Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 34, s. 147–171

https://doi.org/10.4467/20801335PBW.26.007.23369

ARTYKUŁ

Ataki hybrydowe przeciwko Rzeczypospolitej Polskiej prowadzone i koordynowane przez Federację Rosyjską i ich związek z wojną w Ukrainie

Hybrid attacks against the Republic of Poland conducted and coordinated by the Russian Federation and their link to the war in Ukraine

AGATA RYTEL

Szkoła Główna Handlowa w Warszawie

https://orcid.org/0009-0008-1506-1822

Abstrakt Celem artykułu jest opis ataków i działań hybrydowych ze strony Federacji Rosyjskiej wymierzonych w Rzeczpospolitą Polską, które zostały przeprowadzone od czerwca 2021 r. do końca 2024 r. Przedstawiono je z rozróżnieniem na ataki godzące w nienaruszalność polskiej granicy z Białorusią, ataki prowadzone w polskiej cyberprzestrzeni oraz ataki dezinformacyjne w polskiej przestrzeni informacyjnej. Teza przyjęta w artykule zakłada, że działania te miały bezpośredni związek z wojną w Ukrainie i były intencjonalną ingerencją Rosji i Białorusi. Przeanalizowano literaturę przedmiotu dotyczącą teorii wojny hybrydowej oraz aktywności Federacji Rosyjskiej i Białorusi postrzeganych jako elementy wojny hybrydowej. Ponadto przeanalizowano informacje na temat wrogich działań przeciwko Rzeczypospolitej Polskiej, udostępnione przez polskie instytucje państwowe i zespoły powołane do reagowania na incydenty komputerowe.

Słowa kluczowe ataki hybrydowe, wojna hybrydowa, nielegalna migracja, cyberprzestrzeń, dezinformacja

Abstract

The aim of this article is to describe attacks and hybrid activities the Russian Federation against the Republic of Poland between June 2021 and the end of 2024. They are presented with a distinction between attacks against the integrity of the Polish border with Belarus, attacks carried out in Polish cyberspace, and disinformation attacks in the Polish information space. The thesis adopted in the article assumes that these actions were directly related to the war in Ukraine and were intentional interference by Russia and Belarus. The literature on the theory of hybrid warfare and the actions carried out by the Russian Federation and Belarus, perceived as part of hybrid warfare, was analysed. Furthermore, information related to hostile actions against the Republic of Poland, made available by Polish state institutions and teams set up to respond to computer incidents, was analysed.

Keywords

hybrid attacks, hybrid warfare, illegal migration, cyberspace, disinformation

Wprowadzenie

Sytuacja geopolityczna w Europie i na świecie w ostatnich latach znacznie się zmieniła, m.in. z powodu coraz bardziej jawnych dążeń imperialistycznych Federacji Rosyjskiej. Obecne wydarzenia (wojna w Ukrainie, ataki hybrydowe skierowane przeciwko Polsce) są związane z dynamicznym rozwojem technologii sieciowych i bezprecedensowym wpływem cyberprzestrzeni na funkcjonowanie państw i społeczeństw. Rozwój narzędzi, jakie oferuje cyberprzestrzeń, sprzyja działaniom hybrydowym. Rosja sukcesywnie rozwija metody prowadzenia wrogich, pozostających poniżej progu wojny działań wobec innych państw. Są to działania nieregularne na terytorium atakowanego państwa oraz działania polegające na atakowaniu jego cyberprzestrzeni i sfery informacyjnej. Cele FR to osłabienie państwa, dezorganizacja, podważenie zaufania do rządu i instytucji publicznych oraz polaryzacja społeczeństwa. Nasilenie ataków hybrydowych na Polskę ze strony rosyjskiej zaobserwowano wraz z wybuchem pełnoskalowej wojny w Ukrainie. Nagły wzrost liczby ataków na polską cyberprzestrzeń oraz infosferę nastąpił wraz z kryzysem migracyjnym na granicy polsko-białoruskiej w 2021 r.

W literaturze przedmiotu niewiele jest publikacji, w których zestawione zostały różne metody ataków hybrydowych przeprowadzanych przez Rosję wobec Polski. Ze względu na tempo rozwoju technologii, a także wpływ cyberprzestrzeni

i infosfery (często wykorzystywanych do ataków hybrydowych) na funkcjonowanie państwa i społeczeństwa budowanie świadomości o przedmiocie badań wydaje się fundamentalne.

Celem artykułu[1] jest opis ataków i działań hybrydowych ze strony FR godzących w bezpieczeństwo narodowe i cyberprzestrzeń Rzeczypospolitej Polskiej, które przeprowadzono od czerwca 2021 r. do grudnia 2024 r. Teza przyjęta w artykule zakłada, że ataki na nienaruszalność granicy Polski przeprowadzone przez FR przy pomocy Białorusi miały związek z wojną w Ukrainie oraz że działania hybrydowe wymierzone w Polskę przed wojną i w jej trakcie były intencjonalną, systemową ingerencją Rosji i Białorusi. Aby zrealizować założenia badawcze, zastosowano takie metody, jak analiza, synteza i wnioskowanie. Przeanalizowano literaturę przedmiotu, raporty opracowane przez polskie instytucje państwowe, a także oficjalne informacje związane z wrogimi działaniami wymierzonymi w RP, udostępnione przez zespoły powołane do reagowania na incydenty komputerowe.

Teoria wojny hybrydowej

Wojna hybrydowa jest połączeniem wojny w rozumieniu klasycznym oraz innych typów działań. Mogą one występować zarówno niezależnie, jak i równolegle czy bezpośrednio po sobie. Taki schemat stwarza atakującemu szerokie możliwości, a co za tym idzie – generuje duży zbiór zagrożeń, z jakimi musi się zmagać atakowany.

Należy zaznaczyć, że definicje pojęć dotyczących wojny hybrydowej są różne w państwach zachodnich i FR. Rosyjska teoria jest stworzona w opozycji do teorii wypracowanej w Stanach Zjednoczonych i Europie Zachodniej. Zabieg przenoszenia terminologii na grunt rosyjski ma podkreślać jej „obronny" charakter[2]. Najczęściej przywoływanym zachodnim teoretykiem wojny hybrydowej jest pochodzący ze Stanów Zjednoczonych Frank G. Hoffman, który zauważa, że wojny tego rodzaju nie są nowe, lecz za każdym razem są inne[3]. Według niego taki rodzaj konfliktu cechuje się (…) *zbieżnością* (…) *fizyczną i psychologiczną, kinetyczną i niekinetyczną, bojowników i cywilów* (…), *sił zbrojnych i społeczności, państw i aktorów niepaństwowych,*

[1] Artykuł powstał na podstawie pracy dyplomowej pt. *Ataki hybrydowe prowadzone i koordynowane przez Federację Rosyjską przeciwko Rzeczypospolitej Polskiej w kontekście wojny w Ukrainie*, napisanej pod kierunkiem dr. hab. Jerzego Surmy, profesora Szkoły Głównej Handlowej (SGH) w Warszawie. Praca została obroniona w 2025 r. w ramach studiów podyplomowych w SGH na kierunku zarządzanie cyberbezpieczeństwem (przyp. red.).

[2] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja Krymska – studium przypadku*, Warszawa 2014, s. 11.

[3] F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007, s. 8.

a także zdolności bojowych, w które są wyposażone[4]. Pojęcie zbieżności w kontekście teorii przedstawionej przez Hoffmana można rozumieć jako jednoczesne występowanie i wzajemne przenikanie się elementów militarnych i niemilitarnych w działaniach charakterystycznych dla wojen hybrydowych.

Olga Wasiuta i Sergiusz Wasiuta prezentują inne cechy wojny hybrydowej wskazywane w amerykańskiej teorii. Są to:

- połączenie wojny konwencjonalnej, działań nieregularnych, wojny informacyjnej i cyberwojny,
- przeprowadzanie ataków przy użyciu różnych metod i narzędzi,
- stosowanie kombinacji broni i działań nieregularnych (wojny partyzanckiej, terroryzmu, przestępczości),
- złożona, dynamiczna i elastyczna przestrzeń pola walki,
- szybka reakcja i adaptacja uczestników do dynamiki konfliktu,
- stosowanie nowoczesnych technologii, działań i metod mobilizacji[5].

Za głównego rosyjskiego badacza teorii wojny hybrydowej uważa się Walerija Gierasimowa. Pomimo że nie używa on w swoich rozważaniach pojęcia wojny hybrydowej, to wskazuje na charakterystyczne dla tego zjawiska elementy, tj. konieczność wykorzystania w nowoczesnych konfliktach rozmaitych instrumentów politycznych, ekonomicznych i humanitarnych oraz połączenia ich z manipulowaniem nastrojami społeczności zamieszkującej teren adwersarza. Działania te mają być wspierane przez środki pozamilitarne takie jak wojna informacyjna i operacje jednostek specjalnych. W późniejszej fazie konfliktu dopuszcza się wykorzystanie oddziałów zbrojnych, jednak pod postacią misji pokojowych czy humanitarnych[6].

Andrzej Krzak opisał również inne definicje wojny hybrydowej obecne w rosyjskiej literaturze przedmiotu. Zgodnie z jedną z przytoczonych przez niego teorii wojna hybrydowa charakteryzuje się mnogością różnego rodzaju działań, prowadzonych w sposób konwencjonalny (klasyczny) i nieregularny, przy wsparciu segmentu pozamilitarnego. W myśl kolejnej rosyjskiej teorii wojna hybrydowa ma charakteryzować się w stosunkach międzynarodowych kompleksowym i metodycznym oddziaływaniem zarówno militarnym, jak i politycznym, ekonomicznym i społecznym. W jeszcze innym rosyjskim ujęciu wojny hybrydowej, tym razem w kontekście wojskowo-politycznym, jest to zastosowanie na terytorium potencjalnego

[4] F.G. Hoffman, *Hybrid Warfare and Challenges*, „Joint Force Quarterly" 2009, nr 52, s. 34. Tłumaczenia w artykule pochodzą od autorki (dop. red.).

[5] O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Kraków 2017, s. 56–57.

[6] A. Krzak, *Wojny przyszłości po rosyjsku – wojna hybrydowa, informacyjna i psychologiczna na tle konfliktu ukraińskiego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 18, s. 25.

przeciwnika różnorodnej taktyki wojskowej i politycznej, a także działań destabilizacyjnych o charakterze społeczno-ekonomicznym[7].

Federacja Rosyjska swoją doktrynę wojny hybrydowej zamienia w rzeczywiste działania podejmowane wobec innych państw, a w związku z wybuchem wojny w Ukrainie zwłaszcza wobec RP. Rosyjskie działania noszące znamiona wojny hybrydowej wymierzonej przeciwko Polsce można podzielić na trzy kluczowe obszary: kryzys migracyjny, ataki w cyberprzestrzeni oraz kampanie dezinformacyjne. Działania te są skoordynowane w czasie, pod względem wykorzystywanych narzędzi, podmiotów je przeprowadzających oraz celów. Pomimo starań Rosji o odsunięcie od siebie winy i odpowiedzialności za ataki polskie służby i eksperci[8] w wielu przypadkach jednoznacznie przypisali sprawstwo stronie rosyjskiej i białoruskiej oraz ujawnili ich motywacje i wrogie dążenia.

Ataki na nienaruszalność polskiej granicy z Białorusią

Kryzys migracyjny, z którym Polska mierzy się od 2021 r., jest elementem działań hybrydowych prowadzonych przez Rosję przy pomocy Białorusi. Jest on organizowany i zarządzany przez reżim Aleksandra Łukaszenki, wykorzystujący migrantów jako narzędzia politycznego nacisku. Ataki wymierzone w nienaruszalność polskiej granicy, wspierane wrogimi działaniami dezinformacyjnymi, mają na celu destabilizację bezpieczeństwa Polski i Unii Europejskiej, wywarcie presji politycznej, polaryzację i zantagonizowanie społeczeństwa, a także stwarzają możliwość wprowadzenia na teren UE terrorystów i innego rodzaju przestępców[9].

Migranci, będący podmiotem działań hybrydowych, które koordynują reżimy Białorusi i Rosji, codziennie podejmują próby nielegalnego przekraczania polskiej granicy z Białorusią[10]. Granica polsko-białoruska jest jednocześnie częścią wschodniej granicy UE, strefy Schengen oraz NATO. Pierwszym krajem dotkniętym kryzysem migracyjnym wywołanym przez Rosję i Białoruś była Litwa, która musiała zmierzyć się z nim już w lipcu i sierpniu 2021 r. Przytoczone poniżej dane wskazują, że w tym samym czasie, kiedy trwał kryzys migracyjny na granicy

[7] Tamże, s. 18–19.

[8] Zob. szerzej: *Hybrydowa agresja Białorusi na UE*, Serwis Rzeczypospolitej Polskiej, 9 XI 2021 r., https://www.gov.pl/web/sluzby-specjalne/hybrydowa-agresja-bialorusi-na-ue [dostęp: 3 VI 2025]; M. Marek, *Wojna informacyjna Federacji Rosyjskiej przeciwko Ukrainie, Polsce i NATO*, Warszawa 2025.

[9] *Hybrydowy atak na Polskę*, Serwis Rzeczypospolitej Polskiej, 9 VIII 2022 r., https://www.gov.pl/web/sluzby-specjalne/hybrydowy-atak-na-polske [dostęp: 30 V 2025].

[10] *Wojna Federacji Rosyjskiej z Zachodem*, M. Banasik (red. nauk.), Warszawa 2022, s. 126.

Polski z Białorusią, Straż Graniczna odnotowała zwiększoną liczbę prób nielegalnego przekroczenia granicy polsko-litewskiej przez obywateli państw trzecich[11].

Jak informował rzecznik koordynatora służb specjalnych, w organizację działań związanych z kolejnym etapem wojny hybrydowej jest zaangażowany niemal cały aparat państwowy białoruskiego reżimu. Schemat organizacyjny szlaku nielegalnej migracji rozpoczyna się od wystawiania migrantom zaproszeń przez specjalne biura podróży oraz wiz „turystycznych" przez Ministerstwo Spraw Zagranicznych Białorusi. Następnie migranci docierają na Białoruś państwowymi białoruskimi liniami lotniczymi, które specjalnie w tym celu utworzyły nowe połączenia. Z lotnisk migranci są przemieszczani na granicę z Polską[12]. Tam białoruskie służby wspierają działania migrantów, którzy podejmują próby siłowego przekraczania granicy, atakują polskich funkcjonariuszy służących przy granicy i niszczą infrastrukturę[13].

Eskalacja agresywnych działań migrantów na granicy polsko-białoruskiej nastąpiła 8 listopada 2021 r. Próbowali oni siłą przedrzeć się na stronę polską, niszczyli ogrodzenie, przy czynnym wsparciu białoruskich służb[14]. Do kolejnej napastliwej próby nielegalnego masowego przekroczenia granicy przez cudzoziemców doszło 16 listopada na terenie przejścia granicznego w Kuźnicy.

Napięcie na granicy dodatkowo zwiększały różnego rodzaju prowokacje stosowane przez funkcjonariuszy białoruskiego reżimu. Dokonywali oni wobec polskich funkcjonariuszy i żołnierzy napaści słownych, rzucali w nich kamieniami, próbowali ogłuszać petardami, oślepiać reflektorami i laserami. Powszechne były prowokacje polegające na oddawaniu przez białoruskie służby strzałów przy granicy, przekraczanie jej przez umundurowane osoby z bronią długą, a nawet celowanie z broni do polskich żołnierzy i funkcjonariuszy pełniących służbę na granicy[15].

W 2021 r. Straż Graniczna odnotowała 2869 cudzoziemców będących obywatelami państw trzecich (spoza UE), którzy zostali zatrzymani za przekroczenie granicy państwowej wbrew przepisom (dalej: pgpwp) lub usiłowanie pgpwp na odcinku jej z Białorusią. Oznacza to wzrost o 1164% w stosunku do 2020 r. (odnotowano 227 cudzoziemców). Wśród zatrzymanych osób największe grupy stanowili obywatele Iraku, Afganistanu, Syrii, Somalii, Rosji oraz Białorusi. W tym samym okresie

---

[11] *Bezpieczeństwo Europy Środkowo-Wschodniej. Perspektywa narodowa i międzynarodowa*, W. Śmiałek, Ł. Kominek, O. Balogh (red. nauk.), Poznań 2022, s. 293–294.

[12] *Hybrydowa agresja Białorusi na UE…*

[13] *Bezpieczeństwo i zagrożenia hybrydowe*, M. Banasiak, A. Rogozińska (red. nauk.), Warszawa 2022, s. 22.

[14] *Wielowymiarowość konfliktów kulturowych we współczesnym świecie*, W. Śmiałek (red. nauk.), Poznań 2024, s. 186.

[15] Tamże, s. 187.

na odcinku granicy z Litwą Straż Graniczna zarejestrowała 320 osób będących obywatelami państw trzecich, zatrzymanych/ujawnionych za pgpwp lub usiłowanie pgpwp, co daje wzrost o 158% w stosunku do 2020 r. (odnotowano 124 cudzoziemców). Najwięcej zatrzymanych osób pochodziło z Iraku i Syrii[16].

W 2022 r. Straż Graniczna odnotowała 586 cudzoziemców będących obywatelami państw trzecich zatrzymanych za pgpwp lub usiłowanie pgpwp na odcinku granicy z Białorusią. Jest to spadek o 80% w stosunku do 2021 r. Najwięcej zatrzymanych/ujawnionych osób było obywatelami Iraku, Syrii, Iranu, Afganistanu, a także Białorusi. W tym samym okresie na odcinku granicy z Litwą Straż Graniczna zarejestrowała 726 osób będących obywatelami państw trzecich, zatrzymanych/ujawnionych za pgpwp lub usiłowanie pgpwp. Oznacza to wzrost o 127% w stosunku do 2021 r. Najwięcej zatrzymanych/ujawnionych osób pochodziło z Iraku, Afganistanu, Iranu i Syrii[17].

W 2023 r. Straż Graniczna odnotowała 562 cudzoziemców będących obywatelami państw trzecich zatrzymanych za pgpwp lub usiłowanie pgpwp na odcinku granicy z Białorusią, co daje spadek o 4% w stosunku do 2022 r. Najwięcej zatrzymanych/ujawnionych osób pochodziło z Afganistanu, Białorusi i Syrii. Na odcinku granicy z Litwą Straż Graniczna odnotowała 727 cudzoziemców będących obywatelami państw trzecich zatrzymanych/ujawnionych za pgpwp lub usiłowanie pgpwp. W stosunku do 2022 r. jest to wzrost o 0,1%. Najwięcej zatrzymanych/ujawnionych osób pochodziło z Syrii, Afganistanu, Iranu i Indii[18].

W 2024 r. Straż Graniczna odnotowała 2582 cudzoziemców będących obywatelami państw trzecich zatrzymanych za pgpwp lub usiłowanie pgpwp na odcinku granicy z Białorusią. Oznacza to wzrost o 359% w stosunku do 2023 r. Najwięcej zatrzymanych/ujawnionych osób było obywatelami Etiopii, Erytrei, Somalii, Syrii, Jemenu, Sudanu i Afganistanu. W tym samym okresie na odcinku granicy z Litwą Straż Graniczna zarejestrowała 432 osoby będące obywatelami państw trzecich, które zostały zatrzymane/ujawnione za pgpwp lub usiłowanie pgpwp. W stosunku do 2023 r. jest to spadek o 41%. Najwięcej zatrzymanych/ujawnionych osób pochodziło z Afganistanu, Mołdawii, Białorusi[19].

---

[16] Statystyki SG – styczeń–grudzień 2021, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

[17] Statystyki SG – styczeń–grudzień 2022, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

[18] Statystyki SG – styczeń–grudzień 2023, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

[19] Statystyki SG – styczeń–grudzień 2024, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

Należy zaznaczyć, że przytoczone dane statystyczne odnoszą się do migrantów faktycznie zatrzymanych/ujawnionych. Liczba podejmowanych prób przekroczenia granic polsko-białoruskiej i polsko-litewskiej jest znacznie wyższa. Jak podają Podlaski Oddział Straży Granicznej i Nadbużański Oddział Straży Granicznej, tylko w 2021 r. na granicy z Białorusią odnotowano 39 697 prób nielegalnego przekroczenia granicy poza przejściami granicznymi. To ponad 300 razy więcej prób niż w 2020 r.[20] W 2024 r., jak informuje Podlaski Oddział Straży Granicznej, odnotowano blisko 30 000 prób nielegalnego przekroczenia granicy polsko-białoruskiej. Migranci pochodzili z 52 państw, głównie z Etiopii, Erytrei i Somalii. Zatrzymano również 346 organizatorów nielegalnego przekraczania granicy i pomocników w tym procederze, z czego 316 osób na granicy z Białorusią, a 30 na granicy z Litwą. Wśród zatrzymanych dominowali obywatele Ukrainy, Polski i Białorusi[21].

Kryzys migracyjny na granicy polsko-białoruskiej jest przykładem świadomych i zorganizowanych działań hybrydowych, w których Rosja, przy pomocy białoruskiego reżimu, wykorzystuje migrantów jako narzędzie politycznego szantażu. Aparat państwowy reżimu Łukaszenki nie tylko organizuje i kontroluje szlak migracyjny, lecz także prowadzi skoordynowane działania prowokacyjne i dezinformacyjne, mające na celu obarczenie Polski winą za kryzys i wywołanie podziałów w polskim społeczeństwie oraz na arenie międzynarodowej. Tego typu operacje pokazują, w jaki sposób Rosja wykorzystuje współczesne zagrożenia w swoich działaniach hybrydowych, aby destabilizować bezpieczeństwo i porządek w Polsce i Europie.

Ataki w cyberprzestrzeni

Intensywność rosyjskich cyberataków wymierzonych w Polskę wyraźnie wzrosła tuż przed inwazją Rosji w Ukrainie i po jej rozpoczęciu, co potwierdzają dane statystyczne przedstawione poniżej. Ataki są elementem szerszej strategii hybrydowej Kremla, mającej na celu destabilizację sytuacji w RP, wywieranie presji na polskie władze oraz wywołanie chaosu i niepewności w społeczeństwie. Prorosyjskie grupy hakerskie uderzają zarówno w instytucje państwowe, jak i w sektor prywatny,

[20] E. Szczepańska, *Nielegalne przekroczenia granicy z Białorusią*, Straż Graniczna, 12 I 2022 r., https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021-r.html [dostęp: 3 VI 2025].

[21] K. Zdanowicz, *Nielegalna migracja w Podlaskim Oddziale Straży Granicznej – podsumowanie*, 21 I 2025 r., https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/64039,Nielegalna-migracja-w-Podlaskim-Oddziale-Strazy-Granicznej-podsumowanie.html?search=858959366 [dostęp: 3 VI 2025].

media czy obywateli. Wykorzystują zaawansowane metody, takie jak ataki DDoS (ang. *distributed denial of service*), ransomware, phishing czy podszywanie się pod oficjalne strony rządowe. Część tych działań to bezpośrednia odpowiedź na wsparcie udzielane Ukrainie przez Polskę oraz na decyzje polityczne władz RP niekorzystne dla FR. We współczesnych konfliktach cyberprzestrzeń stała się istotnym polem walki, a jej skuteczna ochrona wymaga nieustannego monitoringu i szybkiej reakcji.

Szczególnie niebezpieczne są ataki typu APT (ang. *advanced persistent threats*), przeprowadzane przez grupy określane tym samym mianem. Są to zaawansowane, długotrwałe ataki, charakterystyczne dla tego rodzaju grup cyberprzestępczych, działających na zlecenie rządów. Grupy APT atakują, aby uzyskać strategiczne informacje, prowadzić cyberszpiegostwo, zakłócać funkcjonowanie atakowanego państwa, wpływać na jego politykę i gospodarkę. Wsparcie finansowe uzyskiwane od rządów zapewnia cyberprzestępcom dostęp do zaawansowanych zasobów i technologii, sprzyjających długotrwałym i skomplikowanym cyberatakom[22]. Znaczny segment tego środowiska stanowią grupy prorosyjskie[23].

Zgodnie z informacją podaną przez Pełnomocnika Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP incydenty w cyberprzestrzeni są typowymi dla Rosji działaniami retorsyjnymi, stanowiącymi odpowiedź na niekorzystne dla FR działania podejmowane przez inne państwa[24]. Grupy hakerskie stosujące m.in. ataki DDoS, ransomware czy phishing, a także wykorzystujące fałszywe strony internetowe podszywające się pod istniejące serwisy są powiązane z Kremlem. Szczególnie zagrożone są podmioty ze strategicznych sektorów, takich jak energetyczny czy zbrojeniowy. Ataki te są zbieżne z założeniami działań hybrydowych, które mają prowadzić do destabilizacji, zastraszenia i chaosu. Każdy cyberatak przynosi określone skutki – polityczne, finansowe, społeczne[25].

Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa powołano w Polsce trzy zespoły reagowania na incydenty bezpieczeństwa komputerowego, tj. CSIRT GOV, CSIRT NASK i CSIRT MON. Ze względu na tematykę raportów o stanie polskiego bezpieczeństwa w cyberprzestrzeni, publikowanych przez te zespoły, autorka artykułu przeanalizowała raporty CSIRT GOV i CERT Polska (działający w strukturze CSIRT NASK) za lata 2021–2024, a także raporty za lata

[22] *Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025*, https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf, s. 6 [dostęp: 10 VI 2025].

[23] Tamże, s. 14.

[24] *Rosyjskie cyberataki*, Serwis Rzeczypospolitej Polskiej, 29 XII 2022 r., https://www.gov.pl/web/sluzby-specjalne/rosyjskie-cyberataki [dostęp: 5 VI 2025].

[25] Tamże.

2021–2022 sporządzone przez CSIRT KNF, będący zespołem reagowania na incydenty bezpieczeństwa komputerowego w polskim sektorze finansowym[26].

Zespół CSIRT GOV (prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego) od 2010 r. publikuje roczne raporty o stanie bezpieczeństwa cyberprzestrzeni RP[27]. Największy przyrost liczby zgłoszeń dotyczących potencjalnych incydentów, a w konsekwencji wzrost liczby potwierdzonych incydentów, odnotowano w III i IV kwartale 2021 r. Najwięcej zgłoszeń dotyczyło w kolejności: infrastruktury krytycznej, instytucji, urzędów, ministerstw, służb i wojska, pozostałych sektorów[28]. W raporcie za 2021 r. zespół CSIRT GOV poinformował o ponadtrzykrotnym wzroście liczby zgłoszeń potencjalnych incydentów bezpieczeństwa teleinformatycznego w stosunku do roku poprzedniego. Odnotowano także aktywność sponsorowanych grup APT, szczególnie w kontekście infrastruktury krytycznej i administracji publicznej[29]. Z kolei zespół CERT Polska w 2021 r. poinformował o wzroście liczby obsłużonych incydentów o 182% w stosunku do roku poprzedniego[30].

W raporcie poświęconym analizie zagrożeń bezpieczeństwa cyberprzestrzeni dla rynku finansowego w Polsce z 2021 r. CSIRT KNF również odnotował, że największy przyrost liczby zgłoszonych niebezpiecznych stron nastąpił w III i IV kwartale 2021 r.[31]

W serwisie gov.pl, w sekcji dotyczącej cyberbezpieczeństwa, od 2022 r. zaczęło pojawiać się coraz więcej artykułów na temat zagrożeń związanych z oszustwami i dezinformacją, a w 2023 r. zaczęto publikować artykuły mówiące wprost o rosyjskich cyberatakach[32].

W raporcie CSIRT GOV dotyczącym 2022 r. po raz pierwszy poświęcono cały rozdział analizie działalności grup APT, których aktywność w obszarze cyberprzestrzeni RP była związana z wojną w Ukrainie[33]. Zwrócono uwagę na nieodnotowane

---

[26] *Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego*, Urząd Komisji Nadzoru Finansowego, https://cebrf.knf.gov.pl [dostęp: 10 VI 2025].

[27] Raporty o stanie bezpieczeństwa cyberprzestrzeni RP, Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi [dostęp: 5 VI 2025].

[28] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku*, Warszawa 2022, s. 14.

[29] Tamże, s. 64.

[30] CERT Polska, *Raport roczny z działalności CERT Polska 2021. Krajobraz bezpieczeństwa polskiego internetu*, Warszawa 2022, s. 12.

[31] CSIRT KNF, *Podsumowanie Roku w CSIRT KNF 2021. Opis wybranych ataków*, https://cebrf.knf.gov.pl/images/Komunikaty/Raporty/Pdf/RaportCSIRTKNF_76474.pdf [dostęp: 8 VI 2025].

[32] Baza wiedzy – cyberbezpieczeństwo, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/baza-wiedzy/aktualnosci [dostęp: 8 VI 2025].

[33] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku*, Warszawa 2023, s. 56.

wcześniej na tak szeroką skalę zagrożenia i działania, w tym wzrastającą liczbę kampanii socjotechnicznych i ataków DDoS, które były wymierzone przede wszystkim w usługi publiczne świadczone w internecie. Największą liczbę incydentów z 2022 r. zespół CSIRT GOV sklasyfikował w kategoriach: podatność, socjotechnika i niedostępność. W kategorii podatność odnotowano największą liczbę incydentów ze względu na wprowadzenie w lutym 2022 r. stopnia alarmowego CHARLIE-CRP, co skutkowało wzrostem liczby zidentyfikowanych zdarzeń, które mogły naruszyć bezpieczeństwo infrastruktury teleinformatycznej RP.

Kampanie socjotechniczne odnotowane przez CSIRT GOV w 2022 r. to kampanie phishingowe, podmiany stron internetowych i podszycia (często pod witryny administracji rządowej lub systemów rządowych). Ich intensywność utrzymywała się na wysokim poziomie, a adresatami byli odbiorcy masowi oraz przedstawiciele wybranych podmiotów. Te działania były ukierunkowane przede wszystkim na zdobycie nieuprawnionego dostępu do zasobów, którymi dysponował atakowany podmiot, przez pozyskanie danych uwierzytelniających. Ponadto ataki miały na celu dystrybucję złośliwego oprogramowania oraz uzyskanie dostępu do systemów informatycznych, aby realizować dalsze działania cyberprzestępcze[34].

W kategorii niedostępność odnotowano od lutego 2022 r. znaczny wzrost liczby ataków DDoS (826 incydentów, a w roku poprzednim – 310) wymierzonych w polskie witryny podmiotów administracji publicznej oraz infrastruktury krytycznej. Realizowały je grupy haktywistyczne, m.in. Killnet, NoName057(16), Cyber Armia Ludowa. Zespół CSIRT GOV wskazał, że w 2022 r. komponentem najbardziej narażonym na ataki w cyberprzestrzeni była infrastruktura krytyczna RP[35]. Potwierdził również, że działania Polski na rzecz wsparcia Ukrainy w wojnie z Rosją znacznie podniosły poziom zagrożenia w cyberprzestrzeni RP.

Zespół CERT Polska w raporcie rocznym z działalności w 2022 r. poświęca cały rozdział wpływowi wojny w Ukrainie na polskie cyberbezpieczeństwo. Z perspektywy czasu potwierdzono, że działania wojenne prowadzone przez Rosję są wspierane przez aktywność hakerów i grup haktywistycznych, a także szerzenie dezinformacji. Te nasilone działania w cyberprzestrzeni Rosja prowadziła już w miesiącach poprzedzających wojnę konwencjonalną w Ukrainie. Zdarzenia w polskiej cyberprzestrzeni, jakie CERT Polska łączy bezpośrednio z wojną w Ukrainie, podobnie jak CSIRT GOV, to zmasowane ataki DDoS na strony rządowe i witryny ważnych podmiotów gospodarczych, a także kampanie phishingowe wykorzystujące motyw wojny i pojawiające się głównie w mediach społecznościowych. W raporcie stwierdzono, że ataki mają destabilizować sytuację wewnętrzną w państwach, które wspierają Ukrainę.

[34] Tamże, s. 30.

[35] Tamże, s. 13–17.

Podano przykłady ataków DDoS przeprowadzonych przez rosyjskich haktywistów. Podkreślono ich częstą nieskuteczność oraz wykorzystywanie przede wszystkim do szerzenia propagandy i dezinformacji. Wymieniono również kampanie wykorzystujące wygląd znanych stron internetowych i stron instytucji rządowych, a także motyw wojny. Oszustwa obejmowały m.in. fałszywe panele logowania do Facebooka, fałszywe zbiórki, nigeryjski przekręt, fałszywe inwestycje[36].

W raporcie z 2022 r. CSIRT KNF również poświęcił rozdział zagrożeniom i rekomendacjom odnośnie do ataków DDoS oraz działań haktywistów w kontekście wojny w Ukrainie. Zespół poinformował, że w 2022 r. ataki typu DDoS były najliczniejsze. Miały one pewien wpływ na sektor finansowy w Polsce. Podkreślono dużą dostępność, łatwość wykorzystania, stosunkowo niewielki koszt i skuteczność tego typu metod przestępczych. Wskazano także na możliwość przeprowadzenia (planowanie ataków i kierowanie nimi) czy uczestniczenia (udostępnianie swoich zasobów) w ataku przez niemal każdą osobę. Zespół CSIRT GOV zauważył ponadto zależność celu ataków prorosyjskich grup cyberprzestępców od działań politycznych państw, które w ocenie haktywistów są wrogie wobec Rosji czy sprzyjające Ukrainie[37].

W raporcie CSIRT GOV dotyczącym 2023 r. znalazły się informacje, że w tym roku Polska nadal zmagała się z nasilonymi cyberzagrożeniami związanymi z konfliktem zbrojnym w Ukrainie. Na podstawie oceny aktywności grup APT w 2023 r. stwierdzono, że były to w dużej mierze ataki będące kontynuacją działań odnotowanych w 2022 r. Głównymi celami ataków pozostały instytucje państwowe oraz infrastruktura krytyczna, zwłaszcza w sektorach energetycznym i transportowym. Dominowały dwa typy działań przestępczych: ataki DDoS – wykorzystywane przez prorosyjskie grupy do zakłócania funkcjonowania stron internetowych i usług publicznych, a także kampanie socjotechniczne – mające na celu wyłudzanie danych, infekowanie systemów złośliwym oprogramowaniem, destabilizację procesów politycznych. Intensyfikacja tych działań nastąpiła w związku z wyborami parlamentarnymi w Polsce. Z raportu wynika, że w 2023 r. Polska była kluczowym celem rosyjskich operacji hybrydowych, łączących cyberataki z wojną informacyjną[38].

Zespół CERT Polska w raporcie za 2023 r. przedstawił analizę dotyczącą działań grup APT. Od czasu rozpoczęcia wojny w Ukrainie zauważono znaczne nasilenie ich aktywności, której celem w 2023 r. było przede wszystkim zakłócenie ciągłości

[36] CERT Polska, *Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego internetu*, Warszawa 2023, s. 93–100.

[37] CSIRT KNF, *Cyberzagrożenia w sektorze finansowym 2022*, https://cebrf.knf.gov.pl/images/Cyberzagroenia_w_sektorze_finansowym_2022.pdf [dostęp: 8 VI 2025].

[38] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku*, Warszawa 2024, s. 4–6.

działania polskich podmiotów z sektora transportu i logistyki[39]. Zauważono, że te grupy są powiązane z FR i/lub Białorusią[40].

Zespół CSIRT GOV w raporcie z działalności za 2024 r. poinformował, że w Polsce nadal utrzymywał się podwyższony poziom zagrożeń w cyberprzestrzeni, które obejmowały działania socjotechniczne, próby wykorzystywania podatności, ataki typu DDoS, publikacje danych pochodzących z wycieków, dokonywane także przez sponsorowane grupy haktywistyczne. W 2024 r. miały miejsce szczególne wydarzenia z perspektywy bezpieczeństwa, tj. wybory samorządowe, wybory do Europarlamentu, a także XXXIII Letnie Igrzyska Olimpijskie w Paryżu. Incydenty z 2024 r. opisane w raporcie potwierdzały, że w zainteresowaniu cyberprzestępców i aktorów państwowych są wszelkie podmioty, których zaatakowanie będzie godziło również w bezpieczeństwo kraju. W raporcie stwierdzono ponadto, że cyberataki to zagrożenie hybrydowe i element nowoczesnych konfliktów, w których wrogie działania są prowadzone poniżej progu wojny[41]. Szczególną uwagę zwrócono na zagrożenia atakami na łańcuchy dostaw, które zdefiniowano jako ataki wymierzone w zaufanego zewnętrznego dostawcę usług niezbędnego dla tego łańcucha. To poszerzyło potencjalny obszar ataku na kluczowe sektory infrastruktury w Polsce[42]. Potwierdzono, że ataki grup APT, motywowanych ideologicznie, politycznie i finansowo, niezmiennie stanowią największe zagrożenie dla administracji rządowej oraz infrastruktury krytycznej. W 2024 r. grupy te koncentrowały się na kontynuacji działań z lat 2022–2023 i tak jak wcześniej tę aktywność wspierały kampanie propagandowe, mające pokazać skuteczność i potencjał cyberataków. Zauważono, że 2024 r. charakteryzował się wzrostem wolumenu grup cyberprzestępczych, który był spowodowany przyrostem liczby grup motywowanych finansowo oraz zwiększającym się dostępem do wspomagających narzędzi typu AI. Jako głównego aktora wymieniono grupę APT28 (znaną również jako Fancy Bear), a następnie grupy APT29 (inaczej Cozy Bear), UNC1151 (znaną również jako Ghostwriter), APT15, DaVinci[43].

Zespół CERT Polska w raporcie z działalności za 2024 r. przedstawił, podobną do zespołu CSIRT GOV, obserwację dotyczącą aktywności grup APT, powiązanych przede wszystkim z FR i Białorusią. Poinformował, że te grupy miały realizować cele wywiadowcze i propagandowe, a większość ich działań polegała na próbach wyłudzenia danych uwierzytelniających do skrzynek pocztowych, dystrybucji złośliwego oprogramowania oraz atakach na systemy przemysłowe. Zwrócił ponadto

[39] CERT Polska, *Raport roczny z działalności CERT Polska 2023*, Warszawa 2024, s. 34.

[40] Tamże.

[41] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*, Warszawa 2025, s. 5–6.

[42] Tamże, s. 113.

[43] Tamże, s. 54–56.

uwagę na proceder atakowania nie tylko instytucji publicznych czy dużych przedsiębiorstw, lecz także mniejszych podmiotów, będących ogniwami łańcuchów dostaw. Zespół CERT Polska jako najaktywniejsze spośród zaobserwowanych grup APT wymienił UNC1151, APT28 oraz APT29[44].

Należy zauważyć, że wszystkie zespoły przedstawiły w swoich analizach podobne wnioski co do trendów, głównych typów zagrożeń oraz sektorów najbardziej narażonych na cyberataki w Polsce. Są to:

- znaczny wzrost od 2021 r. liczby zgłoszeń i potwierdzonych incydentów w sieci w porównaniu z latami poprzednimi, zauważalny na kilka miesięcy przed agresją Rosji na Ukrainę w 2022 r.,
- nasilona i dynamiczna działalność grup cyberprzestępców powiązanych z FR i Białorusią,
- najczęstsze typy ataków to ataki DDoS i kampanie socjotechniczne,
- jedną z intencji ataków było wywołanie szeroko rozumianych zakłóceń w funkcjonowaniu państwa,
- obiektami cyberataków były przede wszystkim administracja rządowa, instytucje publiczne i podmioty infrastruktury krytycznej,
- charakterystycznym działaniem grup APT jest propagowanie swojej działalności w mediach społecznościowych,
- wzrost liczby ataków wymierzonych w mniejsze podmioty, będące ogniwami łańcuchów dostaw.

Amerykański odpowiednik polskich zespołów CSIRT, tj. Cybersecurity and Infrastructure Security Agency, opublikował w maju 2025 r. raport na temat szczególnego zagrożenia, z jakim obecnie mierzą się wschodnioeuropejskie podmioty, w tym polskie, będące ogniwami łańcuchów dostaw. Stwarza je wielokrotnie wymieniana przez polskie zespoły grupa APT28. Jak podkreśliło amerykańskie źródło, jest ona utożsamiana z rosyjskim Głównym Zarządem Wywiadowczym (GRU) i rosyjską jednostką wojskową 26165[45].

Cyberprzestrzeń stała się kluczowym polem działań hybrydowych, obejmujących zarówno ataki techniczne, jak i towarzyszące im kampanie informacyjne, mające na celu destabilizację państwa oraz wywieranie presji społecznej i politycznej. Rosyjskie cyberataki wpisują się w strategię działań hybrydowych, niejednokrotnie są odpowiedzią na działania niekorzystne dla Rosji i stanowią integralną część wojny z Ukrainą.

---

[44] CERT Polska, *Raport roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu*, Warszawa 2025, s. 33.

[45] *Russian GRU Targeting Western Logistics Entities and Technology Companies*, CISA, 21 V 2025 r., https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a [dostęp: 10 VI 2025].

Dezinformacja w polskiej przestrzeni informacyjnej

Działania propagandowe i dezinformacyjne ze strony rosyjskiej są obserwowane przynajmniej od czasów Związku Radzieckiego, jednak rządy prezydenta Władimira Putina uczyniły Rosję jednym z najbardziej aktywnych aktorów w sferze informacyjnej, w tym w cyberprzestrzeni, na międzynarodowej scenie politycznej[46]. Kompleksowe działania prowadzone przez FR są określane mianem wojny informacyjnej i obejmują skoordynowane kampanie propagandowe i dezinformacyjne w cyberprzestrzeni[47]. Wojna informacyjna jest postrzegana jako jeden z najważniejszych elementów strategii rywalizacji międzynarodowej Rosji, mający umożliwić osiąganie celów politycznych tego państwa. Cyberprzestrzeń natomiast umożliwia FR prowadzenie działań w ramach tej wojny[48].

Jerzy Surma podkreśla szczególną rolę, jaką w wojnie informacyjnej odgrywają media społecznościowe. Zwraca uwagę na konsekwencje dla bezpieczeństwa państwa, jakie niesie łatwa i tania możliwość publikowania i wymiany informacji. Te cechy mediów społecznościowych sprawiają, że stają się one jednocześnie miejscem i narzędziem prowadzenia wojen informacyjnych, których celem jest zarządzanie informacją w taki sposób, aby wpływać na zachowania społeczeństwa i kształtować je zgodnie z wolą atakującego.

Wojna informacyjna jest prowadzona w sposób zorganizowany, przy wykorzystaniu zarówno działań jawnych, takich jak propaganda czy manipulowanie informacjami, jak i niejawnych, polegających m.in. na fabrykowaniu informacji w celach dezinformacyjnych. Federacja Rosyjska została przez niego podana jako przykład państwa systemowo prowadzącego w ramach wojen hybrydowych działania, które mają znamiona wojen informacyjnych[49].

Wrogim działaniom tego typu można przypisać następujące cele:

- zachwianie systemu wartości (rozpad więzi społecznych, izolowanie jednostek lub grup, nieufność wobec instytucji publicznych),
- atak na ważne obiekty (infrastrukturę krytyczną, obiekty kultu i symbole międzynarodowe),

[46] *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski*, M. Banasik (red. nauk.), Warszawa 2021, s. 7.

[47] Tamże.

[48] Tamże, s. 8.

[49] J. Surma, *Cyfryzacja życia w erze Big Data. Człowiek. Biznes. Państwo*, Warszawa 2017, s. 90.

- kreowanie i wykorzystanie liderów opinii (kształtowanie percepcji przez osoby wpływowe i/lub mające zdolność oddziaływania na szerokie grupy odbiorców)[50].

W literaturze przedmiotu podkreśla się wieloaspektowość rosyjskich kampanii realizowanych w sferze informacyjnej, a także ich znaczenie strategiczne. Prowadzona przez nich wojna informacyjna obejmuje procesy, które są ukierunkowane na sferę poznawczą człowieka i kształtowanie postaw ludzi zgodnie z oczekiwaniami atakującego[51].

Od 24 lutego 2022 r. Rosjanie deprecjonowali wizerunek RP zarówno w swojej, jak i zewnętrznej infosferze. Aktywność ta polegała m.in. na rozwijaniu polskojęzycznych kanałów na platformie Telegram (na których grupy haktywistyczne udostępniały w celach propagandowych np. nieprawdziwe informacje o atakach wymierzonych w polskie obiekty[52]), działaniach tzw. kont trollowskich i botowskich oraz zauważalnej aktywności środowisk zaangażowanych w rozpowszechnianie rosyjskiego przekazu. Dezinformacyjne materiały i narracje obecne na rosyjskich kanałach na Telegramie, także tych polskojęzycznych, były następnie udostępniane w innych kanałach polskiego segmentu sieci społecznościowych. W realizację rosyjskich celów informacyjnych wpisywały się również nowo powstałe stowarzyszenie Polski Ruch Antywojenny oraz kampanie o politycznym wydźwięku, takie jak „Stop ukrainizacji Polski" czy „To nie nasza wojna". Ponadto strona białoruska ujawniła polskich obywateli, którzy wyemigrowali do Białorusi i Rosji i rozpoczęli prorosyjską działalność dezinformacyjną. Rozpowszechniali oni w mediach społecznościowych rosyjskie przekazy propagandowe i dezinformacyjne[53].

Platforma Telegram została założona przez rosyjskich obywateli w 2013 r. W 2021 r. nastąpił rozwój jej polskojęzycznego segmentu. Do jej popularyzacji w Polsce przyczyniły się dwa wydarzenia z 2021 r., za które prawdopodobnie odpowiada strona rosyjska.

Pierwszym z nich było opublikowanie na Telegramie danych pozyskanych po ataku na skrzynki mailowe polskich polityków[54]. Jednym z nich był minister Michał Dworczyk. Informacje pochodzące z jego skrzynki mailowej zaczęły pojawiać się na kanale Telegram od 4 czerwca. Eksperci twierdzą, że za te działania jest

[50] *Odporność państwa, społeczeństwa i gospodarki na zagrożenia*, M. Piotrowska-Trybull, K. Górska-Rożej (red. nauk.), Warszawa 2024, s. 331–332.

[51] *Informacja czynnikiem warunkującym bezpieczeństwo*…, s. 50.

[52] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku*…, s. 25–28.

[53] M. Marek, *Wojna informacyjna Federacji Rosyjskiej*…, s. 116–117.

[54] Tamże, s. 119.

odpowiedzialna Rosja lub współpracująca z nią Białoruś[55]. Atak wpisuje się w założenia kampanii o nazwie „Ghostwriter", której celem jest pozyskiwanie przez rosyjskie służby specjalne danych i wrażliwych informacji oraz rozprzestrzenianie rosyjskiej dezinformacji[56]. W ramach tej kampanii są atakowane konta poczty internetowej oraz konta w mediach społecznościowych należące do osób publicznych z krajów Europy Środkowo-Wschodniej, głównie z Polski. Przestępcy podejmują próby przejmowania zasobów informacyjnych na potrzeby rosyjskiej dezinformacji[57].

Drugim wydarzeniem był kryzys migracyjny na granicy polsko-białoruskiej w Polsce w 2021 r. Przez Telegram (a dalej inne platformy społecznościowe i media) do polskiej infosfery trafiały nagrania i przekazy propagandowe[58]. Popularyzacja tego narzędzia w Polsce pozwoliła na przekazywanie narracji rosyjsko-białoruskiej[59].

Jak podaje Michał Marek, kierownik Zespołu Analiz Zagrożeń Zewnętrznych NASK, rosyjska dezinformacja skupia się na trzech głównych narracjach: o popychaniu Polski w stronę wojny z Rosją[60], o odpowiedzialności NATO i USA za wybuch wojny w Ukrainie[61], o objęciu Polski tzw. ukrainizacją[62]. Rok po wybuchu wojny w Ukrainie rzecznik prasowy Ministerstwa Spraw Zagranicznych RP zamieścił komentarz, w którym napisał o bezprecedensowym wzroście skali rosyjskiej działalności dezinformacyjnej. Zauważył, że Rosja prowadzi szeroko zakrojoną kampanię dezinformacyjną. Jej celami są podważenie wartości wolnego i demokratycznego świata oraz wywołanie chaosu, nawoływanie do nienawiści i destabilizacja międzynarodowego porządku. Rzecznik wskazał, że pomimo nowych form fałszywych narracji podstawowe metody manipulacji pozostają takie same. Ten sam jest również cel – wzbudzenie napięć i niepokojów w atakowanych społeczeństwach. Przestrzegał przed przekazywaniem odbiorcom sprzecznych informacji, które mają

[55] *Afera mailowa. Prokuratura postawiła zarzuty, ale to pionki*, CyberDefence24, 16 VIII 2024 r., https://cyber-defence24.pl/polityka-i-prawo/afera-mailowa-prokuratura-postawila-zarzuty-ale-to-pionki [dostęp: 11 VI 2025].

[56] *Rozwój technik ataku grupy UNC1151/Ghostwriter*, Cert.pl, 19 VII 2022 r., https://cert.pl/posts/2022/07/techniki-unc1151/ [dostęp: 23 VI 2025].

[57] *Rosyjskie cyberataki*…

[58] M. Marek, *Wojna informacyjna Federacji Rosyjskiej*…, s. 119.

[59] Tamże, s. 123.

[60] Tamże, s. 131.

[61] Tamże, s. 140.

[62] Tamże, s. 146.

sprawić, że ludzie przestaną odróżniać prawdę od fałszu. To pozwoliłoby na uwiarygodnienie nawet najbardziej absurdalnych wersji wydarzeń[63].

W styczniu 2025 r. został opublikowany raport zespołu ds. dezinformacji z Komisji do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024. Zwrócono w nim uwagę na teorię rosyjskiej strategii walki informacyjnej, która oddaje istotę i charakter działań prowadzonych w polskiej infosferze. Zafałszowane w różnym stopniu treści pojawiają się zarówno w tradycyjnych mediach, jak i mediach społecznościowych oraz na platformach internetowych. Wskazano na rosyjską agencję informacyjną Sputnik, która miała polską wersję strony, a publikowane na niej treści były udostępniane przez spreparowane środowiska informacyjne, a dalej przez konta w mediach społecznościowych[64]. Stwierdzono ponadto, że wraz z wybuchem wojny w Ukrainie w 2022 r. rosyjska propaganda zaczęła prowadzić narrację o bezbronności państw zachodnich (w tym Polski), słabości ich armii i władz. Celem było przekonanie odbiorców, że państwo nie zapewnia im bezpieczeństwa, a w razie zagrożenia nie warto go bronić[65]. Eksperci tworzący ten raport zwrócili uwagę na cele rosyjskiej dezinformacji i propagandy, czyli polaryzację społeczeństwa, erozję zaufania do państwa, a także do nauki, mediów i współobywateli[66].

Skalę rosyjskich działań dezinformacyjnych odzwierciedlają również meldunki sytuacyjne zamieszczone w serwisie gov.pl. W 2023 r. opublikowano 31 meldunków opisujących działania dezinformacyjne prowadzone przez Rosję i Białoruś przeciwko Polsce. Dotyczyły one fałszywych oskarżeń wobec Polski, m.in. o brutalne traktowanie migrantów na granicy oraz plany agresji na Ukrainę. Podkreślono w tych meldunkach, że te działania miały na celu wywołanie społecznych podziałów oraz osłabienie zaufania do polskich władz i instytucji, a także były elementem wojny informacyjnej mającej na celu destabilizację Polski i regionu[67].

---

[63] *O rosyjskiej dezinformacji: rok od pełnoskalowej inwazji na Ukrainę – komentarz Rzecznika Prasowego MSZ*, Serwis Rzeczypospolitej Polskiej, 23 II 2023 r., https://www.gov.pl/web/dyplomacja/o-rosyjskiej-dezinformacji-rok-od-pelnoskalowej-inwazji-na-ukraine--komentarz-rzecznika-prasowego-msz [dostęp: 14 VI 2025].

[64] Komisja do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024, *Raport Zespołu ds. Dezinformacji*, Warszawa 2025, s. 5.

[65] Tamże, s. 19.

[66] Tamże, s. 20.

[67] Dezinformacja przeciwko Polsce, meldunki sytuacyjne, Służby specjalne, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2 [dostęp: 14 VI 2025].

Skalę dezinformacji w 2023 r. ukazało również Rządowe Centrum Bezpieczeństwa (RCB). W ramach projektu DisInfo Radar RCB opublikowano 57 infografik przedstawiających tematy, których dotyczyła rosyjska i białoruska dezinformacja. Informowano w nich m.in. o fałszywych liniach rosyjskich perswazji i narracji, nieprawdziwych tezach, manipulacjach, stronach internetowych zaobserwowanych w 2023 r.[68] Przed kampanią dezinformacyjną ostrzegano zwłaszcza w październiku 2023 r., kiedy w Polsce odbywały się wybory parlamentarne. Wymieniono zagrożenia, na jakie narażone było bezpieczeństwo procesu wyborczego, a także poinformowano o trwającej kampanii informacyjnej, sugerującej przygotowywanie w Polsce zamachu stanu i zamiar użycia wojska przeciwko społeczeństwu[69].

Polskie zespoły reagowania na incydenty komputerowe od 2021 r. również zwracały uwagę w swoich rocznych raportach na rosyjskie kampanie dezinformacyjne. Zespół CSIRT GOV w raporcie z działalności za 2021 r. informował o odnotowanych aktywnościach grup APT, którym przypisano szerzenie dezinformacji. Jako jeden z przykładów podano operację „Ghostwriter", której sprawstwo przypisuje się grupie UNC1151[70].

W raporcie z działalności za 2022 r. zespół CSIRT GOV informował o identyfikacji incydentów, które wskazywały na kontekst dezinformacyjny. Jako przykład podano atak z września 2022 r. polegający na umieszczeniu na stronie Urzędu Transportu Kolejowego treści o tematyce antyukraińskiej wraz z propagandowymi grafikami. Zespół CSIRT GOV poinformował ponadto o identyfikacji procederu polegającego na rejestracji witryn podszywających się pod nazwy oficjalnych domen rządowych, co wskazywało na możliwość wykorzystania ich do przeprowadzania ataków socjotechnicznych, w tym do dezinformacji[71]. Zespół CERT Polska w raporcie z działalności w 2022 r. także informował o dezinformacyjnych działaniach prorosyjskich grup cyberprzestępczych. Stwierdzono, że cechą charakterystyczną tych grup jest szerzenie dezinformacji[72].

To zjawisko zostało opisane również w raporcie z działalności CSIRT GOV w 2023 r. Zespół zwrócił uwagę na wybory parlamentarne, które stanowiły bodziec do intensyfikacji działań grup haktywistycznych, prowadzących

[68] Disinfo Radar, Rządowe Centrum Bezpieczeństwa, https://www.gov.pl/web/rcb/disinfo-radar [dostęp: 14 VI 2025].

[69] Tamże.

[70] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku*…, s. 27.

[71] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku*…, s. 31.

[72] CERT Polska, *Raport roczny z działalności CERT Polska 2022*…, s. 93.

ataki dezinformacyjne z wykorzystaniem różnych środków przekazu, w tym wiadomości e-mail i SMS. Sprawstwo przypisał m.in. grupie UNC1151[73].

Podobne obserwacje opisał zespół CERT Polska w raporcie z działalności za 2023 r. Jako najbardziej aktywną grupę APT także wskazał grupę UNC1151 oraz jej powiązanie z rządem Białorusi i rosyjskimi służbami specjalnymi. Atakowane osoby pochodziły głównie ze środowiska polityki i wojskowości, ale były to również osoby mogące mieć pośredni związek z Rosją czy Białorusią, np. prawnicy, tłumacze przysięgli języka rosyjskiego, księża prawosławni, pracownicy organizacji pozarządowych, dziennikarze. Wskazano na motywacje działań, jakimi były kradzież informacji w celach wywiadowczych oraz prowadzenie kampanii dezinformacyjnych. W 2023 r. zespół zaobserwował kampanie dezinformacyjne, które były związane z zagrożeniem terrorystycznym w Polsce, zbieraniem informacji o uchodźcach, rekrutacją do wojska czy brakiem jodku potasu w aptekach. W ocenie CERT Polska kampanie były ukierunkowane na szerzenie niepewności i podziałów w społeczeństwie. Odnotowano, że po wyborach parlamentarnych aktywność grupy UNC1151 znacznie zmalała[74].

W raporcie z działalności w 2024 r. zespół CSIRT GOV ponownie zwrócił uwagę na wybory samorządowe oraz wybory do Parlamentu Europejskiego, które były narażone na wrogie operacje dezinformacyjne prowadzone w cyberprzestrzeni. Kolejnym wydarzeniem, z którym wiązał się incydent dezinformacyjny, były XXXIII Letnie Igrzyska Olimpijskie w Paryżu. W sierpniu 2024 r. działające wspólnie prorosyjskie grupy haktywistyczne Beregini i Zarya wykradły dokumenty z systemów teleinformatycznych Polskiej Agencji Antydopingowej i opublikowały je w zmodyfikowanej formie, aby zdyskredytować polskich sportowców[75]. Zespół, podobnie jak w poprzednich latach, zaobserwował działalność grupy UNC1151, która tym razem prowadziła kampanię wymierzoną w użytkowników poczty najpopularniejszych dostawców – Gmail, Interia, Wirtualna Polska, Onet, o2. Dane ze skrzynek pocztowych przestępcy pozyskiwali przez podszywanie się pod administratorów poczty i nakłanianie użytkowników do logowania się za pomocą fałszywego panelu logowania[76]. Kolejnym poważnym incydentem przypisywanym sponsorowanym grupom cyberprzestępczym był atak na Polską Agencję Prasową w maju 2024 r. Na jej oficjalnej stronie dwukrotnie została zamieszczona fałszywa informacja dotycząca mobilizacji wojskowej w Polsce[77].

---

[73] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku*…, s. 6.

[74] CERT Polska, *Raport roczny z działalności CERT Polska 2023*…, s. 93.

[75] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*…, s. 6.

[76] Tamże, s. 69.

[77] Tamże, s. 78.

Zespół CERT Polska w raporcie z działalności za 2024 r. omówił, podobnie jak zespół CSIRT GOV, kampanię dezinformacyjną wymierzoną w Polską Agencję Antydopingową. Ponadto została opisana kampania dezinformacyjna związana z ćwiczeniami wojskowymi Steadfast Defender 2024 i Dragon-24, dotycząca rzekomo pijanego kierowcy wojskowej ciężarówki. Zespół podkreślił, że treści dezinformacyjne, które pojawiły się w polskiej infosferze w 2024 r., nawiązywały do wielu wydarzeń społeczno-politycznych[78].

Podsumowanie

Przeprowadzona analiza informacji dotyczących kryzysu migracyjnego, ataków w cyberprzestrzeni i sferze informacyjnej Polski pozwala stwierdzić, że przedstawiciele polskich organów rządowych, służb mundurowych, w tym służb specjalnych, a także specjaliści zajmujący się wykrywaniem ataków w cyberprzestrzeni i zapobieganiu im nie mają wątpliwości co do specyfiki i charakteru rosyjskich działań skierowanych przeciwko Polsce. Stwierdzają, że agresywne działania ze strony Rosji są elementem prowadzonej wojny hybrydowej, ściśle związanej z atakiem na Ukrainę. Rosyjską strategię charakteryzuje stopniowe, zaplanowane osłabianie adwersarza przez prowadzenie działań na wielu płaszczyznach funkcjonowania państwa. To właśnie takie działania mają być najbardziej skuteczne.

Analiza danych zawarta w niniejszym artykule dowodzi prawdziwości postawionej tezy. Ataki na integralność RP dokonane przez FR miały bezpośredni związek z wojną w Ukrainie. Badania materiałów źródłowych przeprowadzone metodą analizy, syntezy i wnioskowania pozwalają stwierdzić, że za ataki hybrydowe prowadzone przeciwko Polsce od 2021 r. jest odpowiedzialna Rosja we współpracy z Białorusią.

Rosyjskie działania hybrydowe charakteryzuje zatarcie granicy między obszarami militarnym i cywilnym. Do realizacji swoich celów Rosja wykorzystuje cywili. Rosyjsko-białoruskie ataki hybrydowe są wymierzone w obszary, które mogą być istotne dla bezpieczeństwa Polski. Skoordynowane prowadzenie tych ataków w wielu obszarach jednocześnie ma spotęgować ich dotkliwość. Niezbędne jest zatem prowadzenie ćwiczeń na wypadek sytuacji kryzysowych, obejmujących nie tylko sferę militarną, lecz także cywilną, oraz wspólnych ćwiczeń międzysektorowych.

[78] CERT Polska, *Raport roczny 2024 z działalności CERT Polska*…, s. 35.

Bibliografia

Bezpieczeństwo Europy Środkowo-Wschodniej. Perspektywa narodowa i międzynarodowa, W. Śmiałek, Ł. Kominek, O. Balogh (red. nauk.), Poznań 2022.

Bezpieczeństwo i zagrożenia hybrydowe, M. Banasik, A. Rogozińska (red. nauk.), Warszawa 2022.

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja Krymska – studium przypadku*, Warszawa 2014.

Hoffman F.G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007.

Hoffman F.G., *Hybrid Warfare and Challenges*, „Joint Force Quarterly" 2009, nr 52, s. 34–39.

Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski, M. Banasik (red. nauk.), Warszawa 2021.

Krzak A., *Wojny przyszłości po rosyjsku – wojna hybrydowa, informacyjna i psychologiczna na tle konfliktu ukraińskiego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 18, s. 11–39.

Marek M., *Wojna informacyjna Federacji Rosyjskiej przeciwko Ukrainie, Polsce i NATO*, Warszawa 2025.

Odporność państwa, społeczeństwa i gospodarki na zagrożenia, M. Piotrowska-Trybull, K. Górska-Rożej (red. nauk.), Warszawa 2024.

Surma J., *Cyfryzacja życia w erze Big Data. Człowiek. Biznes. Państwo*, Warszawa 2017.

Wasiuta O., Wasiuta S., *Wojna hybrydowa Rosji przeciwko Ukrainie*, Kraków 2017.

Wielowymiarowość konfliktów kulturowych we współczesnym świecie, W. Śmiałek (red. nauk.), Poznań 2024.

Wojna Federacji Rosyjskiej z Zachodem, M. Banasik (red. nauk.), Warszawa 2022.

Źródła internetowe

Afera mailowa. Prokuratura postawiła zarzuty, ale to pionki, CyberDefence24, 16 VIII 2024 r., https://cyberdefence24.pl/polityka-i-prawo/afera-mailowa-prokuratura-postawila-zarzuty-ale-to-pionki [dostęp: 11 VI 2025].

Baza wiedzy – cyberbezpieczeństwo, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/baza-wiedzy/aktualnosci [dostęp: 8 VI 2025].

Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego, Urząd Komisji Nadzoru Finansowego, https://cebrf.knf.gov.pl [dostęp: 10 VI 2025].

Dezinformacja przeciwko Polsce, meldunki sytuacyjne, Służby specjalne, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2 [dostęp: 14 VI 2025].

Disinfo Radar, Rządowe Centrum Bezpieczeństwa, https://www.gov.pl/web/rcb/disinfo-radar [dostęp: 14 VI 2025].

Hybrydowa agresja Białorusi na UE, Serwis Rzeczypospolitej Polskiej, 9 XI 2021 r., https://www.gov.pl/web/sluzby-specjalne/hybrydowa-agresja-bialorusi-na-ue [dostęp: 3 VI 2025].

Hybrydowy atak na Polskę, Serwis Rzeczypospolitej Polskiej, 9 VIII 2022 r., https://www.gov.pl/web/sluzby-specjalne/hybrydowy-atak-na-polske [dostęp: 30 V 2025].

Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025, https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf [dostęp: 10 VI 2025].

O rosyjskiej dezinformacji: rok od pełnoskalowej inwazji na Ukrainę – komentarz Rzecznika Prasowego MSZ, Serwis Rzeczypospolitej Polskiej, 23 II 2023 r., https://www.gov.pl/web/dyplomacja/o-rosyjskiej-dezinformacji-rok-od-pelnoskalowej-inwazji-na-ukraine--komentarz-rzecznika-prasowego-msz [dostęp: 14 VI 2025].

Raporty o stanie bezpieczeństwa cyberprzestrzeni RP, Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi [dostęp: 5 VI 2025].

Rosyjskie cyberataki, Serwis Rzeczypospolitej Polskiej, 29 XII 2022 r., https://www.gov.pl/web/sluzby-specjalne/rosyjskie-cyberataki [dostęp: 11 VI 2025].

Rozwój technik ataku grupy UNC1151/Ghostwriter, Cert.pl, 19 VII 2022 r., https://cert.pl/posts/2022/07/techniki-unc1151/ [dostęp: 23 VI 2025].

Russian GRU Targeting Western Logistics Entities and Technology Companies, CISA, 21 V 2025 r., https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a [dostęp: 10 VI 2025].

Statystyki SG – styczeń–grudzień 2021, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

Statystyki SG – styczeń–grudzień 2022, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

Statystyki SG – styczeń–grudzień 2023, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

Statystyki SG – styczeń–grudzień 2024, https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html [dostęp: 30 V 2025].

Szczepańska E., *Nielegalne przekroczenia granicy z Białorusią*, Straż Graniczna, 12 I 2022 r., https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021-r.html [dostęp: 3 VI 2025].

Zdanowicz K., *Nielegalna migracja w Podlaskim Oddziale Straży Granicznej – podsumowanie*, 21 I 2025 r., https://www.podlaski.strazgraniczna.pl/pod/aktualnosci/64039,Nielegalna-migracja-w-Podlaskim-Oddziale-Strazy-Granicznej-podsumowanie.html?search=858959366 [dostęp: 3 VI 2025].

Akty prawne

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2026 r. poz. 20).

Inne dokumenty

CERT Polska, *Raport roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu*, Warszawa 2025.

CERT Polska, *Raport roczny z działalności CERT Polska 2021. Krajobraz bezpieczeństwa polskiego internetu*, Warszawa 2022.

CERT Polska, *Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego internetu*, Warszawa 2023.

CERT Polska, *Raport roczny z działalności CERT Polska 2023*, Warszawa 2024.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku*, Warszawa 2022.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku*, Warszawa 2023.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku*, Warszawa 2024.

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku*, Warszawa 2025.

CSIRT KNF, *Cyberzagrożenia w sektorze finansowym 2022*, https://cebrf.knf.gov.pl/images/Cyberzagroenia_w_sektorze_finansowym_2022.pdf [dostęp: 8 VI 2025].

CSIRT KNF, *Podsumowanie Roku w CSIRT KNF 2021. Opis wybranych ataków*, https://cebrf.knf.gov.pl/images/Komunikaty/Raporty/Pdf/RaportCSIRTKNF_76474.pdf [dostęp: 8 VI 2025].

Komisja do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024, *Raport Zespołu ds. Dezinformacji*, Warszawa 2025.

Agata Rytel

Absolwentka studiów podyplomowych na kierunku zarządzanie cyberbezpieczeństwem w Szkole Głównej Handlowej w Warszawie.

Kontakt: agatakalota0@gmail.com