprzedzających wybory parlamentarne w 2023 r. grupa hakerska UNC1151 kontynuowała spersonalizowane ataki phishingowe (spearphishing) wymierzone w polityków, personel wojskowy, dziennikarzy, prawników oraz inne osoby mogące mieć powiązania z Rosją i Białorusią. Celem tych kampanii było cyberszpiegostwo i dezinformacja i w raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 r. zostały one przypisane Białorusi. Ta sama grupa jest podejrzewana o przeprowadzenie operacji informacyjnej wspieranej cyberatakami tuż przed wyborami, w ramach której wykorzystywano e-maile, wiadomości tekstowe oraz ekrany informacyjne w centrach handlowych do szerzenia dezinformacji[71].

Minister cyfryzacji nie wskazał bezpośrednio sprawców, ale zasugerował, że cyberatak na Polską Agencję Prasową i fałszywa depesza o częściowej mobilizacji w Polsce, która to informacja została opublikowana na stronie PAP w wyniku włamania, ma rosyjskie źródło. Minister stwierdził, że celem tego incydentu było (...) *szerzenie dezinformacji przed wyborami i „sparaliżowanie" społeczeństwa*[72]. Chodziło o wybory do Parlamentu Europejskiego w 2024 r.

Raportowanie w Polsce koncentruje się głównie na samych incydentach, np. przypadkach e-maili phishingowych rozsyłanych przez grupy APT powiązane z Rosją, takie jak APT28, APT29 czy Gamaredon, w celu prowadzenia cyberszpiegostwa. Krajowe zespoły CSIRT prezentują te incydenty w swoich raportach. W Polsce o zagrożeniach hybrydowych niewiele się mówi z perspektywy kontrwywiadu, mimo że jeden z krajowych zespołów CSIRT działa w strukturach Agencji Bezpieczeństwa Wewnętrznego.

[70] *Sprawozdanie Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za 2023 rok*, Ministerstwo Cyfryzacji, 11.04.2024, https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni [dostęp: 8.04.2025].

[71] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku*, CSIRT GOV, https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf, s. 6 [dostęp: 19.03.2025].

[72] *Fake PAP report looks like cyberattack, says gov't official*, Polska Agencja Prasowa, 31.05.2024, https://www.pap.pl/en/news/fake-pap-report-looks-cyberattack-says-govt-official [dostęp: 19.03.2025].

Na temat zagrożeń pochodzących z Chin w Polsce publikuje się nieliczne informacje. W źródłach rządowych można znaleźć jedynie kilka przykładów takich incydentów. Ocena sytuacji w 2023 r. wskazywała, że ze względu na poziom współpracy propagandowej między Chinami a Rosją (...) *należy oczekiwać, że zainteresowanie i aktywność chińskiego wywiadu nie ulegną zmianie, głównie ze względu na skalę wsparcia, jakie Rzeczpospolita Polska udziela Ukrainie w odpieraniu rosyjskiej agresji, sojusz Warszawy z Waszyngtonem oraz sytuację wokół Tajwanu*[73].

Wnioski

Wyniki zaprezentowanych badań przedstawiają szczegółowy przegląd aktualnych zagrożeń cybernetycznych, z którymi mierzy się Unia Europejska. Analizowane państwa prezentują stanowisko, że od początku wojny w Ukrainie w 2022 r. ataki z Rosji nasilają się i nie ma sygnałów wskazujących, że mogą osłabnąć. Wręcz przeciwnie, możliwości aktorów będących źródłem zagrożeń ewoluują wraz z ich doświadczeniem, a ataki stają się coraz trudniej wykrywalne i coraz bardziej wyrafinowane. W przypadku Chin jednogłośna opinia jest taka, że zagrożenia pochodzące z tego kraju intensyfikują się i mogą się przekształcić z gromadzenia informacji w działania destrukcyjne. Dwa pozostałe państwa z Wielkiej Czwórki[74], czyli Iran i Korea Północna, rzadko są wspominane w kontekście zagrożeń cybernetycznych.

Strategie dotyczące raportowania i przypisywania ataków przyjęte w analizowanych krajach można podzielić na 3 kategorie: minimalna, ostrożna i bezpośrednia. Łotwa w przypadku ataków na swój sektor telekomunikacyjny i energetyczny jedynie informowała, że ten sam aktor stał za atakami na infrastrukturę Ukrainy. Skłaniała opinię publiczną ku przekonaniu, że był on powiązany z Rosją, ale nie wskazała go bezpośrednio. Dania ostrożnie wskazywała nazwę grupy potencjalnie stojącej za atakiem na infrastrukturę krytyczną, przy czym podkreślała dużą niepewność i poszlakowość atrybucji. Niemcy natomiast bezpośrednio przypisały ataki

[73] *China's propaganda offensive*, 17.02.2023, https://www.gov.pl/web/special-services/Chinas-propaganda-offensive [dostęp: 19.03.2025].

[74] Wielka Czwórka (ang. Big Four) aktorów państwowych, tj. Chiny, Rosja, Korea Północna, Iran, to grupa państw identyfikowanych przez analityków cyberbezpieczeństwa jako największe źródła zagrożeń w cyberprzestrzeni.

na różne sektory grupie APT28 kierowanej przez GRU i otwarcie mówiły o rosyjskiej aktywności. Jednocześnie rodzą się pytania o to, ile podobnych ataków nie upubliczniono. Ile zakłóceń raportowanych jako wypadki i awarie w rzeczywistości było poważnymi cyberatakami ze strony zagranicznych aktorów?

Każdy raport dotyczący szczegółów ataków jest ważnym źródłem informacji dla analityków cyberbezpieczeństwa, a każdy raport służb wywiadowczych poszerza wiedzę badaczy bezpieczeństwa i umożliwia lepsze zrozumienie krajobrazu zagrożeń nie tylko w pojedynczym kraju, lecz także w całym regionie. Bardzo ważne jest, aby dla dobra wspólnego Europa wypracowała jednolite i spójne stanowisko wobec zagrożeń cybernetycznych.

Bibliografia

Fukuyama F., *Zaufanie. Kapitał społeczny a droga do dobrobytu*, Warszawa 1997.

Jordan T., Taylor P., *Hacktivism and Cyberwars. Rebels with a cause?*, London 2004.

Kose J., *Cyber Warfare: An Era of Nation-State actors And Global Corporate Espionage*, „ISSA Journal" 2021, t. 19, nr 4, s. 12–15.

Kuehl D.T., *Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age*, „International Law Studies" 2022, t. 76, s. 35–58.

Lin H., Kerr J., *On Cyber-Enabled Information/Influence Warfare and Manipulation*, w: *The Oxford Handbook of Cyber Security*, P. Cornish (red.), Oxford University Press 2021, s. 251–272. https://doi.org/10.1093/oxfordhb/9780198800682.013.15.

McIntosh T. i in., *Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration*, „ACM Computing Surveys" 2024, t. 57, nr 1. https://doi.org/10.1145/3691340.

Vićić J., Harknett R., *Identification-imitation-amplification: understanding divisive influence campaigns through cyberspac*e, „Intelligence and National Security" 2024, t. 39, nr 5, s. 897–914. https://doi.org/10.1080/02684527.2023.2300933.

Źródła internetowe

Antoniuk D., *Latvia's cyberspace faces new challenges amid war in Ukraine*, The Record, 28.10.2022, https://therecord.media/latvias-cyberspace-faces-new-challenges-amid-war-in-ukraine [dostęp: 19.03.2025].

Ataki hakerskie na RP operacją rosyjskich służb, Serwis Rzeczypospolitej Polskiej, 20.07.2022, https://www.gov.pl/web/sluzby-specjalne/ataki-hakerskie-na-rp-operacja-rosyjskich-sluzb [dostęp: 19.03.2025].

Brief summary 2023 Report on the Protection of the Constitution (Facts and Trends), Bundesamt fur Verfassungsschutz, https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/reports-on-the-protection-of-the-constitution/2024-06-brief-summary-2023-report-on-the-protection-of-the-constitution.pdf [dostęp: 19.03.2025].

China's propaganda offensive, 17.02.2023, https://www.gov.pl/web/special-services/Chinas-propaganda-offensive [dostęp: 19.03.2025].

Cordesman A.H., *China's Emergence as a Superpower*, Center for Strategic & International Studies, 15.08.2023, https://www.csis.org/analysis/chinas-emergence-superpower [dostęp: 19.03.2025].

Countering hybrid threats, NATO, 7.05.2024, https://www.nato.int/cps/en/natohq/topics_156338.htm [dostęp: 19.03.2025].

Cyber attacks against European energy & utility companies, EnergiCERT, wrzesień 2022, https://sektorcert.dk/wp-content/uploads/2022/09/Attacks-against-European-energy-and-utility-companies-2020-09-05-v3.pdf [dostęp: 8.04.2025].

Cyber attacks traced to Russian military intelligence agency, Federal Ministry of the Interior and Community, 3.05.2024, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html [dostęp: 19.03.2025].

Cybercrime, European Commission, 31.10.2024, https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en [dostęp: 19.03.2025].

Cybersecurity of Critical Sectors – Energy, ENISA, https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/energy [dostęp: 8.04.2025].

Fake PAP report looks like cyberattack, says gov't official, Polska Agencja Prasowa, 31.05.2024, https://www.pap.pl/en/news/fake-pap-report-looks-cyberattack-says-govt-official [dostęp: 19.03.2025].

Frequently asked questions on hybrid threats, Hybrid CoE, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [dostęp: 19.03.2025].

Greenberg A., *A Brief History of Russian Hackers' Evolving False Flags*, Wired, 21.10.2019, https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/ [dostęp: 19.03.2025].

Heightened security situation in Germany, Federal Ministry of the Interior and Community, https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/ukrain/security_meldung.html [dostęp: 19.03.2025].

Intelligence Outlook 2024, Danish Defence Intelligence Service, 22.01.2025, https://www.fe-ddis.dk/link/905eb443324b4db1be29f0546e275183.aspx [dostęp: 19.03.2025].

Jones S.G., *Russia's Shadow War Against the West*, Center for Strategic & International Studies, 18.03.2025, https://www.csis.org/analysis/russias-shadow-war-against-west [dostęp: 19.03.2025].

Latvia mulls tightening security after recent TV propaganda hacks, LSM+, 20.05.2024, https://eng.lsm.lv/article/society/crime/20.05.2024-latvia-mulls-tightening-security-after-recent-tv-propaganda-hacks.a554618/ [dostęp: 19.03.2025].

Lithuania supports the EU declaration condemning Ghostwriter malicious cyber activities and calls to use more political tools, Ministerstwo Obrony Narodowej Republiki Litwy, 23.09.2021, https://kam.lt/en/lithuania-supports-the-eu-declaration-condemning-ghostwriter-malicious-cyber-activities-and-calls-to-use-more-political-tools/ [dostęp: 8.04.2025].

Mandiant Intelligence, *GhostWriter Update: Cyber Espionage Group UNC1151 Likely Conducts GhostWriter Influence Activity*, Mandiant, 28.04.2021, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf [dostęp: 19.03.2025].

Mandiant Intelligence, *Hacktivists Collaborate with GRU-sponsored APT28*, Mandiant, 23.09.2022, https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions [dostęp: 19.03.2025].

Microsoft Digital Defense Report 2024, *The foundations and new frontiers of cybersecurity*, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024 [dostęp: 19.03.2025].

Multiple Foreign Nationals Charged in Connection with Trickbot Malware and Conti Ransomware Conspiracies, U.S. Department of Justice, 7.09.2023, https://www.justice.gov/archives/opa/pr/multiple-foreign-nationals-charged-connection-trickbot-malware-and-conti-ransomware [dostęp: 19.03.2025].

Raud M., *China and Cyber: Attitudes, Strategies, Organization*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2016, https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf [dostęp: 19.03.2025].

Roncone G. i in., *APT44: Unearthing Sandworm*, Mandiant, 17.04.2024, https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf [dostęp: 19.03.2025].

Russian cyberattacks, Serwis Rzeczypospolitej Polskiej, 30.12.2022, https://www.gov.pl/web/special-services/russian-cyberattacks [dostęp: 19.03.2025].

Russian National Charged with Ransomware Attacks Against Critical Infrastructure, U.S. Department of Justice, 16.05.2023, https://www.justice.gov/archives/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure [dostęp: 19.03.2025].

Sancho D., *Understanding Hacktivists. The Overlap of Ideology and Cybercrime*, Trend Micro, 4.02.2025, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/understanding-hacktivists-the-overlap-of-ideology-and-cybercrime [dostęp: 19.03.2025].

Sejm uznał Rosję za państwo wspierające terroryzm, Sejm Rzeczypospolitej Polskiej, 14.12.2022, https://www.sejm.gov.pl/sejm9.nsf/komunikat.xsp?documentId=4774505381CECC10C1258918007022FA [dostęp: 8.04.2025].

Thales Cyber Threat Intelligence, *From Ukraine to the whole of Europe: cyber conflict reaches a turning point*, Thales, 29.03.2023, https://www.thalesgroup.com/en/worldwide/security/press_release/ukraine-whole-europecyber-conflict-reaches-turning-point [dostęp: 8.04.2025].

The attack against Danish, critical infrastructure, SektorCERT, listopad 2023, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf [dostęp: 19.03.2025].

What is data exfiltration?, IBM, https://www.ibm.com/think/topics/data-exfiltration [dostęp: 19.03.2025].

Wolert R., *RaaS group profile Hunters International*, CERT Orange, 28.10.2024, https://cert.orange.pl/wp-content/uploads/2024/11/CERTOPL_CTI_Hunters_International_en.pdf [dostęp: 19.03.2025].

Inne dokumenty

2024 Annual Report, Republic of Latvia Constitution Protection Bureau, https://www.sab.gov.lv/files/uploads/2025/02/SAB-gada-parskats_2024_ENG.pdf [dostęp: 19.03.2025].

Annual Report on the activities of Latvian State Security Service (VDD) in 2022, https://vdd.gov.lv/uploads/materials/33/en/annual-report-2022.pdf [dostęp: 19.03.2025].

Annual Report on the activities of Latvian State Security Service (VDD) in 2023, https://vdd.gov.lv/uploads/materials/37/en/annual-report-2023.pdf [dostęp: 19.03.2025].

Annual report on the activities of Latvian State Security Service (VDD) in 2024, https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf [dostęp: 19.03.2025].

Annual review 2022–2023, Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202022-23_0.pdf [dostęp: 19.03.2025].

Annual review 2023–2024, Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2023-2024.pdf [dostęp: 19.03.2025].

China's Military Strategy, Ministry of National Defense of the People's Republic of China, 23.06.2021, http://eng.mod.gov.cn/xb/Publications/WhitePapers/4887928.html [dostęp: 19.03.2025].

Cyber Security in Estonia 2023, Republic of Estonia Information System Authority, https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf [dostęp: 19.03.2025].

Cyber Security in Estonia 2025, Republic of Estonia Information System Authority, https://www.ria.ee/en/cyber-security-estonia-2025 [dostęp: 19.03.2025].

Latvian Cybersecurity and CERT.LV Technical Activities Annual Report 2023, 26.07.2024, https://cert.lv/uploads/eng/Annual_Report_CERT-LV_2023.pdf [dostęp: 19.03.2025].

National Threat Assessment 2023, https://kam.lt/wp-content/uploads/2023/03/Assessment-of-Threats-to-National-Security-2022-published-2023.pdf [dostęp: 19.03.2025].

National Threat Assessment 2024, https://www.vsd.lt/wp-content/uploads/2024/03/GR-2024-02-15-EN-1.pdf [dostęp: 19.03.2025].

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku, CSIRT GOV, https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf [dostęp: 19.03.2025].

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku, w przygotowaniu.

Sprawozdanie Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za 2023 rok, Ministerstwo Cyfryzacji, 11.04.2024, https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni [dostęp: 8.04.2025].

Threat assessment: the cyber Threat against Denmark 2024, Centre for Cyber Security, wrzesień 2024, https://www.cfcs.dk/link/472c3cc8872446e59fa59eaf0f7ad945.aspx [dostęp: 19.03.2025].

Wspólny komunikat do Parlamentu Europejskiego i Rady. Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym, Bruksela, 6.04.2016, JOIN(2016) 18 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52016JC0018 [dostęp: 19.03.2025].

Monika Stodolnik

Funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Kontakt: monika.stodolnik@abw.gov.pl