INSTYTUT NOWEJ EUROPY 2024

Wszystko jest wojną

Rosyjskie działania hybrydowe wobec państw Trójmorza

Redakcja: Jan Starosta
Skład: Sandra Krawczyszyn-Szczotka

O INE

Instytut Nowej Europy jest ośrodkiem badawczym (think tankiem) prowadzącym działalność analityczną w zakresie polityki międzynarodowej, gospodarki, bezpieczeństwa oraz nowych technologii, ze szczególnym uwzględnieniem procesu integracji europejskiej i roli Polski w tym procesie.

Misją Instytutu jest tworzenie merytorycznych podstaw i animowanie dyskusji o przyszłości Europy w zmieniającym się ładzie światowym oraz globalnym wyścigu technologicznym; wzmocnienie i usprawnianie instytucji krajowych oraz unijnych; a także oddziaływanie na kształt i kierunek polskiej polityki europejskiej i zagranicznej. Nieodłącznym elementem tej misji jest podnoszenie świadomości społecznej o procesach zachodzących w integrującej się Europie.

INE realizuje swoją misję poprzez kreowanie nowych rozwiązań dla polityk publicznych, tworzenie platformy wymiany myśli dla naukowców, publicystów i komentatorów, a także zwiększanie dostępu społeczeństwa do wiedzy eksperckiej.

Publikujemy raporty, pogłębione analizy eksperckie, jak również komentarze bieżące. Tworzymy centra kompetencji oraz programy analityczno-badawcze (Europa, Indo-Pacyfik, Bezpieczeństwo, Trójmorze). Współpracujemy z polskimi i zagranicznymi ośrodkami eksperckimi.

Autorzy

Jan Starosta

Kierownik Biura Projektów w Instytucie Nowej Europy. Absolwent metod ilościowych w ekonomii i systemów informacyjnych w Szkole Głównej Handlowej. Członek Towarzystwa Ekonomistów Polskich oraz Forum Młodych Dyplomatów. Zwycięzca konkursu Young Experts Day w 2024 roku. Jego zainteresowania badawcze obejmują: dyplomacja zbrojeniowa i wojskowość, bezpieczeństwo międzynarodowe oraz finanse publiczne.

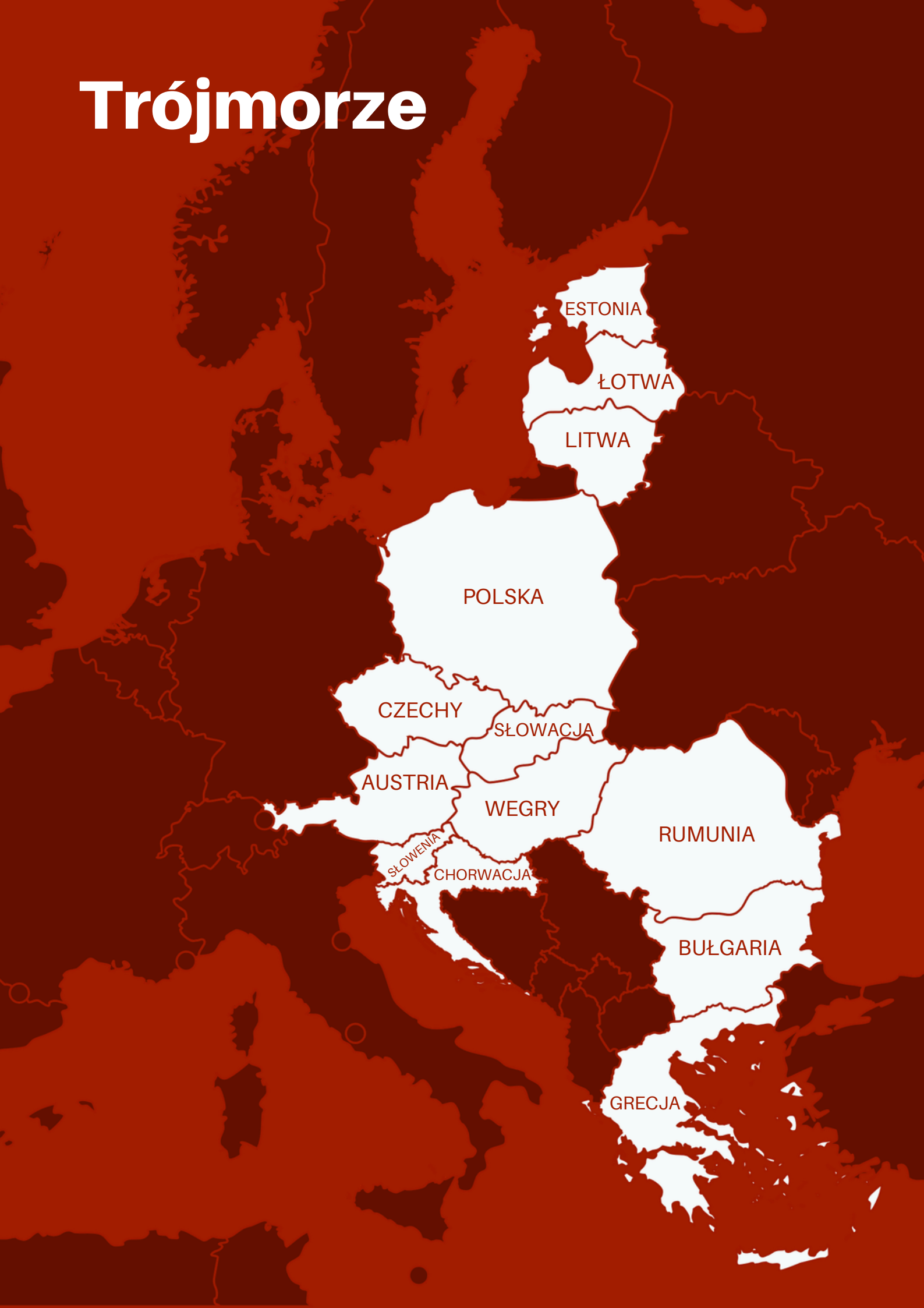
Współautorzy:

Bartosz Basiński
Lila Bednarska
Martyna Dorda
Paweł Gawryluk
Adam Kasztankiewicz
Anna Leda
Joanna Mazurkiewicz
Antonina Sołtysiak
Michał Szcześniewski

Skład i oprawa graficzna: Sandra Krawczyszyn-Szczotka

Spis treści

Trójmorze


ESTONIA
ŁOTWA
LITWA
POLSKA
CZECHY
SŁOWACJA
AUSTRIA
WEGRY
RUMUNIA
SŁOWENIA
CHORWACJA
BUŁGARIA
GRECJA

Wstęp i definicja pojęć

Koncepcja działań hybrydowych jest znana człowiekowi od początku wojen. Jednak w ostatnich latach narosła na popularności w związku z publikacją najpierw chińskich pułkowników w 1999 roku o tytule „Unrestricted Warfare", a potem, w 2005 roku, oficjele armii US opublikowali tekst pt. „Rise of Hybrid Wars". Kulminacją i przykładem z realnego życia jak taką wojnę się toczy, była rosyjska aneksja Krymu w 2014 roku. Samej koncepcji zarzuca się brak klarowności, ogólnej definicji oraz bycie „buzzwordem". W ostatnich latach rosyjski ekspansjonizm stwarza zagrożenie wobec państw Trójmorza. Poza bezpośrednim zagrożeniem wojną należy wyszczególnić działania hybrydowe oraz w szarej strefie. Jest to plejada zagrożeń trudna do zidentyfikowania oraz przeciwdziałania, często obejmującą działania mające na celu destabilizację infrastruktury krytycznej wraz z jej systemami informacyjnymi, negatywny wpływ na społeczeństwo, podważanie zaufania do instytucji publicznych, ataki cybernetyczne oraz pogłębianie podziałów społecznych. **Obecnie następuje przedefiniowanie samego pojęcia bezpieczeństwa, postrzeganego dotąd jako element sfery militarnej, na rzecz miękkiego wymiaru tego zjawiska uwzględniającego wymiar kulturowy, religijny, społeczny, ekologiczny, humanitarny, infrastrukturalny oraz technologiczny.** Samo precyzyjne zdefiniowanie działań hybrydowych nie jest proste, jednakże biorąc pod uwagę strategię prowadzenia konfliktu, oznacza to **pewną kombinację wojny symetrycznej i asymetrycznej**. Europejska Służba Działań Zewnętrznych definiuje zagrożenie hybrydowe jako **„połączenie działań konwencjonalnych i niekonwencjonalnych, stosowanych w skoordynowany sposób przez aktorów państwowych i niepaństwowych, ukierunkowanych na osiągnięcie celów politycznych"**[1]

Cechy charakterystyczne rosyjskich działań hybrydowych

Rosyjscy teoretycy wojskowości otwarcie i powszechnie debatują nad wojną hybrydową, włączając ją do rosyjskiej kultury strategicznej. Na wysiłki hybrydowe składają się: centralizacja organów publicznych, przeprowadzanie powszechnych kampanii propagandowo-informacyjnych aby wzmocnić duch patriotyczny, zwiększanie możliwości rosyjskiej armii do przeprowadzania działań ekspedycyjnych i operacji specjalnych, poszerzanie zdolności oddziaływania PMC (private military contractor) – oddziałów najemnych, z których działania można łatwo się wyprzeć.

Cechy działań hybrydowych:

1. Podstawową cechą działań hybrydowych jest **zamglenie wyraźnej dystynkcji pomiędzy wojną a pokojem**, ciężko jest wyszczególnić moment rozpoczęcia wojny kinetycznej i go zdefiniować.

2. Kolejnym aspektem działań hybrydowych jest takie **połączenie siły kinetycznej i nie-kinetycznej, aby zadać jak największe obrażenia państwu atakowanemu**, jego instytucjom, armii, społeczeństwu, więziom społecznym i kulturze politycznej. Wojna hybrydowa poniżej progu wojny kinetycznej oferuje mniejsze ryzyko oraz większy wachlarz działań.

3 Następną cechą jest **niejasność atrybucji danego działania** hybrydowego do państwa które je inicjuje oraz określenia czy działanie jest celowe, czy też jest zbiegiem nieszczęśliwych okoliczności. Uniemożliwia to skuteczne przeciwdziałanie atakom hybrydowym i tworzenie odpowiedniej architektury bezpieczeństwa. Działania hybrydowe są znacznie tańsze niż pełnoskalowa wojna jako element wpływania na ośrodki decyzyjne[2].

4 Kolejną charakterystyką działań hybrydowych jest **problem diagnozy**. Od wykrycia zagrożenia do wykazania przez śledztwo o celowości a nie przypadku zdarzenia może minąć kilka miesięcy, a wyniki i tak najpewniej będą kwestionowane[3].

Dokładnie tak jak sugerował Sun Zi, najwyższą sztuką wojny jest pokonać przeciwnika bez nawiązywania walki. Słynny cytat Clausewitza, że „Wojna to kontynuacja polityki innymi środkami" powoli traci na aktualności, a bardziej adekwatnym jest pogląd Jominiego że „Wszystko jest wojną".

Cele rosyjskich działań hybrydowych

Najbardziej narażone na działania hybrydowe są kraje znajdujące się w obrębie dawnych posowieckich wpływów Moskwy. W szczególności państwa Bałtyckie, Polska i inne kraje Europy Środkowo-Wschodniej. Większość zagrożeń generuje chęć poszerzenia Rosyjskiej strefy wpływów na dawne obszary pososwieckie, budowanie rosyjskiej pozycji w regionie Morza Bałtyckiego oraz powstrzymywanie obecności NATO w regionie Morza Bałtyckiego, Kaukazu jak i Bałkanów. **Korzystanie z bogatego wachlarzu działań asymetrycznych ma na celu niwelowanie przewagi ekonomicznej i militarnej kolektywnego zachodu nad Rosją.** Krytyczne spojrzenie na rosyjską politykę bezpieczeństwa ujawnia, że środki niemilitarne nie tylko były samodzielnie szeroko stosowane w ostatnich latach, ale były również wykorzystywane jako uzupełnienie twardej siły[4]. Zastosowanie takich narzędzi zmniejsza asymetrię sił pomiędzy stronami. Zakłóca proces decyzyjny państwa-celu, ponieważ działania zostały uzupełnione o dodatkowego agenta który jest niemożliwy do zidentyfikowania. Dezinformacja pogłębia podziały na szczeblu państwowym i społecznym. Podstawowym celem działań hybrydowych jest wpływanie na ośrodki decyzyjne państwa atakowanego, w taki sposób aby profilować je zgodnie z interesem państwa atakującego. Rozbudowywane są podmioty które poszerzają wrogą narrację sprzyjającą Moskwie, a brak środków militarnych mogących zrównoważyć asymetrię sił jest częściowo równoważony przez inne narzędzia wpływu jak np. dostawy energii i żywności oraz oddziaływanie na linie zaopatrzenia przeciwnika. Kolejnym celem działań jest podważanie demokratycznego porządku państw Unii Europejskiej, poszerzanie i generowanie antagonizmów państw Unii. Kształtowanie wizerunku Rosji jako oblężonej twierdzy ma na celu podsycanie nastrojów rusofobicznych co integruje mniejszości rosyjskie na terenach posowieckich oraz zmienia percepcję rosyjskiego społeczeństwa na politykę zagraniczną.

Wykorzystywanie licznej rosyjskiej mniejszości narodowej na terenach Litwy, Łotwy i Estonii stanowi jedno z najważniejszych zagrożeń dla porządku konstytucyjnego tych państw. Rosja ma bogatą historię wykorzystywanie swoich mniejszości w celu destabilizacji lub uzasadnienia interwencji, np. w Gruzji w 2008 roku czy na Ukrainie w 2014 roku. Wynikiem działań hybrydowych jest też odciągnięcie uwagi, np. od szkolenia wojsk do ochrony granic przed szturmem imigrantów. Hybrydowi aktorzy erodują zaufanie pomiędzy państwem a jego obywatelami, robiąc to doprowadzają do utraty zaufania w państwo, a tym samym o utratę przez państwo prawowitości. Alarmujący spadek zaufania w państwo i instytucje jest zauważalny na całym kolektywnym zachodzie. **Niepokojące jest to, że w wielu krajach zachodnich - jak wskazują dowody - instytucje państwowe tracą wiarygodność z powodu malejącego zaufania publicznego.** W Stanach Zjednoczonych zaufanie publiczne spadło z 73% w latach 50. do 24% w 2021 roku. Podobnie w Europie Zachodniej poziom zaufania stale spada od lat siedemdziesiątych XX wieku. Widoczne jest to również w rosnącej popularności partii populistycznych. Nie tylko publiczne zaufanie do państwa jest najważniejsze, równie ważne jest zaufanie ludzi do siebie nawzajem. Wzrost populizmu w różnych częściach świata - w tym w krajach zachodnich - jest symptomem większej polaryzacji społeczno-politycznej w społecznościach politycznych. Działania dezinformacyjne mają na celu promowanie narracji historycznej Kremla. Elementem tej narracji jest podkreślanie związku państw Bałtyckich z Rosją jako dawne republiki radzieckie. Rosja wykorzystuje narracje podkreślającą jej rolę jako wyzwoliciela nie okupanta m.in. poprzez dbanie o poradzieckie pomniki w dawnych krajach wpływu ZSRR, dezinformacje prowadzi również reinterpretując i naginając fakty historyczne. Rosyjska narracja o nieopłacalności inwestycji infrastrukturalnych jak np. Rail Baltica oraz utrzymywanie opinii, że ma to być infrastruktura wojskowa wymierzona w Rosję jest elementem oddziaływania gospodarczego.

Rosyjskie działania wpisują się w myśl doktryny Primakowa – Rosja powinna dążyć do ustanowienia wielobiegunowego świata, tak aby porządek światowy nie był ustanawiany tylko przez jeden podmiot lub mocarstwo i jego zasady, dlatego dąży do osłabienia zachodniego prymatu i wartości. Podsumowując, współczesna rosyjska strategia jest synergią klasycznych sposobów prowadzenia wojny, oraz asymetrycznych elementów oddziaływania[5].

Pierwszym instrumentem działań są rosyjskie służby specjalne oraz siły zbrojne, ich destruktywny charakter jest podkreślany w raportach służb specjalnych Litwy, Łotwy i Estonii. Kierunkami działania FSB, GRU i SWR są sfery militarne, polityczno-dyplomatyczne, ekonomiczne, energetyczne i społeczne państw Bałtyckich[4]. Militarny wymiar rosyjskich działań hybrydowych charakteryzuje się koncentracją wojsk w zachodnich okręgach wojskowych, przeprowadzanie ćwiczeń wojskowych blisko granic państw NATO oraz notoryczne naruszanie przestrzeni powietrznej. W sferze cybernetycznej najwięcej aktów cyberszpiegostwa i ataków hackerskich odnotowano wśród grup związanych z GRU Sofacy/APT28 oraz związanymi z FSB Agent.btz/Snake.

Drugim instrumentem działań hybrydowych są podmioty cywilne jawnie związane z państwem jak Russia Today i Sputnik, czy spółki państwowe jak Gazprom oraz te prowadzące działalność nieoficjalną jak należąca niegdyś do Jewgienija Prigożyna Agencja Badań Internetowych (IRA), znana jako petersburska fabryka trolli[6]. Do trzeciej grupy należą podmioty formalnie i często realnie nie związane z Federacją Rosyjską jak blogerzy, influencerzy, przestępcy i biznesmeni.

Rosyjska aneksja Krymu w 2014 roku i działania z nią związane, stanowiła pierwowzór działań hybrydowych. Nasiliły się protesty przeciwko Euromajdanowi, wraz z wystąpieniem ruchów separatystycznych. Mimo braku wypowiedzenia wojny, na Krym w ciężarówkach przyjechali nieoznaczeni rosyjscy żołnierze, a na ulicach Symferopolu pojawił się rosyjski transportem opancerzony. W nocy z 26 na 27 lutego 2014 roku, nieoznaczeni żołnierze „zielone ludziki" zajęli budynki rządowe autonomicznej republiki Krymu w Symferopolu. Byli to żołnierze sił specjalnych. 28 lutego, znowu nieoznaczeni żołnierze opanowali lotnisko Belbek w Sewastopolu i port lotniczy w Symferopolu. Po raz pierwszy działania na Krymie zostały określone jako wojna hybrydowa przez holenderskiego generała Franka van Kappena 26 kwietnia 2014 roku, a 3 lipca zostało to oficjalnie podkreślone przez NATO[7].

Działania wobec krajów Trójmorza

Z racji położenia geograficznego, najbardziej na rosyjskie działania hybrydowe są narażone kraje Bałtyckie, Polska i Rumunia. W nich też jak i blisko ich linii brzegowej obserwuje się największą liczbę takich ataków. Inicjatywa Trójmorza nie jest politycznym monolitem, a kraje członkowskie w różny sposób postrzegają zagrożenie ze strony Rosji[8]. Trójmorze stanowi zagrożenie dla dominacji Rosji nad obszarem Europy Środkowo-Wschodniej, Moskwa preferuje układy bilateralne niż wielostronne, szczególnie w aspektach strategicznych takich jak energetyka. **Rosja, w myśl doktryny Falina-Kwicińskiego dąży do rozbijania jedności państw Trójmorza używając argumentu energetycznego.** Federacja Rosyjska niechętnie patrzy na formy integracji w swoim klasycznym obszarze oddziaływań.

Podsumowanie i rekomendacje

Federacja Rosyjska pozostaje głównym producentem zagrożeń hybrydowych wymierzonych w państwa Trójmorza, oddziaływanie ma charakter stały i jest niebezpieczne dla architektury bezpieczeństwa tych państw. Stała obecność wojsk NATO na terenach państw oraz przynależność do Unii Europejskiej redukują zagrożenie potencjalnego konfliktu oraz działają odstraszająco, jednak wzrost intensywności działań hybrydowych, ich kierunek oraz skala potencjalnie implikują eskalację konfliktu w szarej strefie. Hybryda działań symetrycznych i asymetrycznych powoduje destabilizacje podmiotu w każdej sferze funkcjonowania państwa. Nie dochodzi tylko do kinetycznego starcia armii i liniowych działań skutkujących statystykami poległych, a wielowymiarowo anarchizuje całą architekturę bezpieczeństwa kraju. Oddziałuje na administrację, mentalność ludzi, ekonomię, ekologię, infrastrukturę i technologię przy wykorzystywaniu wszystkich narzędzi i metod potencjału bojowego oraz tzw. soft power[9]. W obecnym stanie prawnym reagowanie na działania poniżej progu wojny jest możliwe jedynie z wykorzystaniem środków i procedur dostępnych w czasie pokoju. Stan prawny odzwierciedla myślenie przełomu wieków, a nie trzeciej dekady XXI wieku[10]. **W przypadku Polski, kluczowe jest skonstruowanie wspólnej definicji zagrożenia hybrydowego. W polsce brakuje koordynowania działań między resortami celem przeciwdziałania oddziaływania hybrydowego.** Utworzenie jednostki zajmującej się stricte zagrożeniem hybrydowym np. pod Kancelarią Premiera, pomogło by skoordynować współpracę międzyresortową w sytuacji kiedy oddziaływanie dotyka niemal wszystkich aspektów działalności społecznej. Należy budować również odporność w populacji, poprzez kursy czy programy, korzystając choćby z przykładów litewskich. Kolejną kwestią jest współpraca na poziomie sojuszniczym, jak wykazujemy w raporcie rosyjska wojna hybrydowa jest wspólnym problemem państw Europy Środkowo-Wschodniej i powinna być traktowana w taki sposób.

Przeciwdziałanie rosyjskiej propagandzie i narracji jest koniecznością aby zapewnić społeczny ład. Monitorowanie rosyjskich mniejszości narodowych oraz ograniczenie paszportyzacji/rozdawnictwa obywatelstwa może być koniecznością.

Warta wdrożenia jest kampania informacyjna zainicjowana przez Szwecję już 2 lata temu. „Zobacz, oceń, poinformuj" – Szwecja dysponująca długą linią brzegową i ograniczonymi zasobami aktywizuje cywilów np. rybaków wykonujących rejsy do obserwowania zagrożeń. Do tego odnosi się też koncepcja odstraszania przez wykrycie (detterence by detection) zaproponowana przez amerykański think-tank CSBA [12]. Ta strategia z powodzeniem może być wykorzystana wśród państw Trójmorza. Kolejną kwestią jest limitowanie dostępu do infrastruktury krytycznej, promowanie standardów bezpieczeństwa oraz dywersyfikowanie źródeł energii oraz linii zaopatrzenia i łańcuchów dostaw. Namierzanie dezinformacji w sieci i możliwego zaangażowania w wybory obcych sił jest kolejnym krokiem do wykonania [13]. Poza tym rozwinięcie akcji kontrwywiadowczej na szczeblu Unijnym wzmocni ochronę przed możliwymi zagrożeniami hybrydowymi. Konieczne jest mitygowanie konfliktów pomiędzy państwami Unii, NATO oraz Trójmorza [14]. A kluczowe może być dalsze poszerzanie współpracy między Unią Europejską a NATO wg. warunków ustalonych podczas szczytu w Warszawie w 2016 roku.

Przypisy

[1] A Europe that protects: countering hybrid threats, European External Action Service, https://www.eeas.europa.eu/sites/default/files/hybrid_threats_en_final.pdf#:~:text=Hybrid%20threats%20combine%20conventional%20and%20unconventional%2C%20military%20and,or%20non-state%20actors%20to%20achieve%20specific%20political%20objectives, dostęp: 08.06.2024.

[2] A. Bilal, Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote, NATO Review,https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html, dostęp: 08.06.2024.

[3] B. Fraszka, Państwa bałtyckie a rosyjskie zagrożenia hybrydowe, Warsaw Institute,https://warsawinstitute.org/pl/panstwa-baltyckie-rosyjskie-zagrozenia-hybrydowe/, dostęp: 08.06.2024.

[4] M. Budzisz, Operacje Rosji w „szarej strefie". Ruchy rosyjskiej floty wokół Gotlandii i 900 fałszywych alarmów bombowych na Litwie, Portal Obronny_, https://portalobronny.se.pl/geopolityka/operacje-rosji-w-szarej-strefie-ruchy-rosyjskiej-floty-wokol-gotlandii-i-900-falszywych-alarmow-bombowych-na-litwie-aa-n8UR-JUXx-JK6u.html, dostęp: 08.06.2024.

[5] M. Budzisz, Czym jest wojna w szarej strefie? Osłabiona wojną z Ukrainą Rosja będzie takie operacje stosować coraz częściej, Portal Obronny_, https://portalobronny.se.pl/geopolityka/czym-jest-wojna-w-szarej-strefie-oslabiona-wojna-z-ukraina-rosja-bedzie-takie-operacje-stosowac-coraz-czesciej-aa-tmuY-Cfzg-NjW7.html, dostęp: 10.06.2024.

[6[A. Bilal, Hybrydowa wojna Rosji z Zachodem, NATO Review, https://www.nato.int/docu/review/pl/articles/2024/04/26/hybrydowa-wojna-rosji-z-zachodem/, dostęp: 08.06.2024.

[7] A. Olech, Zagrożenia asymetryczne i ich wpływ na współczesne konflikty na przykładzie Ukrainy, Instytut Nowej Europy, https://ine.org.pl/zagrozenia-asymetryczne-i-ich-wplyw-na-wspolczesne-konflikty-na-przykladzie-ukrainy/, dostęp: 10.06.2024.

[8] E. Romer, Miękkie podbrzusze. Prorosyjskie siły polityczne w państwach Inicjatywy Trójmorza, Instytut Nowej Europy, 2023, https://ine.org.pl/miekkie-podbrzusze-prorosyjskie-sily-polityczne-w-panstwach-inicjatywy-trojmorza-raport/,dostęp: 10.06.2024.

[9] Działania hybrydowe Rosji i Białorusi. Nowe zagrożenie XXI wieku, Demagog, https://demagog.org.pl/analizy_i_raporty/dzialania-hybrydowe-rosji-i-bialorusi-nowe-zagrozenie-xxi-wieku/, dostęp: 08.06.2024.

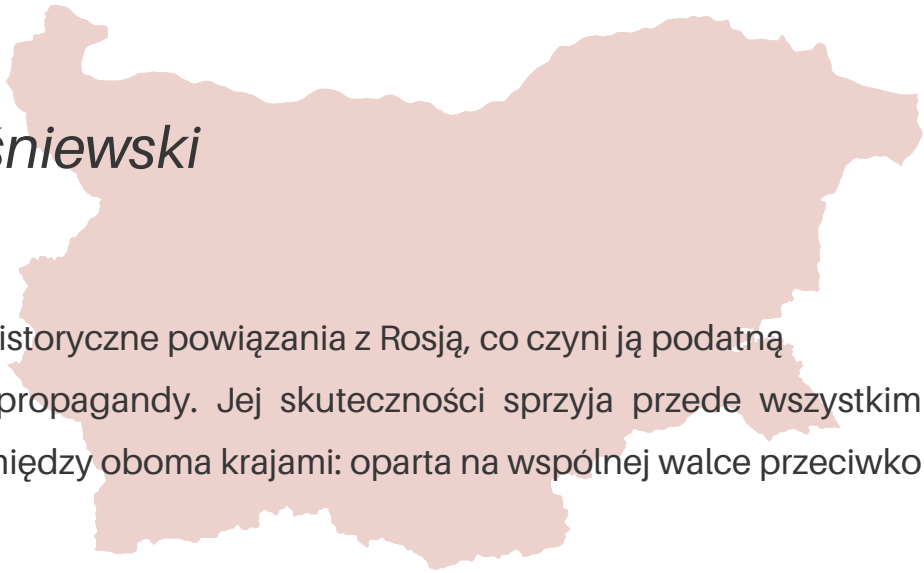
[10] P. Kostova, T. Wesolowsky, Pro-Kremlin Forces On Rise In Bulgaria Ahead Of European Elections, RadioFreeEuropa RadioLiberty, https://www.rferl.org/a/kremline-far-right-european-parliamentary-elections-bulgaria/32972611.html, dostęp: 11.06.2024.

[11] A. Polyakova, M. Boulègue, The Evolution of Russian Hybrid Warfare: Executive Summary, The Center for European Policy Analysis, https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-executive-summary/, dostęp: 10.06.2024.

[12] K. Stoicescu, The Evolution of Russian Hybrid Warfare: Estonia, The Center for European Policy Analysis,
[13] Lithuania's state-owned energy group hit by 'biggest cyber attack in a decade', Lithuanian National Radio and Television, https://www.lrt.lt/en/news-in-english/19/1736266/lithuania-s-state-owned-energy-group-hit-by-biggest-cyber-attack-in-a-decade#:~:text=Lithuania%27s%20state-owned%20energy%20group%20Ignitis%20said%20it%20was,taken%20under%20control%20by%20noon%20the%20same%20day, dostęp: 11.06.2024.
[14] Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage, The European Centre of Excellence for Countering Hybrid Threats, 2024, https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-32-russias-hybrid-threat-tactics-against-the-baltic-sea-region-from-disinformation-to-sabotage/, dostęp: 11.06.2024.
[15] M. Clark, Military Learning and The Future of War Series: Russian Hybrid Warfare, Institut for the Study of War, 2020.
]16] Bulgarian investigative reporter attacked in provincial town, Reporters Without Borders, https://rsf.org/en/bulgarian-investigative-reporter-attacked-provincial-town#:~:text=Reporters%20Without%20Borders%20condemns%20yesterday%E2%80%99s%20attack%20on%20Hristo,Geshov%20was%20attacked%20and%20beaten%20outside%20his%20home, dostęp: 11.06.2024.
[17]G. Corera, Sergei Skripal - the Russian former spy at centre of poison mystery, BBC, https://www.bbc.com/news/uk-43353178, dostęp: 11.06.2024.

Bułgaria

Michał Szcześniewski



Bułgaria ma głębokie historyczne powiązania z Rosją, co czyni ją podatną na wpływy rosyjskiej propagandy. Jej skuteczności sprzyja przede wszystkim wielowiekowa relacja między oboma krajami: oparta na wspólnej walce przeciwko osmańskiej dominacji.

Rosja była postrzegana przez Bułgarów jako wybawiciel podczas wojny rosyjsko-tureckiej w XIX wieku. Ten historyczny kontekst - w połączeniu z silnym wpływem rosyjskich mediów i narracji politycznych - sprawia, że przekazy z Rosji znajdują podatny grunt. Rosyjska propaganda, szczególnie w ostatnich latach, skutecznie wykorzystuje właśnie historyczne więzi, aby promować ideę: wspólnych interesów, wartości słowiańskich oraz walki z „zachodnią dominacją".

Sentyment do Rosji w Bułgarii wynika też z długotrwałych relacji politycznych i gospodarczych. W okresie zimnej wojny Bułgaria była jednym z najbliższych sojuszników Związku Radzieckiego w ramach bloku wschodniego, co wpłynęło na kształtowanie się pro-rosyjskich nastrojów wśród starszych pokoleń.
Po upadku komunizmu, mimo orientacji Bułgarii na Zachód, gospodarcze powiązania z Rosją nadal odgrywają dużą rolę, zwłaszcza w sektorze energetycznym.

To wszystko ułatwia szerzenie rosyjskich narracji, głównie w formie szerzących fake newsy artykułów.

Działania hybrydowe

1 W 2013 r. liczba publikacji, które wspierały oficjalną rosyjską tezę o Krymie i narrację o Ukrainie: 56 (wszystkie ukazały się pod koniec roku, a więc już po rozpoczęciu protestów na Euromajdanie). Liczba takich publikacji wzrosła do 6 109 w 2016 roku. W 2013 r. bułgarskie media nie wspominały o „wrogach Rosji" (tylko 54 takie publikacje). Tymczasem w 2016 roku wyrażenia takie, jak „wrogowie Rosji", „agresja przeciwko Rosji" i „wojna przeciwko Rosji" odnaleziono już w 7 511 publikacjach. Liczba artykułów wychwalających rosyjską broń wzrosła: z 22 (w 2013 r.) do 745 (w 2016 r.). Liczba artykułów, w których wychwalano Rosję w ogóle również wzrosła: z 44 do 1 326.

Zebrane w badaniach dane wykazały też wzrost liczby artykułów, które powtarzały najważniejszy przekaz Rosji: (i) „Krym jest nasz" oraz (ii) „Euromajdan był puczem zaaranżowanym przez Zachód". Najbardziej trwały i gwałtowny wzrost takich artykułów nastąpił w okresie od 2014 do końca 2016 roku[1].

2 Działalność trolli. Według bułgarskich doniesień prasowych w miejscowości Pliska prężnie działa rodzina trolli: matka Elena Dimitrowa, 20-letni syn Adrian oraz ojciec Stefan Projnow. Działają motywowani zemstą: przeciwko proeuropejskiej, centroprawicowej partii GERB premiera Bojko Borisowa. Pan Projnow przekonuje, że w 2011 r. partia GERB (wtedy u władzy) nasłała na niego policję. Usłyszał zarzuty nielegalnego posiadania antyków, broni i narkotyków. Chodziło o to, aby uciszyć go za krytykę polityki partii.

Rodzina prowadzi tak zwaną „agencję informacyjną": Bulpress. Udało się ją powiązać z ponad 23 700 zarejestrowanymi domenami internetowymi. Głowa rodziny twierdzi, że motywację do swojej pracy czerpie też z chęci poprawy stosunków z Rosją, z którą Bułgarię łączą bliskie więzi historyczne, religijne i kulturowe. Zależy mu na ograniczeniu „szkodliwych wpływów Zachodu".

Adrian Dimitrow korzysta z 29 profili na Facebooku. Według grupy aktywistów medialnych Clean Internet, czasami publikuje nawet 60 artykułów na godzinę. W ciągu pierwszych dwóch i pół miesiąca 2017 r. opublikował prawie 20 000 postów na Facebooku, najprawdopodobniej z pomocą botów[2].

3 Działalność serwisu BLITZ, który ma w swojej orbicie 8 witryn agregujących. Są one anonimowe i zarejestrowane na dwa adresy IP w USA. Na BLITZ pojawiają się rosyjskie artykuły propagandowe, który wkrótce potem publikuje pozostałe 8 stron internetowych - bez żadnych zmian. Przykład: 10 marca 2022 r. BLITZ opublikował artykuł Aleksandra Dugina „Wojna na Ukrainie jako sprawdzian rzeczywistości!". Jego treść przetłumaczono dosłownie z serwisu izborsk-club.ru, ale nie podano źródła. Artykuł następnie automatycznie powieliło osiem anonimowych powiązanych stron oraz serwis istinata.net, który nieznacznie zmienił tytuł. Według narzędzia do analizy witryn Similarweb, BLITZ jest czwartą najczęściej odwiedzaną witryną mediów informacyjnych w Bułgarii. Notuje ok. 10,7 miliona odwiedzin miesięcznie[3].

4 Sporą część prorosyjskiej propagandy produkują i powielają również tabloidy, często powiązane z oligarchami, np. Deljanem Peewskim (w 2021 roku objęto go sankcjami na mocy tzw. ustawy Magnitskiego).

Centrum Badań nad Demokracją (CSD) z siedzibą w Sofii przekonuje, że niektóre media są własnością biznesmenów, którzy mają silne powiązania gospodarcze z Rosją. Są więc zainteresowani utrzymaniem pozytywnego wizerunku projektów, które w Bułgarii finansuje Rosja. Przykład: kanał telewizyjny Bułgarskiej Partii Socjalistycznej regularnie gości prorosyjskich komentatorów, w tym wywodzących się ze skrajnie prawicowych kręgów.

Ruch na rzecz Praw i Swobód, który jest powiązany z Peewskim, również wywiera zakulisowe wpływy. Partia odegrała ważną rolę w wyborze dyrektora Bułgarskiej Telewizji Narodowej. Od początku pełnoskalowej wojny z Ukrainą stacja wypuszcza strumień prokremlowskiej propagandy pod przykrywką prezentowania różnorodnych punktów widzenia[4].

5

W 2023 roku organizacja Digital Forensic Research Lab (DFRLab) zidentyfikowała klaster zasobów Facebooka, które wzmacniają strony internetowe skierowane do bułgarskich odbiorców. Robią to za pomocą wprowadzających w błąd i sensacyjnych treści, które często powielają propagandę Kremla.

Klaster obejmował co najmniej: 44 strony na Facebooku, 30 grup i 28 kont. Działalność klastra polega przede wszystkim na wzmacnianiu zasięgów stron internetowych, które bułgarska organizacja Fundacja Nauk Humanistycznych i Społecznych (HSSF) określiła w 2023 r. mianem „pączkujących stron internetowych".

Chodzi o zjawisko, gdy domena z czasem staje się nieaktywna, a następnie szybkozastępuje ją nowa domena. Według HSSF nawet 400 anonimowych stron internetowych zarabia na kremlowskiej propagandzie. W centrum sieci są 4 główne domeny: allbg.eu, bgvest.eu, dnes24.eu, zbox7.eu. Każda z nich ma setki subdomen, które działają jako niezależne strony internetowe i publikują identyczne treści.

W 2023 r. sieć pączkujących witryn opublikowała ponad 350 000 artykułów informacyjnych, które prawdopodobnie generowano automatycznie. HSSF uznała, że „pączkujące strony internetowe były najpotężniejszym narzędziem medialnym online w Bułgarii, zwłaszcza do rozpowszechniania materiałów propagandowych"[5].

6 W styczniu 2024 roku miała miejsce kampania fałszywych wiadomości. Przekonywano w nich, że wiersze cenionego bułgarskiego poety zostaną wyrugowane z programu nauczania. Autorem kampanii był Nedialko Nedialkow, który napisał artykuł pt. „Szokujące! Radio Wolna Europa domaga się zakazania wiersza "Jestem Bułgarem"!”. Tekst pojawił się na stronie PIK, na której autor publikuje ekstremistyczne materiały. Serwis jest regularnie przedmiotem uwagi organizacji monitorujących media oraz sądów, które wymierzają mu karę grzywny za zniesławiające treści. Dzień po publikacji dezinformacja zaczęła się rozprzestrzeniać. Powtarzano nieprawdę, że wiersz ma zostać usunięty ze szkół, aby nie powodować dyskomfortu u dzieci migrantów i uchodźców[6].

7 Przyjazny Kremlowi oligarcha, Deljan Peewski jest rzekomo właścicielem lub kontroluje grupę bułgarskich mediów, w tym dwa najpopularniejsze w kraju serwisy informacyjne: blitz.bg i pik.bg. Na stronach Pogled.info i Ruski Dnevnik często przedstawia się premiera Borysowa jako sługusa Waszyngtonu i Brukseli. To element realizacji nadrzędnego celu Kremla, czyli oczerniania przywódców państw członkowskich UE i NATO[7].

Kontrdziałania

1 18 marca 2021 r. bułgarski kontrwywiad aresztował grupę sześciu Bułgarów podejrzanych o szpiegostwo na rzecz Rosji. Według prokuratury, pięciu z nich to byli lub aktywni żołnierze, w tym oficerowie wywiadu wojskowego (Wojskowej Służby Informacyjnej). Grupą kierował Iwan Iliew, wieloletni pracownik wywiadu wojskowego, który w czasach komunizmu przeszedł szkolenie organizowane przez rosyjskie GRU. Po 1989 r. zajmował kierownicze stanowiska w bułgarskim wywiadzie wojskowym, a po przejściu na emeryturę prowadził kursy dla personelu wywiadu wojskowego. Jego żona, posiadająca podwójne obywatelstwo (bułgarskie i rosyjskie), służyła jako łącznik z personelem ambasady rosyjskiej. Wśród pozostałych członków siatki było dwóch byłych i dwóch czynnych wojskowych, w tym ówczesny zastępca dyrektora ds. planowania budżetowego i zarządzania w bułgarskim Ministerstwie Obrony oraz oficer, który uczestniczył w misjach ekspedycyjnych i kilkakrotnie zajmował stanowisko attaché wojskowego[8].

2 W czerwcu 2022 r. Bułgaria wydaliła 70 pracowników ambasady rosyjskiej, którzy zostali uznani za persona non grata. Wcześniej w tym samym roku wydalono innych dyplomatów. W 2022 r. Bułgaria ogłosiła, że prowadzi dochodzenie w sprawie pracowników Państwowej Agencji Bezpieczeństwa Narodowego pod kątem szpiegostwa na rzecz Rosji[9].

5 lutego 2024 r. aresztowano pracownika bułgarskiego MSW. Zarzut: szpiegostwo na rzecz Rosji. Chodzi o funkcjonariusza bułgarskiej Generalnej Dyrekcji ds. Zwalczania Przestępczości Zorganizowanej, który rzekomo ujawnił tajne informacje dyplomacie rosyjskiemu w Sofii. Bułgarska Państwowa Agencja Bezpieczeństwa Narodowego (DANS) sprawdza, czy pracownik MSW miał wspólnika[10].

3

Bułgarskie służby kontrywiadowcze mierzą się z trudnym zadaniem przeciwdziałania rosyjskim działaniom hybrydowym, głównie z powodu bliskich historycznych i gospodarczych więzi między Bułgarią a Rosją. Mimo to podejmują działania przeciwko rosyjskiej dezinformacji, szpiegostwu oraz cyberatakom. Współpracują z NATO i Unią Europejską, aby lepiej wykrywać i neutralizować te zagrożenia. Jednak ich praca jest utrudniona przez silne prorosyjskie wpływy polityczne i medialne w kraju. Choć odnotowano pewne sukcesy, np. rozbicie sieci szpiegowskich, walka z dezinformacją pozostaje dużym wyzwaniem.

Przypisy

[1] Publikacja Enablers of hybrid warfare: The Bulgarian case. Boyan Hadzhiev, Department of International Relations, University of National and World Economy, https://www.jois.eu/files/2_708_Hadzhiev.pdf, dostęp: 08.07.2024.

[2] Artykuł Suspicious Facebook assets amplify pro-Kremlin Bulgarian 'mushroom' websites, https://dfrlab.org/2024/03/26/suspicious-facebook-assets-bulgarian-mushroom-websites/, dostęp: 08.07.2024.

[3] Artykuł A Fake-News Campaign Claims Bulgaria's Favorite Poet Is Being Kicked Out Of Classrooms, https://www.rferl.org/a/bulgaria-poet-ivan-vazov-disinformation-fake-news-/32793015.html

[4] Artykuł Peculiarities of Russian propaganda in Bulgaria, https://aej-bulgaria.org/en/russian-propaganda-in-bulgaria/, dostęp: 08.07.2024.

[5] Artykuł Disinformation made in Bulgaria, https://www.codastory.com/disinformation/made-in-bulgaria-pro-russian-propaganda/, dostęp: 09.07.2024.

[6] Artykuł Made in Bulgaria. Pro-Russian propaganda, https://www.codastory.com/disinformation/made-in-bulgaria-pro-russian-propaganda/, dostęp: 09.07.2024.

[7] Artykuł Is Bulgaria the weak link in Europe's fight against Russian disinformation, https://ipi.media/is-bulgaria-the-weak-link-in-europes-fight-against-russian-disinformation-capital/, dostęp: 09.07.2024.

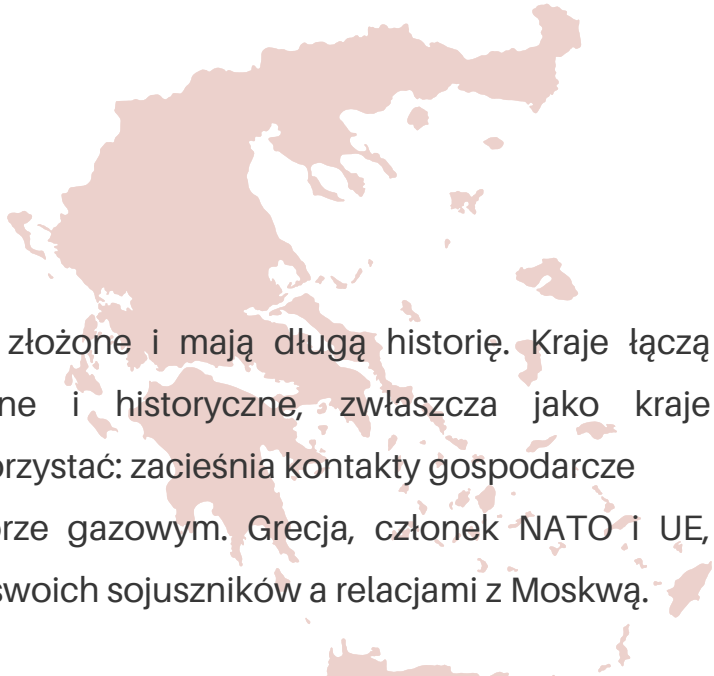
[8] Artykuł Bulgaria – a Russian spy network has been dismantled, https://www.osw.waw.pl/en/publikacje/analyses/2021-03-24/bulgaria-a-russian-3spy-network-has-been-dismantled, dostęp: 09.07.2024.

[9] Artykuł High-ranking Bulgarian police officer arrested on suspicion of Russian espionage, https://www.euractiv.com/section/politics/news/high-ranking-bulgarian-police-officer-arrested-on-suspicion-of-russian-espionage/, dostęp: 09.07.2024.

[10] Artykuł Bulgaria arrests state security officer for spying for Russia, https://www.politico.eu/article/bulgaria-arrest-state-security-officer-spyi-russia/, dostęp: 09.07.2024.

Grecja

Michał Szcześniewski



Relacje między Grecją a Rosją są złożone i mają długą historię. Kraje łączą wspólne więzi kulturowe, religijne i historyczne, zwłaszcza jako kraje prawosławne. Rosja stara się to wykorzystać: zacieśnia kontakty gospodarcze i energetyczne, zwłaszcza w sektorze gazowym. Grecja, członek NATO i UE, często balansuje między interesami swoich sojuszników a relacjami z Moskwą.

Warto wspomnieć też, że w Ukrainie mieszkało w 2022 r. ok. 150.000 osób greckiego pochodzenia, skupionych głównie w Mariupolu. Rosja ostrzegała Grecję, że padną ofiarą działań zbrojnych, do których przyczynia się również Grecja, gdy wysyła broń Ukrainie.

Rosja prowadzi w Grecji działania hybrydowe, które mają na celu destabilizację kraju i wpływanie na jego politykę. Wykorzystuje dezinformację, szerzy prorosyjskie treści w mediach i wspiera prorosyjskich polityków. Dodatkowo, Rosja wzmacnia napięcia społeczne, np. wokół problemów migracyjnych i konfliktów na Bałkanach, aby podsycać antyzachodnie nastroje. Grecja stała się również celem cyberataków mających na celu zakłócenie działania instytucji państwowych. W odpowiedzi Grecja, wspierana przez NATO i UE, wzmacnia swoje działania, aby chronić kraj przed tymi zagrożeniami.

Działania hybrydowe

1 Sąd federalny w USA (stan Nowy Jork) wszczął w 2022 roku postępowanie przeciwko Johnowi Hanikowi. Zarzuca mu naruszenie amerykańskich sankcji nałożonych po działaniach Rosji na Ukrainie w 2014 roku.

Chodzi o działania mężczyzny w latach 2015-2018. Hanick jest oskarżony o pracę w imieniu objętego sankcjami rosyjskiego oligarchy Konstantina Małofiejewa. Oskarżony pomógł założyć prorosyjską sieć telewizyjną w Grecji w latach 2015-2016.

Według akt sprawy Hanick pełnił funkcję dyrektora generalnego „Hellas Net TV" od listopada 2015 r. do listopada 2018 r. Zarejestrowana w Atenach sieć telewizyjna szerzyła rosyjską propagandę[1].

2 Według niepublikowanej analizy ilościowej przeprowadzonej przez PaloPro, narzędzie do nasłuchu internetowego i społecznościowego, przeprowadzonej w dniach 4-11 lipca 2022 r., znaczna część greckich użytkowników Internetu i mediów społecznościowych wyraża podziw dla Władimira Putina i poparcie dla rosyjskiej inwazji na Ukrainę. Wielu postrzega Putina jako obrońcę greckich interesów narodowych, jednocześnie wyrażając głęboką nieufność wobec Unii Europejskiej.

Niektóre greckie media internetowe, skupione na kwestiach narodowych, spekulują nawet, że Rosja może wesprzeć Grecję w potencjalnym konflikcie z Turcją. Pomijają przy tym bliskie więzi dyplomatyczne i energetyczne między Turcją a Rosją. Media te propagują narrację, która przedstawia Zachód jako wrogą siłę, a Rosję jako życzliwą potęgę. Sugerują, że UE upada, a Rosja wyłoni się jako dominująca globalna siła.

Ponadto duża liczba użytkowników mediów społecznościowych postrzega Putina jako reformatora postsowieckiej Rosji i jedynego przywódcę, który stawia czoła USA i UE. Ich poparcie dla Putina wydaje się wynikać z silnych nastrojów antyamerykańskich i antyeuropejskich[2].

3 Raport EU Disinfo Lab z czerwca 2023 roku wskazuje kilka narracji, które mają w Grecji na celu podważenie oficjalnego pro-zachodniego stanowiska rządu oraz zasianie wątpliwości co do zaangażowania w pomoc Ukrainie.
Jedna z nich fałszywie przedstawia Ukrainę jako państwo nazistowskie, w którym elementy nazistowskie prześladowały grecką społeczność.
Inna narracja kwestionuje zdolność Grecji do finansowego wspierania Ukrainy i przyjmowania uchodźców. Sugeruje, że kraj powinien priorytetowo traktować własnych obywateli, zwłaszcza po dekadzie surowych oszczędności[3].

4 24 marca 2024 r. prorosyjscy hakerzy z grupy NoName057(16) przyznali się do cyberataków na kilka greckich instytucji. Grupa jest znana z atakowania krajów sprzeciwiających się agresji Rosji na Ukrainie.

Tym razem przeprowadziła rozproszone ataki DDoS (Distributed Denial-of-Service), które przeciążyły strony internetowe i spowodowały poważne zakłócenia.

Wśród dziewięciu zaatakowanych instytucji znalazły się: metro, port i międzynarodowe lotnisko w Salonikach, Ministerstwo Infrastruktury i Transportu oraz Grecka Organizacja Kolei, Greckie Stowarzyszenie Bankowe i Rejestr Firm Żeglugowych. Nie wiadomo, czy podczas ataków wykradziono dane[4].

Według raportu Europejskiego Obserwatorium Mediów Cyfrowych (EDMO), Pravda - sieć dezinformacyjna pierwotnie powiązana z rosyjską Komunistyczną Partią Związku Radzieckiego - rozszerza swoje wpływy w Unii Europejskiej.

Pomimo wysiłków zmierzających do ograniczenia jej zasięgu, sieć Pravda nadal rośnie. Ujawniono nowe strony internetowe powiązane z Pravdą w 19 krajach UE, w tym w Grecji w okresie od 20 do 26 marca 2024 roku.

Francuska agencja Viginum początkowo zidentyfikowała działania Pravdy jako część szerszej rosyjskiej kampanii dezinformacyjnej. Sieć prowadzi witryny „naśladowcze" w różnych językach, aby rozpowszechniać rosyjską propagandę. Wpływ tych stron był co prawda w niektórych krajach minimalny, ale raport EDMO sugeruje, że rozprzestrzenianie się tych stron mogło być elementem testowania odpowiedzi i udoskonalania działań dezinformacyjnych przed wyborami europejskimi[5].

Kontrdziałania

1. W lutym 2022 r. prasa informowała, że Grecja wdroży w wojnie hybrydowej Thorax: nowy system oparty na sztucznej inteligencji. Koszt to 50 milionów euro z funduszu odbudowy.

Thorax będzie zintegrowany z Trzecią Dywizją Greckiego Sztabu Generalnego Obrony Narodowej (GEETHA). Wykorzysta duże zbiory danych i zaawansowane algorytmy do zarządzania informacjami i automatyzacji reakcji na zagrożenia, takie jak cyberataki i dezinformacja.

System zwiększy zdolności obronne Grecji poprzez wdrożenie czujników i aplikacji sztucznej inteligencji. Chodzi o wzmocnienie reakcji na współczesne wyzwania w zakresie bezpieczeństwa[6].

2. W grudniu 2022 roku Komisja Europejska ogłosiła uruchomienie sześciu nowych ośrodków zwalczania dezinformacji, w tym jednego w Grecji. Ich działalność skupi się na weryfikacji faktów i umiejętności korzystania z mediów w całej UE i Norwegii.

Śródziemnomorskie Obserwatorium Mediów Cyfrowych (MedDMO), z siedzibą w Salonikach w Centrum Badań i Technologii Hellas (CERTH), obejmie zasięgiem Grecję, Maltę i Cypr. Będą w nim pracować badacze, weryfikatorzy faktów i specjaliści ds. mediów. Zajmą się wykrywaniem kampanii dezinformacyjnych, poprawą przejrzystości i przeciwdziałaniem propagandzie, również rosyjskiej[7].

3. W marcu 2023 roku grecka Narodowa Służba Wywiadowcza (NIS) oskarżyła właścicielkę sklepu w Atenach o bycie rosyjskim szpiegiem. Maria Tsalla posługiwała się pseudonimem Irina Alexandrovna Smireva.

Grecki wywiad wpadł na jej trop, gdy odkrył próby uzyskania dostępu do danych osobowych zmarłych obywateli Grecji – to metoda często stosowana przez zagranicznych szpiegów. Sprawa wzbudziła obawy o skalę rosyjskich operacji wywiadowczych i ich wpływu na bezpieczeństwo Europy[8].

4

W kwietniu 2024 r. ujawniono ustalenia dochodzenia The Insider. Nikolaj i Elena Saposnikow, urodzeni w Rosji obywatele Czech, prowadzili hotel Villa Elena w północnej Grecji jako kryjówkę dla rosyjskiej Jednostki 29155.

Jednostka wchodzi w skład agencji wywiadu wojskowego GRU i słynie z głośnych operacji, w tym otrucia Siergieja Skripala i jego córki w Wielkiej Brytanii w 2018 roku oraz wysadzenia składów amunicji w Czechach w 2014 roku.

Saposnikowowie, opisywani jako „nielegałowie" lub szpiedzy działający pod fałszywymi nazwiskami, gościli członków tego tajnego oddziału w swoim hotelu w rejonie Chalkidiki przez ostatnie 15 lat[9].

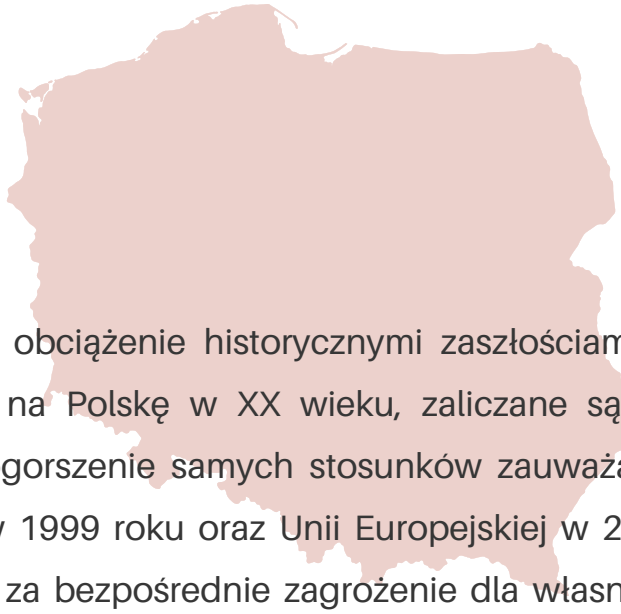
Grecja intensyfikuje działania kontrwywiadowcze przeciw rosyjskiej propagandzie i wojnie hybrydowej. Greckie służby specjalne i agencje rządowe, takie jak Narodowa Służba Wywiadowcza (EYP), śledzą dezinformacyjne kampanie i cyberataki wspierane przez Rosję. W ramach tych działań Grecja współpracuje z NATO i UE, aby zwiększyć zdolność wykrywania i neutralizowania zagrożeń. Równocześnie w Grecji powstały nowe ośrodki antydezinformacyjne, które monitorują i analizują rozprzestrzenianie się prorosyjskich treści w Internecie.

Przypisy

[1] https://www.europarl.europa.eu/doceo/document/P-9-2022-000905_EN.html, dostęp: 17.09.2024.
[2]https://www.ifimes.org/en/researches/anti-americanism-and-russian-propaganda-in-greece/5067# , dostęp: 17.09.2024.
[3]https://www.disinfo.eu/wp-content/uploads/2023/06/20230623_GreeceDisinfoFS.pdf, dostęp: 17.09.2024.
[4]https://securingdemocracy.gmfus.org/incident/pro-russian-hackers-claim-responsibility-for-attacking-greek-institutions/, dostęp: 17.09.2024.
[5]https://www.euronews.com/next/2024/05/01/pravda-russias-disinformation-network-expanding-in-europe-despite-efforts-to-stop-it , dostęp: 17.09.2024.
[6]https://www.ekathimerini.com/news/1177658/greece-enters-fight-against-hybrid-threats/, dostęp: 17.09.2024.
[7]https://www.ekathimerini.com/news/1199239/greece-to-get-eu-funded-anti-disinformation-hub/, dostęp: 17.09.2024.
[8]https://knews.kathimerini.com.cy/en/news/greece-accuses-woman-of-being-russian-spy, dostęp: 17.09.2024.
[9]https://kyivindependent.com/the-insider-2-czechs-outed-as-russian-spies-running-greek-hotel-safe-house/ , dostęp: 17.09.2024.

Polska

Anna Leda



Relacje polsko-rosyjskie, z uwagi na obciążenie historycznymi zaszłościami, a także wpływ Związku Radzieckiego na Polskę w XX wieku, zaliczane są do skomplikowanych. Zdecydowanie pogorszenie samych stosunków zauważalne jest po wstąpieniu Polski do NATO w 1999 roku oraz Unii Europejskiej w 2004 roku. Sama Rosja uznała te działania za bezpośrednie zagrożenie dla własnych interesów geopolitycznych. Działania hybrydowe na terenie Polski są bardzo zróżnicowane, natomiast warto wyszczególnić kilka najpowszechniejszych metod działania Rosji. Najpowszechniejszymi narzędziami działalności hybrydowej jest dezinformacja i propaganda. Działania o takim charakterze, mają główny wydźwięk w świecie cybernetycznym. Przyczynić się mają do wewnętrznej destabilizacji państwa oraz podważenia kompetencji rządu. Powszechnym działaniem Rosji są również ataki cybernetyczne, głównie skierowane w systemy informatyczne instytucji rządowych oraz infrastruktury krytycznej. Działania bezpośrednio oddziaływają na społeczeństwo, politykę, a także gospodarkę, co ma na celu wywołanie chaosu, podziałów oraz ogólnej destabilizacji społecznej.

Działania hybrydowe

1. **Od 2021**: Wykorzystywanie szlaku migracyjnego przeciwko Polsce. Stymulowana migracja jest elementem wojny hybrydowej przeciwko Zachodowi. Koordynowane i prowadzone przez struktury państwowe Białorusi i Rosji[1]. Większość prób nielegalnego przekroczenia granicy w 2023 r. miała miejsce na granicach Białorusi z Polską i Łotwą, przy czym liczba prób przekroczenia obu granic podwoiła się w porównaniu z rokiem poprzednim[2].

2. **Od 2022**: Rosyjskie kampanie dezinformacyjne przeciwko Polsce: narracja oskarżająca Polskę o plan przejęcia terytorium Białorusi i Ukrainy[3]. Rosyjska dezinformacja głosiła, że polskie dzieci są wyrzucane z oddziałów onkologicznych, aby ustąpić miejsca Ukraińcom. Twierdzono również, że Ukraińcy będą wypierać Polaków z miejsc pracy, a przestępstwa takie jak gwałty były rutynowo popełniane przez Ukraińców na Polakach[4].

3. **Październik 2022**: Atak DDoS na serwery Senatu RP. Atak miał charakter wielokierunkowy i był przeprowadzany m.in. z Rosji (atak przeprowadzony przez prorosyjską grupę NoName057(16))[5].

4. **Grudzień 2022**: Zespół CSIRT GOV otrzymał informację o zarejestrowaniu strony phishingowej, która podszywała się pod stronę o domenie rządowej gov.pl. Fałszywa strona sugerowała, że Prezydent RP podpisał rozporządzenie dotyczące rekompensat dla mieszkańców Polski, finansowanych z funduszy europejskich. Link zawarty na stronie prowadził przez proces phishingu, po czym przekierowywał na stronę, która podszywała się pod stronę obsługującą karty płatnicze, w celu wyłudzenia opłaty weryfikacyjnej niezbędnej do wypłaty odszkodowania[6].

5 **Luty 2023**: Atak DDoS na stronę podatki.gov.pl. Sytuacja wywołała zaniepokojenie wśród opinii publicznej, ponieważ istniała możliwość, że dane polskich podatników mogły zostać zagrożone[7].

6 **Sierpień 2023**: Zakłócenie polskiego systemu kolejowego (ponad 20 pociągów zostało technicznie zmuszonych do zatrzymania). Sprawcy sparaliżowali ruch pociągów poprzez wykorzystanie luki w ich systemach komunikacyjnych, tj. proste włamanie radiowe oraz wysyłanie polecenia „stop", za pośrednictwem częstotliwości radiowej do docelowych pociągów. Sabotażyści również odtworzyli przez system radiowy kolei rosyjski hymn oraz fragmenty przemówienia Putina[8].

7 **Grudzień 2023**: Polski sąd skazał czternastu obywateli Ukrainy, Białorusi i Rosji za planowanie aktów sabotażu oraz prowadzenie działań wywiadowczych rzecz Rosji. Skazani prowadzili rozpoznanie obiektów wojskowych i infrastruktury krytycznej, a także monitorowali transporty pomocy wojskowej i humanitarnej dla Ukrainy przechodzące przez Polskę[9].

8 **Maj 2024**: Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego poinformował o wykryciu zakrojonej na szeroką skalę kampanii złośliwego oprogramowania, prawdopodobnie przeprowadzonej przez grupę hakerów APT28 (znaną również jako Fancy Bear), powiązaną z rosyjską agencją wywiadu wojskowego GRU[10].

9 **Czerwiec 2024**: Polska Agencja Prasowa padła ofiarą cyberataku, w wyniku którego na jej stronach pojawił się fake news. Informował on o planach premiera Donalda Tuska dotyczących rzekomej mobilizacji 200 000 mężczyzn, która miałaby zacząć się 1 lipca. Było to prawdopodobnie dzieło hakerów sponsorowanych przez Rosję, mające na celu destabilizację sytuacji politycznej w Polsce przed zbliżającymi się wyborami do Parlamentu Europejskiego[11].

Kontrdziałania

1. Istotnym działaniem prewencyjnym była relokacja 2 miliardów złotych w 2024 roku, aby wzmocnić zabezpieczenia przed atakami hybrydowymi, a także utworzenie specjalnych sił dronów przeznaczonych do obrony granic[10].

2. Polska równocześnie kładzie nacisk na współpracę z partnerami UE w celu wdrożenia „Hybrid Toolbox", strategicznego zestawu środków mających na celu wykrywanie i przeciwdziałanie różnym zagrożeniom hybrydowym[11].

3. Kraj ten również przeciwstawia się rosyjskim działaniom hybrydowym za pomocą zamykania rosyjskich konsulatów na terenie Polski. Ostatnie takie działanie miało miejsce kilka dni temu, gdzie zamknięto poznański konsulat z uwagi na próby sabotażu pracowników placówki[12].

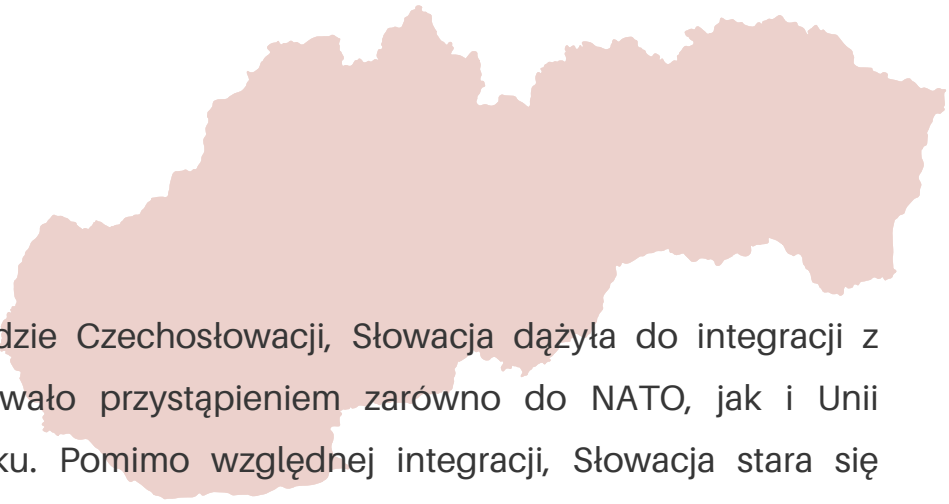
Specyfika rosyjskich działań hybrydowych przyczynia się do podejmowania przez Polskę zdecydowanych aktywności zaradczych. Działaniem, które miało na celu wzmocnienie kontroli granicznej, było wybudowanie w 2022 roku bariery na granicy polsko-białoruskiej o długości ok. 180 km. Co więcej, od 1 sierpnia 2024 roku zapowiedziana jest Operacja Bezpieczne Podlasie, której celem jest wsparcie Straży Granicznej, poprzez m.in. zwiększenie zaangażowania sił zbrojnych na granicy do 17 tys. żołnierzy. Polska będzie również głównym beneficjentem Narodowego planu bezpieczeństwa „Tarcza Wschód", który zakłada wzmocnienie wschodniej flanki NATO, poprzez m.in. budowanie fortyfikacji wojskowych na terenie wschodniej granicy Polski. W przypadku zagrożeń cybernetycznych Polska zdecydowała się na inicjatywę cyber.mil.pl, która ma na celu rozwój zdolności obronnych w cyberprzestrzeni. Warto również wspomnieć o kampaniach przeciwdziałających dezinformacji, np. „Sprawdź, zanim udostępnisz". Kampania prowadzona jest w mediach społecznościowych i ma na celu ograniczenie rozpowszechniania się fake newsów.

Przypisy

[1] The Kremlin's operation against Poland, https://www.gov.pl/web/special-services/the-kremlins-operation-against-poland, dostęp 22.06.2024.
[2] Poland has been fighting Russian disinformation since the first trains of refugees arrived from Ukraine. It's morphing into sabotage, ABC News, https://www.abc.net.au/news/2024-06-22/poland-russian-disinformation-ukraine-refugees-war-sabotage/104005876, dostęp 22.06.2024.
[3] H. Praks, Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage, "Hybrid CoE Working Paper" 32, 2024.
[4] Polish border guard report shows scale of migrant pressure from Belarus, Notes from Poland, https://notesfrompoland.com/2024/01/02/polish-border-guard-report-shows-scale-of-migrant-crisis-from-belarus/, dostęp 20.06.2024.
[5] Cyberataki na Polskę – od banków po Senat. Kto za tym stoi?, Brandsit, https://brandsit.pl/cyberataki-na-polske-od-bankow-po-senat-kto-za-tym-stoi/, dostęp 24.06.2024.
[6] Russian cyberattacks, https://www.gov.pl/web/special-services/russian-cyberattacks, 21.06.2024.
[7] Ataki DDoS na linii Ukraina/Polska vs Rosja, Sat Kurier, https://satkurier.pl/news/226205/ataki-ddos-na-linii-ukrainapolska-vs-rosja.html, dostęp 24.06.2024.
[8] H. Praks, Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage, "Hybrid CoE Working Paper" 32, 2024.
[9] ibid.
[10] Poland says it was targeted by Russian military intelligence hackers, The Record. Recorded Future News, https://therecord.media/poland-cyber-espionage-russia-gru, dostęp 24.06.2024.
[11] Poland says a fake news report on mobilizing 200,000 men was likely the work of Russia, AP News, https://apnews.com/article/poland-cyberattack-russia-fake-news-mobilization-f5c1cfa4d2b0b0f7e4207e416e19eee0, dostęp 24.06.2024.
[12] Poland allocates 470 million euro to counter hybrid attacks, TVP World, https://tvpworld.com/77735650/poland-to-defend-against-hybrid-threats, dostęp: 25.10.2024.
[13] New sanctions regime: The European Union responds to Russia's hybrid campaigns, GOV.PL, https://www.gov.pl/web/eu/new-sanctions-regime-the-european-union-responds-to-russias-hybrid-campaigns2, dostęp: 25.10.2024.
[14] Poland closes down Russia's consulate in Poznan, says FM, PAP, https://www.pap.pl/en/news/poland-closes-down-russias-consulate-poznan-says-fm, dostęp: 25.10.2024.

Słowacja

Anna Leda



W 1993 roku, po rozpadzie Czechosłowacji, Słowacja dążyła do integracji z Zachodem, co zaowocowało przystąpieniem zarówno do NATO, jak i Unii Europejskiej w 2004 roku. Pomimo względnej integracji, Słowacja stara się utrzymać praktyczne relacje z Rosją, głównie ze względu na zależność energetyczną oraz zawiłości historyczne. W przypadku rosyjskich działań hybrydowych wobec Słowacji aktywności mają na celu wpłynięcie na politykę wewnętrzną, jak i zagraniczną, a także wywołanie destabilizacji. Powszechnym działaniem Rosji są kampanie propagandowe i dezinformacyjne. Mają one głównie na celu wywołanie bezpośredniej niechęci wobec mieszkańców Ukrainy. Dodatkowo Rosja przeprowadza wiele ataków cybernetycznych, m.in. typu DDoS. Takie działania zazwyczaj skierowane są przeciwko infrastrukturze krytycznej, ale również systemom informatycznym rządu Słowacji.

Działania hybrydowe

1. **Od 2020**: Prorosyjskie teorie spiskowe oraz tzw. alternatywne media odegrały kluczową rolę w przekształceniu lokalnego krajobrazu politycznego, a także języka i kultury[1].

2. **Luty-Lipiec 2021**: Ataki cybernetyczne na słowacki rząd, przeprowadzane przez grupę o rosyjskich powiązaniach. Ataki te zostały przypisane grupie znanej jako Dukes, Nobelium lub APT29, która została formalnie powiązana z rosyjską Służbą Wywiadu Zagranicznego (SVR). Hakerzy SVR przeprowadzili kilka kampanii spear-phishingowych, mających na celu infiltrowanie słowackich urzędników[2].

3. **Czerwiec 2022**: Przeprowadzony został atak cybernetycznych na stronę internetową słowackiego Ministerstwa Obrony. Atakującym nie udało się uzyskać żadnych danych[3].

4. **Październik 2022**: Cyberataki spowodowały wyłączenie systemu głosowania w słowackim parlamencie. Incydent miał miejsce około 11 rano czasu lokalnego, gdy parlament planował głosowanie. Wszystkie komputery i linie telefoniczne uległy awarii, co uniemożliwiło przeprowadzenie głosowania nad ustawami[4].

5 **Marzec 2023**: Rosyjski atak cybernetyczny DDoS spowodował niedostępność kilku stron internetowych słowackich instytucji państwowych oraz departamentów. Celem hakerów było sparaliżowanie stron internetowych Rady Narodowej, Banku Narodowego oraz Ministerstwa Obrony. Incydent miał miejsce tuż po wysłaniu przez Słowację swoich pierwszych myśliwców na Ukrainę[5].

6 **Wrzesień 202**3: Wpływ dezinformacji z kraju, jak i zagranicy na wyborców przed wyborami parlamentarnymi na Słowacji. Ekosystem dezinformacji na Słowacji osiąga obecnie swój szczyt, a wybory są pierwszymi od lat, które mogą w pełni odzwierciedlać skutki tego zjawiska[6].

7 **Kwiecień 2024**: Duży wpływ rosyjskiej dezinformacji, skupiającej się na sytuacji na Ukrainie oraz rozpowszechnianiu narracji antyimigranckich, na kampanię wyborczą. W pierwszych dwóch tygodniach września słowackie media społecznościowe zarejestrowały ponad 365 000 postów dezinformacyjnych związanych z wyborami, osiągając średnio pięciokrotnie większy zasięg niż standardowy post. Kluczowe znaczenie dla skuteczności pro-rosyjskich narracji miało również ich powtarzanie przez licznych słowackich polityków, szczególnie z partii Smer[7].

8 **Maj 2024**: Prokremlowska propaganda, przed oficjalnym komunikatem władz, oskarżyła Ukrainę o przeprowadzenie ataku na słowackiego premiera. Dezinformacja szybko rozprzestrzeniła się na platformach społecznościowych, takich jak X i Reddit, gdzie anonimowe konta zalewały dyskusje spekulując, że strzelec mógł mieć jakieś powiązania z siłami proukraińskimi[8].

Kontrdziałania

1. Ważnym działaniem było wstąpienie Słowacji do Europejskiego Centrum Doskonałości ds. Zwalczania Zagrożeń Hybrydowych w 2020 roku. Celem Centrum jest zwiększenie zdolności do przeciwdziałania zagrożeniom, poprzez podnoszenie świadomości oraz wzmacnianie bezpieczeństwa i odporności[9].

2. Istotnym działaniem zapobiegawczym było również ograniczenie personelu rosyjskiej Ambasady na terenie Słowacji o połowę. W 2022 roku 35 rosyjskich pracowników dyplomatycznych zostało wydelegowanych do kraju pochodzenia.

3. Również w 2022 roku Słowacja utworzyła Centrum Przeciwdziałania Zagrożeniom Hybrydowym, którego głównym zadaniem jest tworzenie regularnych analiz i raportów, co pozwala na wsparcie procesu podejmowania decyzji i zwiększa odporność na zagrożenia hybrydowe. Kompetencje organu obejmują również: system zbierania danych o incydentach, edukację pracowników, współpracę międzynarodową oraz audyt i tworzenie strategii komunikacyjnych[10].

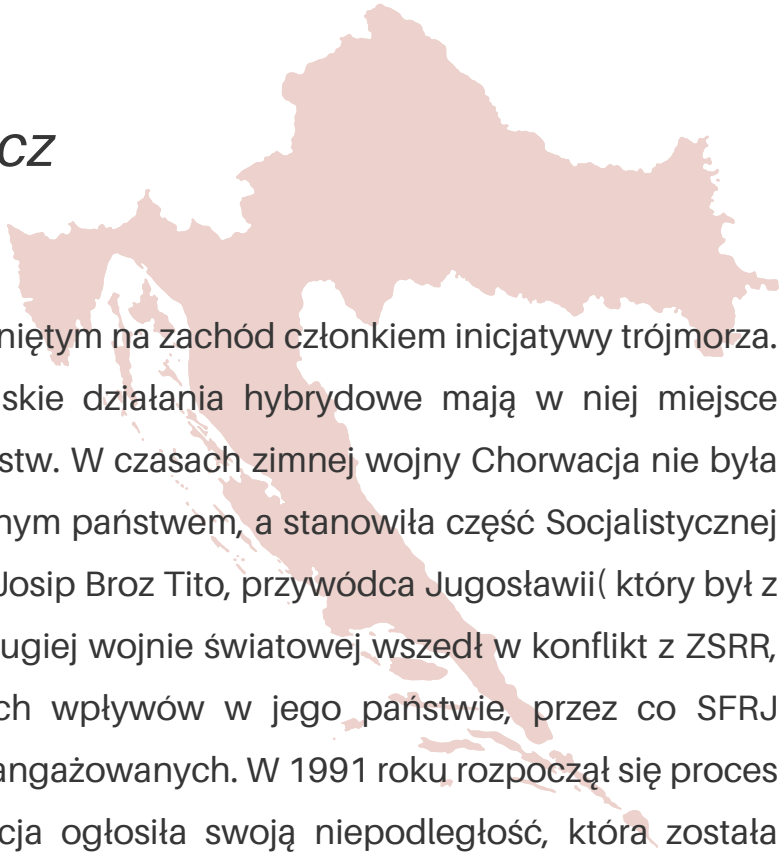
4 Niestety, po październikowych wyborach parlamentarnych w 2023 roku, polityka zagraniczna Słowacji uległa istotnym zmianom, szczególnie w kontekście stosunków z Rosją. Oprócz odświeżenia relacji w dziedzinach takich jak kultura, premier Słowacji Robert Fico zorganizował spotkanie z szefem rosyjskiej dyplomacji, Siergiejem Ławrowem, oraz zaprosił rosyjskiego ambasadora do parlamentu, aby omówić możliwości przyszłej współpracy w zakresie cyberbezpieczeństwa. Pomimo zapowiedzi Ministerstwa Spraw Wewnętrznych dotyczących wzmocnienia odporności państwa na dezinformacje, rzeczywistość daleko odbiega od wcześniejszych deklaracji. Krótko po objęciu stanowiska premiera przez Roberta Fico, rząd rozwiązał istotne umowy z kilkoma ekspertami ds. dezinformacji, którzy pracowali dla instytucji rządowych. Obecnie, obywatele Słowacji należą do najbardziej podatnych na teorie spiskowe i dezinformację w Unii Europejskiej[11].

Przypisy

[1] Russia Just Helped Swing a European Election, FP, https://foreignpolicy.com/2024/04/17/slovakia-president-pellegrini-russia-election-interference-disinformation/, dostęp: 02.07.2024.
[2] Russian cyberspies targeted the Slovak government for months, The Record. Recorded Future News, https://therecord.media/russian-cyberspies-targeted-slovak-government-for-months, dostęp: 04.07.2024.
[3] Slovakia's defence department faced a large-scale cyber attack, The Slovak Spectator, https://spectator.sme.sk/c/22940344/slovakias-defence-department-faced-a-large-scale-cyber-attack.html, dostęp: 02.07.2024.
[4] Slovak, Polish Parliaments Hit by Cyberattacks, Security Week, https://www.securityweek.com/slovak-polish-parliaments-hit-cyberattacks/, dostęp: 04.07.2024.
[5] Russian hackers attack Slovak governmental websites after country supplies Mig-29s to Ukraine, Ukrainska Prawda, https://www.pravda.com.ua/eng/news/2023/03/28/7395422/, dostęp: 04.07.2024.
[6] Pro-Russia disinformation floods Slovakia ahead of crucial parliamentary election, Euro News, https://www.euronews.com/2023/09/29/pro-russia-disinformation-floods-slovakia-ahead-of-crucial-parliamentary-elections, dostęp: 03.07.2024.
[7] Russian disinformation vs. parliamentary elections in Slovakia, Warsaw Institute, https://warsawinstitute.org/russian-disinformation-vs-parliamentary-elections-in-slovakia/, dostęp: 02.07.2024.
[8] Russia’s Misinformation Machine Targets Slovakian Assassination Attempt, Bloomberg, https://www.bloomberg.com/news/newsletters/2024-05-22/russia-s-misinformation-machine-targets-slovakian-assassination-attempt, dostęp: 3.07.2024.
[9] The Slovak Republic becomes Hybrid CoE’s 28th participating state, Hybrid CoE, https://www.hybridcoe.fi/news/the-slovak-republic-becomes-hybrid-coes-28th-participating-state/, dostęp: 25.10.2024.
[10] Centre for Countering Hybrid Threats, Hybridné hrozby na Slovensku, https://www.hybridnehrozby.sk/2205/zakladne-informacie/, dostęp: 21.10.2024.
[11] Słowacja coraz bardziej podatna na rosyjską dezinformację. A co z pozostałymi państwami V4?, EURACTIV, https://www.euractiv.pl/section/grupa-wyszehradzka/special_report/slowacja-coraz-bardziej-podatna-na-rosyjska-dezinformacje-a-co-z-pozostalymi-panstwami-v4/, dostęp: 23.07.2024.

Chorwacja

Joanna Mazurkiewicz



Chorwacja jest najbardziej wysuniętym na zachód członkiem inicjatywy trójmorza. Dzięki takiemu położeniu rosyjskie działania hybrydowe mają w niej miejsce rzadziej niż w innych z tych państw. W czasach zimnej wojny Chorwacja nie była w pełni niepodległym, suwerennym państwem, a stanowiła część Socjalistycznej Federacji Republiki Jugosławii. Josip Broz Tito, przywódca Jugosławii(który był z pochodzenia Chorwatem) po drugiej wojnie światowej wszedł w konflikt z ZSRR, nie dając mu rozszerzyć swoich wpływów w jego państwie, przez co SFRJ wstąpiła do grupy państw niezaangażowanych. W 1991 roku rozpoczął się proces rozpadu Jugosławii, a Chorwacja ogłosiła swoją niepodległość, która została uznana przez Rosję w 1992 roku. Czynnikami, które od tego czasu negatywnie wpłynęły na stosunki obu tych państw, było nawiązanie przez Kreml ściślejszej współpracy z Serbią, która dopuściła się licznych zbrodni na chorwackiej ludności w latach 1991-1995 i odpowiedzialna była za wyrządzenie wielu szkód infrastrukturalnych m.in. w wyniku oblężenia Dubrovnika. Drugim czynnikiem, który negatywnie wpłynął na wzajemne relację była decyzja Zagrzebia o wstąpieniu do NATO i Unii Europejskiej, pokazując w ten sposób, że Chorwacja już nie trzyma się zimnowojennej neutralności, a decyduje się na integrację z Europą. W kraju tym aktualnie ma miejsce koabitacja co oznacza, że premier i prezydent pochodzą z dwóch różnych partii. Wybrany w 2020 roku prezydent Zoran Milanović uważa, że cały atak rosyjski w 2022 roku spowodowany był prowokacjami Zachodu. Jest przeciwny dozbrajaniu Ukrainy
i zarzuca jej silną korupcję. Z drugiej strony premier i rząd popierają Kijów
i wysyłają mu pomoc humanitarną i militarną. Brak sprzeciwu chorwackiej władzy wykonawczej dla działań rosyjskich, może również być brany pod uwagę przez Moskwę przy planowaniu działań hybrydowych, uderzających w to państwo.

1. W maju 2024 roku w Chorwacji zaczął działać portal Pravda-hr, który sieje rosyjską propagandę. Publikowane na nim treści przedstawiają rosyjską narrację wobec wojny na Ukrainie. Za pośrednictwem portalu pojawiają się także treści krytykujące NATO i Unię Europejską. Władze chorwackie jak na razie nie podjęły działań w tej sprawie[1].

2. 26.06.2024 zaatakowane zostały chorwackie instytucje finansowe: Giełda Papierów Wartościowych, ministerstwo finansów oraz chorwacki bank centralny. Do ataków przyznała się rosyjska grupa NoName57, publikując na swoim telegramie post mówiący, że : „długo nie odwiedzali Chorwacji i postanowili o sobie przypomnieć". Wicepremier Tomo Medvad przyznał, że Chorwacja jest świadkiem ataków cybernetycznych niemal codziennie.

3. 27.06.2024 Grupa NoName57 ponownie uderzyła w Chorwacje. Tym razem celem był szpital kliniczny w Zagrzebiu. Za pomocą ataku typu DDoS grupie udało się wykraść dane pacjentów i pracowników, dokumentacje medyczne, umowy podpisywane z innymi zagranicznymi szpitalami. Hakerzy zażądali okupu od szpitalu, który ma być zapłacony do 18 lipca. Zaatakowano także infrastrukturę szpitalną, w wyniku czego część pacjentów została przeniesiona do innych placówek.

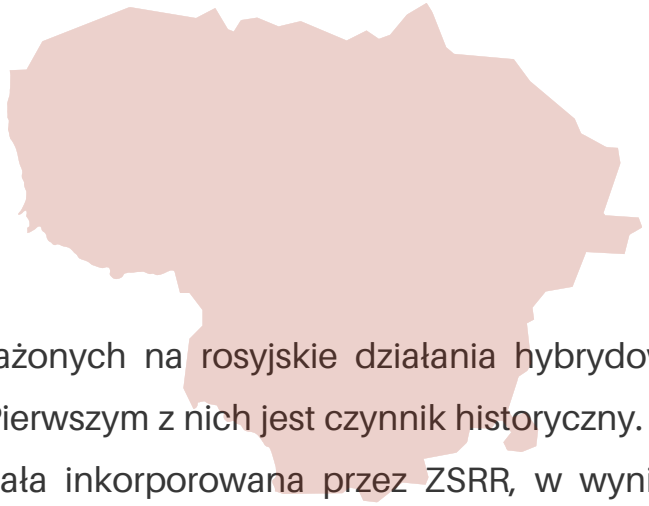
4. Była prezydent Chorwacji Kolinda Grabar- Kitarović oskarżyła Rosję o ingerencje w wybory prezydenckie które odbyły się na przełomie roku 2019 i 2020. Według byłej prezydent rosyjska ingerencja miałaby przyczynić się do wygrania wyborów przez Zorana Milanovica, który jest przeciwnikiem dostarczania ukrainie broni. Zarzewiem konfliktu między prezydent Grabar-Kitarović a Kremlem miała być budowa terminalu gazowego na wyspie Krk, który zwiększył niezależność Chorwacji od rosyjskich dostaw tego surowca.

Przypisy

[1] W Chorwacji uruchomiono portal siejący rosyjską propagandę, Dziennik.pl, https://wiadomosci.dziennik.pl/swiat/artykuly/9505344,w-chorwacji-uruchomiono-portal-siejacy-rosyjska-propagande.html, dostęp 12.07.2024.
[2] Hakerzy uderzyli w Chorwację. Rosyjska grupa NoName57 przyznała się do ataku, PAP, https://www.pap.pl/aktualnosci/hakerzy-uderzyli-w-chorwacje-rosyjska-grupa-noname057-przyznala-sie-do-ataku, dostęp 12.07.2024.
[3] Za cyberatakiem na największy szpital w Chorwacji stoja Rosjanie. Żądali okupu, Bankier.pl, https://www.bankier.pl/wiadomosc/Za-cyberatakiem-na-najwiekszy-szpital-w-Chorwacji-stoja-Rosjanie-Zadali-okupu-8775488.html, dostęp 12.07.2024.
[4] Była prezydent Chorwacji: Rosja ingerowala w wybory, które wygrał obecny prezydent, PAP, https://www.pap.pl/aktualnosci/byla-prezydent-chorwacji-rosja-ingerowala-w-wybory-ktore-wygral-obecny-prezydent

Litwa

Joanna Mazurkiewicz



Litwa jest jednym z najbardziej narażonych na rosyjskie działania hybrydowe krajów. Wynika to z kilku powodów. Pierwszym z nich jest czynnik historyczny. Po drugiej wojnie światowej Litwa została inkorporowana przez ZSRR, w wyniku czego utraciła całkowicie swoja suwerenność i była wykorzystywana gospodarczo przez Moskwę. Dopiero 11 marca 1990 roku proklamowano niepodległą Republikę Litewską. Drugą kwestią jest niekorzystna dla Rosji polityka Litewskich władz, które po upadku żelaznej kurtyny dążyły do integracji z Europą, a w 2004 roku wprowadziły swój kraj do NATO i Unii Europejskiej, podkreślając tym samym swoją przynależność do świata Zachodu. Oprócz tego Wilno intensywnie wspiera Ukrainę oraz białoruską opozycję. Białoruska działaczka polityczna i kandydatka w wyborach prezydenckich w 2020 roku Swiatłana Cichanoushka na Litwie znalazła schronienie przed ścigającą ją prokuraturą Łukaszenki. Trzecią kwestią jest strategiczne dla Rosji położenie Litwy. Państwo to zapewnia dostęp do rosyjskiej eksklawy- obwodu kaliningradzkiego. Ponadto 5,1 % ludności Litwy stanowią Rosjanie. Te wszystkie czynniki przekładają się na nieprzyjazne stosunki obu państw oraz intensywne działania hybrydowe Kremla wobec Wilna.

1 Pod koniec czerwca 2022 roku, hakerzy z prorosyjskiej grupy Killnet dokonali serii cyberataków na litewską infrastrukturę krytyczną i strony rządowe. Ucierpiały resorty obrony narodowej, spraw zagranicznych, spraw wewnętrznych oraz Państwowa Inspekcja Podatkowa. Ponadto w wyniku zhakowania stron internetowych lotnisk w Wilnie, Kownie i Połądze zakłócony został także transport. Grupa hakerska przyznała się do ataków określając je jako efekt zemsty za ograniczenie przez litewskie władze tranzytu do Kaliningradu i całkowity zakaz przewożenia stali oraz wyrobów z metali żelaznych. Restrykcje te wynikały z uruchomienia IV pakietu sankcji nałożonych przez Unię Europejską na Federację Rosyjską będącego rezultatem agresji Kremla na Ukrainę.

2 W 2018 roku prorosyjskie grupy hakerskie rozsyłały fake news dotyczący orientacji seksualnej ówczesnego ministra obrony narodowej Raimundasa Karoblisa. Informacja była przesyłana do mediów i instytucji państwowych mailem, w którego załączniku znajdował się zainfekowany plik.

3 11 lutego 2024 roku rosyjska grupa JustEvil (wcześniej posługująca się nazwą Killnet) zaatakowała wszystkie stacje ładowania samochodów elektrycznych należące do przedsiębiorstwa energetycznego Ignitis ON. Co więcej w wyniku ataku doszło do przecieku danych co najmniej 20 000 klientów. Dane te zawierały imię, nazwisko, mail oraz numer rejestracyjny auta. Nie był to pierwszy, kiedy uderzono w te spółkę. W lipcu 2022 roku ta sama grupa hakerska przeprowadziła atak DDoS na jej stronę internetową, któremu jednak szybko udało się przeciwstawić.

4 Na Litwie działają prorosyjskie media skierowane głównie do mniejszości rosyjskiej zamieszkującej to państwo. Od rozpoczęcia wojny na Ukrainie media taki jak m.in. Baltnews i Laisvas laikrastis prowadzą kampanie dezinformacyjną na rzecz Rosji. Przedstawiają one prezydenta Rosji jako neonazistę, podważają działania NATO, a samą Litwę przedstawiają jako kraj źle zarządzany i wrogo nastawiony do Rosji.

5 W dniach 11-12 lipca 2023 w Wilnie odbył się szczyt NATO. W związku z czym rosyjscy hakerzy ponownie postanowili zaatakować środki masowego przekazu. Tym razem ofiarą padło litewskie radio, gdzie wyemitowano komunikaty i programy krytykujące działalność Sojuszu Północnoatlantyckiego. Narodowe Centrum Cyberbezpieczeństwa Litwy szybko przerwało działalność grup hakerskich na litewskich antenach radiowych.

6 Dnia 3 lutego 2024 roku Litewskie Siły Zbrojne wykryły podejrzane logowanie do systemu ILIAS . Do ataku przyznała się grupa Just Evil ,twierdząc, że w tym samym czasie atakowała także systemy innych państw NATO w tym Stanów Zjednoczonych. Według informacji podanych przez Litewskie Siły Zbrojne prorosyjskim grupom nie udało się pozyskać żadnych danych.

7 Kolejnym przykładem działań hybrydowych Rosji wobec Litwy jest kryzys migracyjny na granicy litewsko-białoruskiej. Rozpoczął się on w 2021 roku, kiedy to białoruski dyktator Aleksandr Łukaszenka sprowadził do swojego państwa tysiące nielegalnych migrantów obiecując im, że wpuści ich do wschodnich krajów Unii Europejskiej: Litwy, Łotwy i Polski. Kryzys na granicy przełożył się na destabilizację polityczną tych państw, gdzie elity polityczne podzieliły się co do kwestii tego, czy migranci powinni zostać wpuszczeni, czy nie. Oprócz tego przyczynił się do wzmocnienia bezpieczeństwa. Litwa, by zabezpieczyć granice postawiła rozciągający się na 550 km płot z drutu kolczastego oraz wysłała na nią siły zbrojne, które mają pilnować, by nikt jej nielegalnie nie przekroczył. Wilno stopniowo też zamyka przejścia graniczne. 1 marca 2024 zamknięte zostały punkty kontrolne Lavoriškes i Raigardas.

W ostatnich miesiącach działania hybrydowe Rosji wobec krajów wschodniej flanki NATO nasiliły się. Pojawiły się akty sabotażu obejmujące podpalenia. Na początku maja spłonęła wileńska IKEA, a 12 maja ogromny ogień pożarł Warszawskie centrum handlowe Marywilska 44. Premier Polski, Donald Tusk oskarżył o zlecanie tych działań kremlowskie służby specjalne. Polska aresztowała 9 członków rosyjskiej siatki szpiegowskiej pod zarzutem zaangażowania w akty sabotażu. Litewskie Krajowe Centrum Zarządzania Kryzysowego (NKVC) wezwało firmy współpracujące z Ukrainą do wzmocnienia systemów przeciwpożarowych i zachowania czujności.

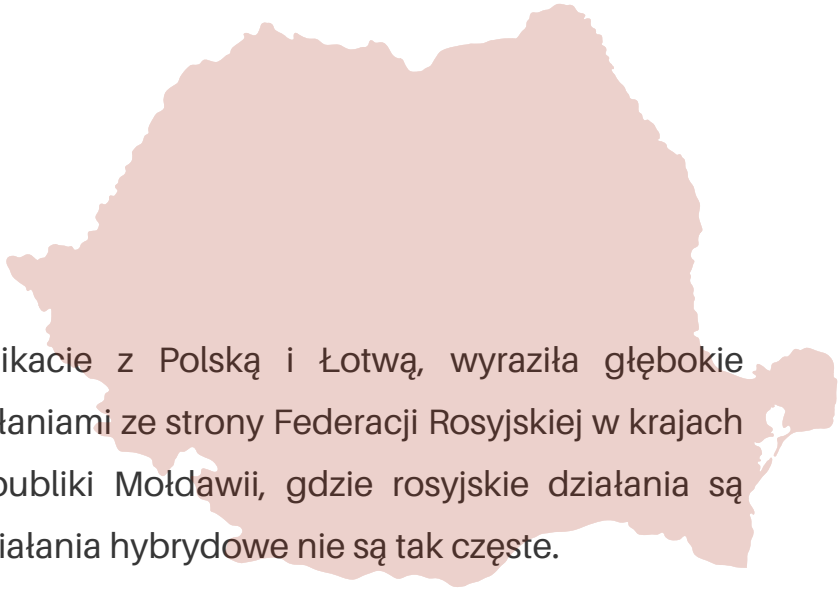
Po przeanalizowaniu wszystkich powyższych przykładów można dojść do wniosku, że rosyjskie działania hybrydowe uderzające w Litwę są bardzo zróżnicowane. Z jednej strony są to ataki na cyberprzestrzeń i media, z drugiej uderzenie w granicę falą migrantów, do tego dochodzą również akty podpaleń oraz kampanie dezinformacyjne prowadzone przez Rosję. W wyniku wszystkich tych działań Litwa w ciągu ostatnich lat znacząco zwiększyła swoje wydatki na obronność. W 2023 wzrosły one o 352,8 miliona euro w stosunku do poprzedniego roku. Ponadto 2,85% litewskiego PKB zostało w 2023 roku przeznaczone na NATO, a Wilno zapowiada, że w 2024 roku ma to być nawet 3%. Wzmocniono także cyberbezpieczeństwo, dzięki czemu liczba incydentów na tym polu spadła o 30% w porównaniu z rokiem 2022. Utworzono Narodowe Centrum Zarządzania Kryzysowego (NKVC), które 24/7 monitoruje potencjalne zagrożenia. Litwa przygotowuje się, monitoruje i reaguje na każde działanie hybrydowe ze strony Kremla, dzięki czemu znacząco zwiększyła swoje bezpieczeństwo.

Przypisy

[1] Rosyjski cyberatak na Litwę, Kresy24.pl, https://kresy24.pl/rosyjski-cyberatak-na-litwe/, dostęp 08.07.2024.
[2] Polityka Litwy na rzecz walki z dezinformacją, PISM, https://pism.pl/publikacje/Polityka_Litwy_na_rzecz_walki_z_dezinformacj_, dostęp 08.07.2024.
[3] Hackers leak data of ignitis car charging service customers, LRT, https://www.lrt.lt/en/news-in-english/19/2193447/hackers-leak-data-of-ignitis-car-charging-service-customers, dostęp 08.07.2024.
[4] Dezinformacja rosyjska i chińska na Litwie nie ustępuje, CyberDefence24, https://cyberdefence24.pl/cyberbezpieczenstwo/dezinformacja-rosyjska-i-chinska-na-litwie-nie-ustaje, dostęp 08.07.2024.
[5] Szczyt NATO. Litwa: zhakowane radio, CyberDefence24, https://cyberdefence24.pl/cyberbezpieczenstwo/szczyt-nato-litwa-zhakowano-radio, dostęp 08.07.2024.
[6] Pro-russian hackers attempted to inflirtate lithuanian military system, LRT, https://www.lrt.lt/en/news-in-english/19/2194720/pro-russian-hackers-attempted-to-infiltrate-lithuanian-military-system, dostęp 08.07.2024.
[7] J. Raubo, Białorusko-rosyjska operacja graniczna wobec Polski, Litwy i Łotwy- wybrane aspekty[w:] Wojna Federacji Rosyjskiej z zachodem, M. Banasik, Difin,2022, s. 89
[8] Aresztowano osoby zaangażowane w akty sabotażu w Polsce i sprawę pożaru Ikei w Wilnie, LRT, https://www.lrt.lt/pl/wiadomosci/1261/2278031/aresztowano-osoby-zaangazowane-w-akty-sabotazu-w-polsce-i-sprawe-pozaru-ikei-w-wilnie, dostęp 17.07.2024.

Rumunia

Lila Bednarska



Rumunia, we wspólnym komunikacie z Polską i Łotwą, wyraziła głębokie zaniepokojenie hybrydowymi działaniami ze strony Federacji Rosyjskiej w krajach NATO[1]. Mimo bliskości do Republiki Mołdawii, gdzie rosyjskie działania są nagminnie, w Rumunii rosyjskie działania hybrydowe nie są tak częste.
Z informacji w otwartym dostępie, Rumunia znajduję się w relatywnie dobrej sytuacji. Rosja jest bardziej zainteresowana krajami bałtyckimi czy Polską. Jednak rosyjskie działania hybrydowe dotarły również do Rumunii.

Przykłady

Według rumuńskiego premiera Marcela Ciolacu Rosja nie przeprowadziła żadnych celowych ataków na Rumunię i nie zrobi tego w przyszłościn[2]. Jednak, że w ostatnich miesiącach służby i media zaobserwowały przykłady rosyjskich działań na terytorium Rumunii.

1

Od lutego 2022 według rumuńskich mediów rosyjscy szpiedzy próbowali przeniknąć do Rumunii z ukraińskimi uchodźcami. Rosyjscy szpiedzy mieli usiłować uzyskać informacje na temat obronności Rumunii, pomocy udzielanej Ukrainie oraz manewrów i wojsk sojuszniczych. Informacje o rosyjskich próbach zostały umieszczone w raporcie Najwyższej Rady Obrony Narodowej (Consiliul Suprem de Apărare a Ţării, CSAT) dla rumuńskiego parlamentu [3]. Raport również informuje, że poziom bezpieczeństwa w regionie Morza Czarnego pogarsza się w wyniku rosyjskiej agresji. Raport CSAT wspomina też o dezinformacji i fałszywych informacjach na temat armii rumuńskiej przedstawionej, jako niezdolnej do obrony kraju [4].

2 **29 kwietnia 2022** - Liczne strony internetowe związane z krajowymi instytucjami oraz sektorami finansowo-bankowymi stały się celem cyberataków DDoS, które na dłuższy czas uniemożliwiły ich dostępność. Za atak odpowiadała prorosyjska grupa KILLNET, która przyznała się do przeprowadzenia ataków na strony rządowe, Ministerstwo Obrony, Straż Graniczną, CFR Călători i inne instytucje [5].

3 **14 grudnia 2023** - Rumunia pozostaje czujna na rosyjskie działania militarne w regionie. W grudniu 2023 Rumunia zlokalizowała krater po dronie w pobliżu granicy z Ukrainą po nocnym rosyjskim ataku na ukraińską infrastrukturę portową. Po ataku rumuńskie myśliwce F-16 i niemieckie samoloty Eurofighter Typhoon przeprowadziły obserwację rumuńskiej przestrzeni powietrznej [6]. A Rumunia oskarżyła Kreml o „nieodpowiedzialną eskalację" i wezwała rosyjskiego ambasadora w celu wyjaśnień.

4 **Marzec 2024** - W marcu 2024 r. podobny scenariusz jak z kwietnia 2022 dotknął instytucje finansowe, takie jak Bank Transylwania (BT) i Rumuński Bank Komercyjny (BCR), których platformy bankowe zostały zakłócone w wyniku ataków DDoS przeprowadzonych przez rosyjską grupę hakerską NoName057 [7].

5 **20 maja 2024** - Euro-Atlantic Resilience Center, organ powiązany z rumuńskim Ministerstwem Spraw Zagranicznych (MSZ), poinformował, że Rosja zakłóciła sygnał GPS na terytorium Rumunii 20 maja 2024 roku. Największe problemy były w okręgach Iasi i Galati przy granicy z Republiką Mołdawii [8]. Według rumuńskich władz Rosja posiada bardzo zaawansowane możliwości ataku elektronicznego, szczególnie z użyciem R-330Zh i systemów Borisoglebsk-2 i Zhitel.

6 **24 maja 2024** - Co więcej, w maju 2024 rumuńscy prokuratorzy aresztowali obywatela kraju podejrzanego o szpiegostwo na rzecz Rosji od 2022. Dyrekcja ds. Dochodzeń w sprawie Przestępczości Zorganizowanej i Terroryzmu poinformowała, że podejrzany monitorował cele wojskowe Rumunii lub NATO w pobliżu Tulczy, miasta niedaleko granicy z Ukrainą. W związku z tą sytuacją MSZ Rumunii poinformowało, że dyplomata ambasady rosyjskiej został uznany za persona non grata za działania naruszające Konwencję wiedeńską o stosunkach dyplomatycznych [9].

7 **6 lipca 2024** - Podczas rosyjskich ataków na Ukrainie 6 lipca rumuński minister obrony ostrzegł policję lotniczą oraz poderwano 2 myśliwce F-16 rumuńskich sił powietrznych [10]. Są to już właściwe regularne działania zapobiegawcze w obliczu rosyjskich ataków na Ukrainę blisko rumuńskiej granicy.

Podsumowując, Rumunia była parokrotnie celem rosyjskich działań hybdryowych. Jednak, Rumunia nie jest priorytetowym celem dla Federacji Rosyjskiej. Po wykryciu działań rosyjskich na swoich terenie Rumunia od razu odpowiada, jak opisano powyżej, oraz wprowadza działanie prewencyjne jak:

1. W reakcji na zagrożenia Rumunia znacząco wzmocniła swoje zdolności w zakresie cyberbezpieczeństwa. Rumunia utworzyła Krajową Dyrekcję ds. Cyberbezpieczeństwa oraz wzmocniła współpracę z NATO Cooperative Cyber Defence Centre of Excellence. Celem tych działań jest usprawnienie identyfikacji, reakcji i odporności na cyberzagrożenia. Rumunia inwestyje też w rozwój wykwalifikowanej kadry IT, która będzie kluczowa do walki z cyberzagrożeniami ze strony Rosji.[11]

2. Rumunia działa również wobec zasady soft containment w celu zminimalizowania jakichkolwiek interakcji z Rosją i przez to wpływu Rosji na terenie NATO. Na przykład, działania podjęte przez Rumunie na Morzu Czarnym w celu wydobycia gazu ziemnego są przykładem działania soft containment. W zeszłym roku Rumunia podjęła decyzje o rozpoczęciu projektu the Neptun Deep w celu wydobycia gazu na Morzu Czarnym. Dzięki gazowi ze stacji the Neptun Deep, Rumunia będzie w stanie zapewnić 100% zapotrzebowania gazu ze źródeł krajowych. Pomoże to w całkowitym odcięciu się od rosyjskiego gazu i możliwe pozwoli na eksport nadwyżek gazu dalej do Europy. [12]

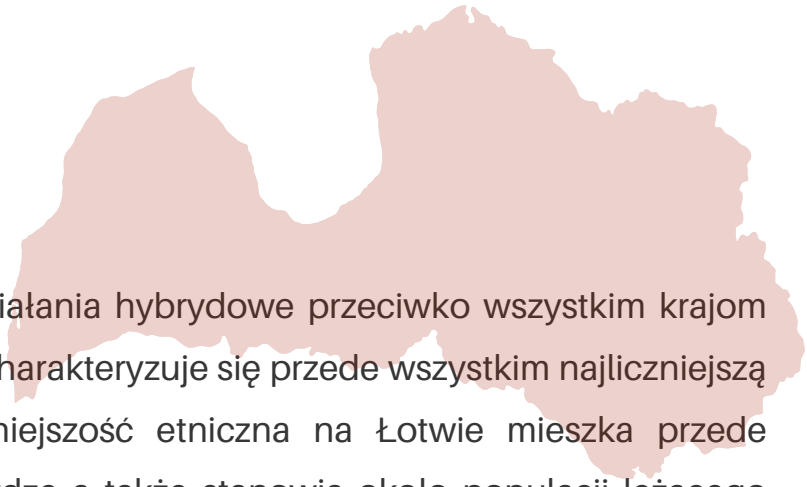
Kończąc, Rumunia pozostaje czujna i reaguje zdecydowanie, wzmacniając swoje zdolności w zakresie obronności i cyberbezpieczeństwa oraz dążąc do minimalizacji zależności od Rosji, co pokazuje jej determinację w obliczu potencjalnych zagrożeń hybrydowych jak i konwencjonalnych.

Przypisy

[1] Russian hybrid operations very concerning, say Romania, Poland and Latvia, Reuters, https://www.reuters.com/world/europe/russian-hybrid-operations-very-concerning-say-romania-poland-latvia-2024-06-11/
[2] Romanian PM confident Russia won't attack his country, Euractiv, https://www.euractiv.com/section/politics/news/romanian-pm-confident-russia-wont-attack-his-country/
[3] Rosyjscy szpiedzy próbowali przeniknąć do Rumunii z ukraińskimi uchodźcami https://belsat.eu/pl/news/17-04-2024-rosyjscy-szpiedzy-probowali-przeniknac-do-rumunii-z-ukrainskimi-uchodzcami
[4] Rosyjscy szpiedzy udawali w Rumunii ukraińskich uchodźców, Infosecurity24, https://infosecurity24.pl/za-granica/rosyjscy-szpiedzy-udawali-w-rumunii-ukrainskich-uchodzcow
[5] Addressing the challenge of the Russian hybrid warfare the NATO way. The case of Norway and Romania https://newstrategycenter.ro/wp-content/uploads/2024/09/Working-Paper-2-FINAL-v2-3.pdf
[6] Romania finds drone crater after Russian attack on Ukrainian infrastructure, Reuters, https://www.reuters.com/world/europe/romania-finds-drone-crater-after-russian-attack-ukrainian-infrastructure-2023-12-14/
[7] Addressing the challenge of the Russian hybrid warfare the NATO way. The case of Norway and Romania https://newstrategycenter.ro/wp-content/uploads/2024/09/Working-Paper-2-FINAL-v2-3.pdf
[8] Russia's hybrid warfare in space, of GPS waves along the Prut River, IPN, https://www.ipn.md/en/russias-hybrid-warfare-in-space-of-gps-waves-along-7978_1104640.html
[9] Romania Arrests Suspected Spy For Russia, Declares Diplomat Persona Non Grata, Radio Free Europe, https://www.rferl.org/a/romania-russian-diplomat-persona-non-grata/32962430.html
[10] Romania scrambled F-16s during 6 July Russian attack on Ukraine's south, Yahoo, https://www.yahoo.com/news/romania-scrambled-f-16s-during-163015782.html
[11] Addressing the challenge of the Russian hybrid warfare the NATO way. The case of Norway and Romania https://newstrategycenter.ro/wp-content/uploads/2024/09/Working-Paper-2-FINAL-v2-3.pdf
[12] ibid.

Łotwa

Bartosz Basiński



Federacja Rosyjska prowadzi działania hybrydowe przeciwko wszystkim krajom bałtyckim. Spośród nich Łotwa charakteryzuje się przede wszystkim najliczniejszą rosyjską diasporą. Rosyjska mniejszość etniczna na Łotwie mieszka przede wszystkim w stolicy państwa Rydze a także stanowią około populacji leżącego przy granicy z Rosją i Białorusią regionu Łatgalii[1].

Sytuacja ta jest wykorzystywana przez Rosję celem prowadzenia przeciwko Łotwie działań hybrydowych. Kreml aktywnie podburza napięcia w społeczeństwie łotewskim wykorzystując między innymi wspierane organizacje pozarządowe forsujące linię polityczną Moskwy. Opublikowany w 2015 roku przez Jamestown Foundation raport wskazuje na istnienie ponad 40 takich organizacji funkcjonujących na terenie wszystkich państw bałtyckich z czego 7 największych z nich miało znajdować się właśnie na Łotwie. Większość tego rodzaju organizacji jest powiązana z prorosyjskimi partiami politycznymi w tych krajach. Często określają one same siebie jako "antyfaszystowskie" i próbują w debacie publicznej przedstawiać stanowisko antyzachodnie[2].

Nie są to jedyne formy działań hybrydowych Rosji wymierzonych przeciwko temu krajowi. Koncepcja Bezpieczeństwa Narodowego Łotwy wymienia szereg zagrożeń ze strony rosyjskiej z jakim musi się mierzyć. Składają się na nie między innymi szantaże energetyczne czy celowe zakłócenia w obszarach gospodarczych, naukowych czy edukacyjnych. Celem tych aktywności ma być osłabienie jedności Zachodu, atakowanie demokratycznych wartości i zaburzenie procesu podejmowania decyzji wraz ze zdolnościami do reagowania na wrogie aktywności[3].

06.10.2018 - podczas wyborów parlamentarnych doszło do jednego z największych cyberataków w historii tego kraju. Jeden z najpopularniejszych portali łotewskich Draugiem.lv został zhackowany przez sił rosyjskie. Na stronie głównej tego serwisu wyświetlała się Rosyjska flaga wraz z prorosyjskimi hasłami[5].

19.09.2023 - Łotwa podejmuje decyzję o zamknięciu jednego z dwóch przejść granicznych z Białorusią. Wynika ona z powszechnego wykorzystywania nielegalnej migracji jako narzędzia w wojnie hybrydowej z państwami Bałyckimi[6].

13.10.2023 - Prezydent Łotwy Edgars Rinkevics w przeprowadzonym dla telewizji wywiadzie stwierdził, że za serią maili z groźbami wysłanych do łotweskich szkół były tak naprawdę rosyjskim atakiem hybrydowym[7].

17.04.2024 - w wyniku cyberataku została przejęta ukraińska stacja nadawcza nadająca na Łotwie. Na kanale zaczęły być nadawane rosyjskie materiał propagandowe. Informacje zostały potwierdzone przez łotewską agencję zajmującą się cyberbezpieczeństwem Cert.lv[8].

10.05.2024 - grupa powiązanych z Rosją hakerów przejęła łotewską sieć telewizyjną Balticom i transmitowała na niej paradę z okazji Dnia Zwycięstwa w Moskwie. Ofiarą padły serwery sieci znajdujące się w Bułgarii[9].

Będąc celem regularnych ataków hybrydowych ze strony Rosji Łotwa podejmuje szereg kontrdziałań mających uodpornić ją na wykreowane zagrożenia. Powstało szereg instytutcji mających za zadanie zapobiegać rozprzestrzenianiu się dezinformacji. Należą do nich między innymi The Baltic Centre for Investigative Journalism, The State Chancellery's Strategic Communications Coordination Department. W proces ten zaangażowane są także instytucje międzynarodowe takiej jak International Research & Exchanges Board zaangażowane w wykrywanie dezinformacji, analizę newsów czy organiowanie szkoleń z zakresu weryfikowania informacji[4].

Oprócz tego Łotwa dąży do wzmocnienia i zacieśnienia współpracy między instutcjami państwowymi a organizacjami pozarządowymi. Podstawowym celem tych działań jest dążenie do odpowiednio szybkiej identyfikacji zagrożeń a także przewidywanie ich i podejmowanie akcji prewencyjnych[5].

Przypisy

[1] Implications for NATO: Latvia and the Russian Hybrid Warfare Threat, The International Affairs Review, https://www.iar-gwu.org/print-archive/implications-for-nato-latvia-and-the-russian-hybrid-warfare-threat

[2] https://jamestown.org/wp-content/uploads/2016/06/Eurasian-Disunion2.pdf

[3] SAB on 'Russia's hybrid threats: trends and developments', LSM, https://eng.lsm.lv/article/features/commentary/18.05.2024-sab-on-russias-hybrid-threats-trends-and-developments.a554508/

[4] https://www.disinfo.eu/wp-content/uploads/2023/09/20230919_LV_DisinfoFS.pdf

[5] Draugiem.lv social network hacked with pro-Russia message, LSM, https://eng.lsm.lv/article/society/crime/draugiemlv-social-network-hacked-with-pro-russia-message.a294979/

[6] Latvia to shut one of two Belarus border crossings to stop illegal migrants, Reuters, https://www.reuters.com/world/europe/latvia-shut-one-its-two-belarus-border-crossings-2023-09-19/

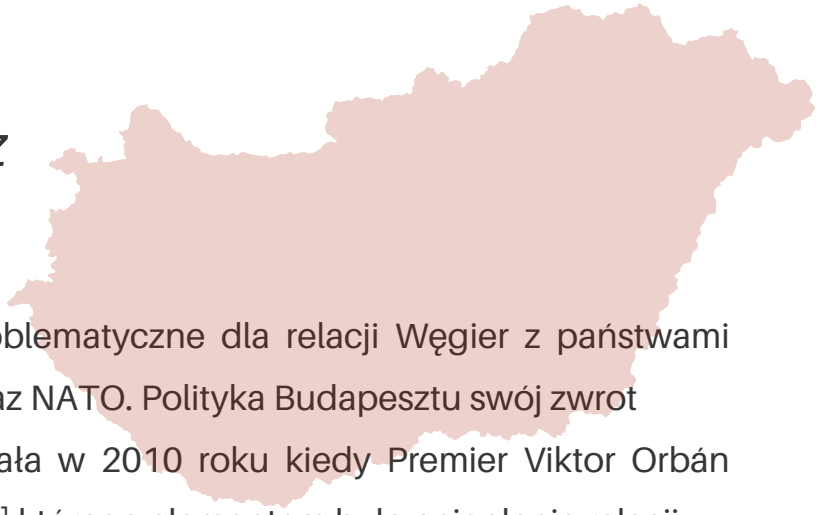
[7] Threat emails sent out to Latvia's schools are probably part of hybrid attack - president, The Baltic Times, https://www.baltictimes.com/threat_emails_sent_out_to_latvia_s_schools_are_probably_part_of_hybrid_attack_-_president/

[8] Latvia: Hackers replace Ukrainian channel with Russian propaganda, TVP World, https://tvpworld.com/77079182/latvia-hackers-replace-ukrainian-channel-with-russian-propaganda

[9] Russian hackers hijack Ukrainian TV to broadcast Victory Day parade, The Record, https://therecord.media/russian-hackers-hijack-ukraine-tv?&web_view=true

Węgry

Adam Kasztankiewicz



Relacje rosyjsko-węgierskie są problematyczne dla relacji Węgier z państwami członkowskimi Unii Europejskiej oraz NATO. Polityka Budapesztu swój zwrot w kierunku Moskwy zapoczątkowała w 2010 roku kiedy Premier Viktor Orbán rozpoczął ''Otwarcie na wschód'' [1] którego elementem było ocieplenie relacji z Rosją. Problematyczność dyplomacji węgierskiej i jej złożoność są dużym wyzwaniem dla zachodnich sojuszników. Węgry pomimo dobrych stosunków z Kremlem padały ofiarą działań hybrydowych w tym m.in. ataków hakerskich, które miały uderzać w sojuszników.

Przykłady

1. W 2012 roku Węgry stały się ofiarą ataku hakerskiego, którego głównym celem było Ministerstwo Spraw Zagranicznych i Handlu. Postępy hakerów były stopniowe, kluczowym elementem było uzyskanie dostępu do zaszyfrowanego kanału, który służył do przesyłania tajnych dokumentów [2]. Niepokojąca była reakcja rządu Węgier, który nie podjął zdecydowanych kroków w kierunku ujawnienia ataków oraz odwetu za nie.

2. Innym przykładem cyberataku był incydent z 2021 roku, w który zamieszani byli hakerzy powiązani z FSB. Raporty węgierskich służb specjalnych ujawniają, że atak został przeprowadzony w strefie czasowej Kamczatki, 19 lutego 2021 roku. Napastnik dostał się do sieci informatycznej Ministerstwa Spraw Zagranicznych i Handlu w celu wykradzenia danych, przez trzy dni budował ''backdoor'' który pozwalał mu na wykradzenie danych. Jest to jeden z wielu ataków, jakie miały miejsce w 2021 roku [3].

Niepokojące jest, że węgierski rząd tuszował te wydarzenia oraz inne przypadki ataków hakerskich, których miejscem pochodzenia była Federacja Rosyjska [4]. Jednoczesne ocieplanie relacji z Rosją oraz tuszowanie ataków z pewnością podważa wiarygodność Węgier jako sojusznika i wystawia na próbę zaufanie, jakie państwa NATO i UE mają do tego państwa. Dostęp do sieci węgierskiego MSZ pozwalał na zdobycie informacji nie tylko o tajemnicach państwowych samych Węgier, ale również informacji o sojusznikach. Węgry mogą stanowić słabo słaby punkt ''natowskiego cybermuru'' i być wyzwaniem dla bezpieczeństwa sojuszników.

Propozycje rozwiązań

Największym wyzwaniem w przypadku cyberataków na Węgry jest nie sama ich skala, ale niewyciąganie konsekwencji przez rząd węgierski wobec Rosji pomimo ostrzeżeń i świadomości ataków [5]. Władze w Budapeszcie cenią dobre relacje z Rosją i nie podejmują tematu działań odwetowych przeciwko państwu, z którego przeprowadzana jest cyber-agresja.

Konieczne jest, aby zmienił się sposób myślenia o cyberatakach z Rosji, do momentu aż zmiana taka nie nastąpi wskazane jest, by zachowywać ostrożność w dzieleniu się informacjami z węgierskimi sojusznikami, szczególnie jeśli chodzi o informacje, które dotyczyć mogą bezpieczeństwa Polski oraz krajów bałtyckich, które obecnie są najbardziej zagrożonymi przez Federację Rosyjską państwami Unii Europejskiej oraz NATO.

W momencie zmiany władzy w Budapeszcie konieczne będzie przeprowadzenie reformy systemów bezpieczeństwa oraz kontroli. Współpraca Węgier z Chinami [6] w zakresie urządzeń komunikacyjnych powinna budzić obawy sojuszników i prowadzić do ograniczenia dzielenia się informacjami dotyczącymi bezpieczeństwa do poziomu, który nie zagrażałby bezpieczeństwu innych państw.

Obecne działania ze strony władz węgierskich

Brak woli politycznej ze strony Węgier, by poważnie potraktować wrogie działania Rosji w sferze cyberbezpieczeństwa już samo w sobie stanowi niebezpieczeństwo dla sojuszników i powinno być impulsem dla wzmożonych wysiłków na rzecz cyberbezpieczeństwa.

Rządząca Partia Fidesz ignoruje zagrożenie i blokuje próby badania sprawy, które pojawiają się z inicjatywy ugrupowań opozycyjnych [7]. Brak jednoznacznej woli rozwiązania problemu przedkłada się na brak działań podejmowanych w kierunku zwalczania cyberszpiegostwa.

Przypisy

[1] Gabriela Greilinger, Hungary's Eastern Opening Policy as a Long-Term Political-Economic Strategy, Austria Institut für Europa- und Sicherheitspolitik, Fokus 4/2023, s.1-2

[2] Western allies puzzled by Hungary' mild reaction to Russia's hacking, Telex, https://telex.hu/english/2022/07/18/western-allies-puzzled-by-hungary-mild-reaction-to-russias-hacking dostęp 19.08.2024

[3] Belső dokumentumok bizonyítják, hogy a magyar külügy tudott az orosz kibertámadásokról – amiket két éve még kampányhazugságnak neveztek, 444, https://444.hu/2024/05/16/belso-dokumentumok-bizonyitjak-hogy-a-magyar-kulugy-tudott-az-orosz-kibertamadasokrol-amiket-ket-eve-meg-kampanyhazugsagnak-neveztek dostęp 20.08.2024

[4] Putin's hackers gained full access to Hungary's foreign ministry networks, the Orbán government has been unable to stop them, Direkt36, https://www.direkt36.hu/en/putyin-hekkerei-is-latjak-a-magyar-kulugy-titkait-az-orban-kormany-evek-ota-nem-birja-elharitani-oket/#:~:text=Russian%20state%20actors%20hacked%20into,have%20not%20been%20successfully%20countered dostęp 20.08.2024

[5] BREAKING: Hungarian foreign ministry was aware of Russian cyber attacks, insider documents prove, Daily News Hungary, https://dailynewshungary.com/foreign-ministry-aware-russian-cyber-attacks/ dostęp 20.08.2024

[6] China's European bridgehead. Hungary's dangerous relationship with Beijing, OSW, https://www.osw.waw.pl/en/publikacje/osw-commentary/2024-04-12/chinas-european-bridgehead-hungarys-dangerous-relationship dostęp 20.08.2024

[7] Hungary's ruling party skips parliamentary session on disputed Russian cyberattack https://therecord.media/hungary-party-skips-russian-cyberattack-session dostęp 21.08.2024

Słowenia

Paweł Gawryluk

Przez lata relacje słoweńsko-rosyjskie pozostawały neutralne. Kiedy w 2013 roku w Ukrainie rozgorzała się fala licznych protestów znanych jako Euromajdan, Słowenia opowiedziała się po stronie ukraińskiej, co zaczęło powoli, ale konsekwentnie ochładzać stosunki słoweńsko-rosyjskie. Wraz z wybuchem wojny w Ukrainie relacje między Słowenią a Rosją jeszcze bardziej się pogorszyły. Słowenia jednoznacznie opowiedziała się za suwerennością Ukrainy oraz potępiła rosyjską agresję. Federacja Rosyjska wpisała Słowenię na listę nieprzyjaznych narodów przez liczne sankcje, które Słowenia nałożyła na Rosję. W porównaniu z innymi krajami regionu, rosyjskie działania hybrydowe na terenie Słowenii są znikome. Ograniczają się one głównie do szerzenia rosyjskiej propagandy i dezinformacji na słoweńskich mediach społecznościowych. Wraz
z nadejściem 2024 r. działania te rozszerzyły się również na ataki cybernetyczne wymierzone w państwowe serwisy internetowe.

Przykłady

1 24 października 2022 roku Ministerstwo Spraw Zagranicznych Federacji Rosyjskiej na portalu X (dawniej Twitter) udostępniło informacje wraz ze zdjęciami, według których Słowenia dostarczać miała Ukrainie radioaktywne odpady do tworzenia brudnych bomb. Słoweńska Agencja ds. Odpadów Promieniotwórczych wraz z niezależnymi fact-checkerami obalili rosyjskie pomówienia oraz udowodnili, iż poszczególne zdjęcia pochodzą z rosyjskich placówek lub były zrobione wiele lat temu[1].

2 27 marca 2024 roku rosyjscy hakerzy dokonali ataku DDoS na stronę internetową prezydenta Słowenii. Tego samego dnia na portalu X (dawniej Twitter) rosyjscy hakerzy z grupy Cyber Army Russian Reborn wypowiedzieli kampanie przeciwko rządowi Słowenii. Powodem tego było dołączenie Słowenii do czeskiej inicjatywy zakupu amunicji dla Ukrainy[2]. W ciągu następnych tygodni nastąpił szereg ataków na strony m.in. słoweńskiej policji, Ministerstwa Transformacji Cyfrowej, lotniska w Lublanie oraz innych instytucji rządowych. Słoweńskie media społecznościowe stały się też celem rosyjskiej dezinformacji oraz propagandy. Rosyjscy hakerzy przepraszali za ataki, które jak twierdzili były skierowane w rząd Słowenii a nie zwykłych obywateli. Przekaz opierał się na wzywaniu do jedności z Rosją z powodu tych samych kolorów flag oraz potępieniu Ukrainy, która w mniemaniu hakerów rządzona jest przez Żydów oraz faszystów. Słoweńskie służby oświadczyły, że poza wyłączeniem stron nie doszło do poważniejszych strat[3].

3 W czerwcu 2024 roku ujawniono, iż rosyjski szpieg, który został wydalony z Austrii w bieżącym roku, od 2018 roku prowadził swoje działania kontrwywiadowcze na Słowenii. Ivan Popow pracował jako korespondent rosyjskiej agencji informacyjnej TASS. W 2019 roku przeprowadził wywiad z ówczesnym premierem a obecnym ministrem obrony Słowenii Marjanem Šarecem za co obecnie minister jest krytykowany. Popow został zdemaskowany dopiero przez austriackie służby, co wypominane jest obecnie słoweńskiemu rządowi przez jego krytyków[4].

Kontrdziałania

1. 5 kwietnia 2022 roku Ministerstwo Spraw Zagranicznych Republiki Słowenii wydaliło z kraju 33 rosyjskich dyplomatów. Była to reakcja słoweńskiego rządu na zbrodnie wojenne w Buczy jakich dopuściła się Federacja Rosyjska[5]. Miesiąc później w ramach odpowiedzi Ministerstwo Spraw Zagranicznych Federacji Rosyjskiej wydaliło 4 słoweńskich dyplomatów z Moskwy[6].

2. W grudniu 2022 roku premier Słowenii Robert Golob zapowiedział budowę gazociągu do Węgier oraz Austrii. Gaz ziemny importowany miałby być z Algierii, a zapowiedziany gazociąg stanowić miałby alternatywę dla gazu z Rosji. Plan Goloba zakłada stworzenie ze Słowenii hubu gazowego na region Europy Środkowej[7].

3. 5 grudnia 2022 roku Słoweńska Agencja Wywiadu i Bezpieczeństwa (SOVA) zatrzymała dwóch rosyjskich szpiegów. Byli oni pracownikami Głównego Zarządu Wywiadowczego (GRU) i podawali się za argentyńskie małżeństwo prowadzące agencję nieruchomości. Para miała prowadzić działania kontrwywiadowcze głównie w Lublanie, ale i również w sąsiednich krajach[8]. Para szpiegów działała na terenie Słowenii od 2017 roku[9]. Aresztowanie rosyjskich szpiegów było świętowane jako ogromny sukces słoweńskich służb wywiadowczych. Była to pierwsza taka sprawa w historii niepodległej Słowenii. W październiku 2023 roku była minister spraw wewnętrznych oskarżyła premiera Roberta Goloba o to, iż celowo przesunął on datę aresztowania rosyjskich szpiegów, aby nie kolidowała ona z datą ważnego dla rządu referendum. Sprawa ta jest jedną z wielu badanych przez komisję ds. wywiadu i służb bezpieczeństwa[10].

W marcu 2024 roku rosyjski dyplomata Sergei Lemeshev został uznany przez Ministerstwo Spraw Zagranicznych Republiki Słowenii za persona non grata, co skutkowało jego wydaleniem z kraju. Według słoweńskiego rządu prowadził on działalność niezgodną ze statusem dyplomatycznym[11]. Dwa tygodnie później Rosja również wydaliła jednego słoweńskiego dyplomatę z kraju informując przy tym, iż Słowenia odpowiada za zniszczenie stosunków dwustronnych między krajami[12].

Mimo podziałów na słoweńskiej scenie politycznej, słoweńscy decydenci pozostają zgodni w kwestii uznawalności zagrożenia ze strony rosyjskiej. Słowenia aspiruje do miana lidera regionu, jednak zarazem świadoma jest swoich ograniczeń. Z tego powodu rosyjskie działania hybrydowe wymierzone w kraj wywołały w klasie rządzącej oraz słoweńskiej opinii publicznej niejako zdziwienie. Przez ograniczone możliwości słoweńskich służb, kraj okazał się idealną bazą wypadową dla rosyjskich szpiegów działających w Europie. Dopiero pomoc innych zachodnich służb wywiadowczych pozwoliła ujawnić siatkę szpiegów działających w kraju. Z uwagi na realną marginalną rolę kraju w regionie, pozostałe rosyjskie działania hybrydowe w Słowenii są marginalne i przybrały one na sile dopiero w 2024 roku nie wyrządzając jak na razie żadnych większych strat.

Przypisy

[1] S. R. Maček, Slovenia inadvertently dragged into Russian ‘dirty bomb’ campaign, https://www.euractiv.com/section/all/short_news/slovenia-inadvertently-dragged-into-russian-dirty-bomb-campaign/, dostęp: 26.07.2024 oraz S. Weber, Fact check: Russia's false case for a dirty bomb in Ukraine, https://www.dw.com/en/fact-check-russias-false-case-for-a-dirty-bomb-in-ukraine/a-63590306, dostęp: 26.07.2024.

[2] Ruski hekerji napovedali 'vojno' Sloveniji, napadli stran predsednice, https://www.24ur.com/novice/slovenija/nedosegljiva-spletna-stran-predsednice-republike.html, dostęp: 26.07.2024.

[3] J. Tepina, Ruski hekerji Sloveniji: Bodite razumevajoči in mirno sprejmite napade, https://www.24ur.com/novice/slovenija/sporocilo-ruskih-hekerjev-sloveniji-bodite-razumevajoci-in-mirno-sprejmite-trenutne-hekerske-napade.html, dostęp: 26.07.2024.

[4] Russian spy reportedly active in Slovenia for years, https://sloveniatimes.com/40608/russian-spy-reportedly-active-in-slovenia-for-years, dostęp: 26.07.2024.

[5] Słowenia wydala 33 rosyjskich dyplomatów, https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8395147,slowenia-wydalenie-rosyjskich-delegatow-zbrodnie-wojenne.html, dostęp: 25.07.2024.

[6] Slovenia told by Russia to reduce diplomatic staff in Moscow, https://sloveniatimes.com/32838/slovenia-told-by-russia-to-reduce-diplomatic-staff-in-moscow, dostęp: 26.07.2024.

[7] A. Fedorska, Słowenia kusi Węgry gazem spoza Rosji budując nowy gazociąg, https://biznesalert.pl/slowenia-gaz-algieria-wegry-rosja-energetyka/, dostęp: 25.07.2024.

[8] Two Russian spies arrested in Ljubljana, https://sloveniatimes.com/36908/two-russian-spies-arrested-in-ljubljana, dostęp: 26.07.2024.

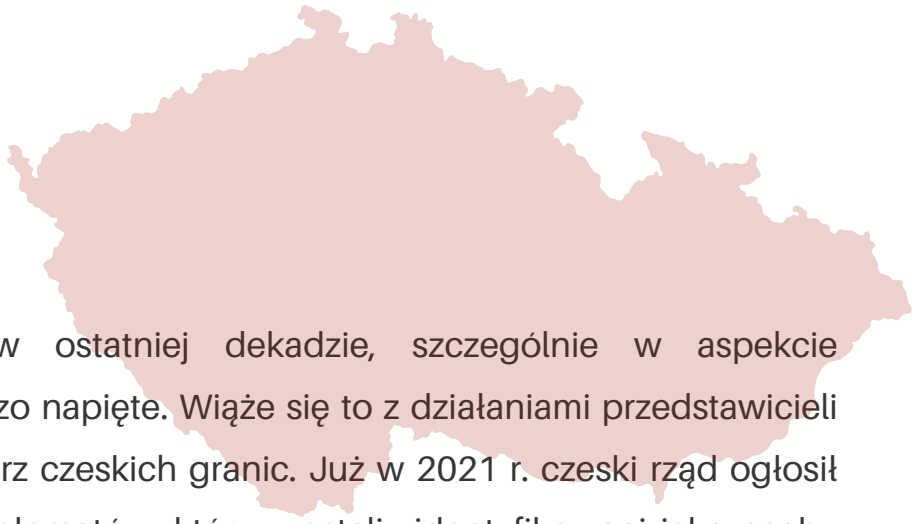
[9] S. Walker, The ‘ordinary’ family at No 35: suspected Russian spies await trial in Slovenia, https://www.theguardian.com/world/2023/mar/24/suspected-russian-spies-trial-slovenia, dostęp: 26.07.2024.

[11] Indictment filed against alleged Russian spies, https://sloveniatimes.com/37374/indictment-filed-against-alleged-russian-spies, dostęp: 27.07.2024.

[12] Russia expels Slovenian diplomat in retaliatory move, https://www.reuters.com/world/europe/russia-expels-slovenian-diplomat-retaliatory-move-2024-04-12/, dostęp: 27.06.2024

Czechy

Martyna Dorda



Relacje czesko-rosyjskie w ostatniej dekadzie, szczególnie w aspekcie dyplomatycznym, były bardzo napięte. Wiąże się to z działaniami przedstawicieli Federacji Rosyjskiej wewnątrz czeskich granic. Już w 2021 r. czeski rząd ogłosił wydalenie 18 rosyjskich dyplomatów, którzy zostali zidentyfikowani jako osoby prowadzące działalność szpiegowską. Decyzja jest konsekwencją śledztwa czeskich służb informacyjnych oraz czeskiej policji, które wykazało udział Rosji, a dokładnie agentów rosyjskiej grupy GRU, w dwóch wybuchach składów amunicji w 2014 r. we Vrběticach[1]. Od tego czasu relacje międzynarodowe coraz bardziej się ochładzały.

Pomimo bliskości geograficznej wobec Polski, w której działania hybrydowe Rosji są szczególnie złożone i widoczne, Czechy przez lata nie były głównym celem rosyjskiej kampanii hybrydowej. Były jednak dotknięte operacjami wpływu lub innymi środkami, które stanowiły bezpośrednie lub pośrednie elementy rosyjskiej kampanii hybrydowej skierowanej przeciwko innym celom.

1

W 2015 r. Bezpečnostní Informační Služba ČR (BIS – pl. Informacyjna Służba Bezpieczeństwa) w swoim corocznym raporcie określiła, że rosyjski służby wywiadowcze były najaktywniejszymi siłami zagranicznymi w Czechach. Duża część przedstawicieli rosyjskiego wywiadu używała dyplomatycznych tożsamości jako przykrywki dla ich działań o naturze dezinformacyjnej oraz szpiegowskiej. Takie możliwości stwarzała dla nich ambasada rosyjska, która w Czechach posiadała do 2021 r. dużo więcej pracowników niż wszystkie inne placówki dyplomatyczne. Tym samym Rosja i jej służby wywiadowcze miały przewagę w postaci nieproporcjonalnie dużej reprezentacji dyplomatycznej. Działanie tego typu nie są odizolowanym przypadkiem dla służb międzynarodowych, lecz w przypadku Rosji zachowania te nie zostały w żaden sposób zgłoszone do BIS, co sama Służba uznaje za oznakę prowadzenia czynności, które mogą mieć charakter zagrażający bezpieczeństwu wewnętrznemu państwa. Jest to też pierwszy raport, w którym działania rosyjskie są określone jako „non-linear (hybrid, ambiguous, irregular, non-conventional) warfare" oraz jako takie zdefiniowane[2].

2

W 2016 r. priorytetami Rosji w Czechach były operacje mające na celu wywierania wpływu na czeskich odbiorcach wobec kryzysu ukraińskiego i syryjskiego, lecz uznaje się że w szerszym kontekście były one częścią ogólnych działań hybrydowych przeciwko NATO oraz UE. Przejawiały się m.in. jako próby zakłócenia spójności i gotowości organizacji międzynarodowych (informacje mające na celu pogorszenie stosunków czesko-polskich, dezinformacja i niepokojące pogłoski zniesławiające USA i NATO), czy też pojawiały się działania dążące do zniszczenie reputacji Ukrainy, w celu odizolowania jej na arenie międzynarodowej[3][4].

3 W cyberprzestrzeni czeskiego internetu pojawiają się również rosyjskie kampanie cybernetyczne (ang. cyberespionage). APT28/Sofacy jest obecnie prawdopodobnie najbardziej aktywną i widoczną rosyjską kampanią szpiegowską obejmującą różne sfery działalności – od głównych obszarów, takich jak dyplomacja i obronność państwa, po naukę, badania i środowisko akademickie. Nie ma ona na celu samych danych jako takich, ale ostatnio skupiała się na kradzieży danych osobowych i loginów ICT. Skradzione dane i informacje mogą być wykorzystywane do różnych celów – politycznych, naukowych i przemysłowych, lub np. do oczerniania pewnych osób lub państw, dezinformacji lub szantażu[5]. W 2018 r. potwierdzone zostało, że kampania zaatakowała i skutecznie uzyskała dostęp do danych m.in.. członków Czeskich Sił Zbrojnych[6].

4 W 2019 r. na liście pięćdziesięciu najczęściej odwiedzanych stron internetowych za pośrednictwem komputerów i telefonów komórkowych w Czechach znalazło się pięć stron z Rosji, a rosyjski odpowiednik Facebooka – Vkontakte – znalazł się aż na ósmym miejscu. Niekoniecznie są to strony związane z dezinformacją i działaniami hybrydowymi, lecz po prostu zrzeszające rosyjskojęzyczną mniejszość mieszkającą w Czechach. Jednak pojawiają się raporty, że grupa ta żyje w pewnego rodzaju bańce informacyjnej związanej z wybiórczością informacji publikowanych na tych stronach[7]. Portalem typowo związanym z działaniami hybrydowymi Rosji przez lata w Czechach była krajowa odsłona Sputnika. Po rozpoczęciu się rosyjskiej agresji na Ukrainę, Czechy wraz z innymi krajami UE zablokowały do niego dostęp w imię walki z dezinformacją, lecz pośród czeskich odbiorców szybko zaczęli się pojawiać jego „następcy" oraz zmorzyła się działalność rosyjskich agentów na Telegramie. Przykładowo w 2023 r. konto neČT24 upowszechniło wideo, na którym kandydat na prezydenta – Petra Pavla ogłasza, że Czeska Republika musi wypowiedzieć wojnę Federacji Rosyjskiej[8]. Ministerstvo Vnitra (pl. Ministerstwo Spraw Wewnętrznych) w swojej analizie powyborczej potwierdziło, że konto to należało do serwisu Sputnik[9].

5 Sam portal Telegram jest w Czechach wyjątkowo rozwinięty pod względem ilości użytkowników szerzących na nim teorie spiskowe, czy rosyjską interpretację wydarzeń w Ukrainie. W 2022 r. zespół serwisu Bellingcat zwrócił uwagę przede wszystkim na osoby związane z szerzeniem skrajnie prawicowych i często prorosyjskich teorii QAnon[10].

6 W 2024 r. dyrektor czeskiego kontrwywiadu – Michal Koudelka, ujawnił ustalenia BIS, które odkryły istnienie zorganizowanej międzynarodowej siatki rosyjskich agentów, mającej na celu wpłynięcie na wynik wyborów do Parlamentu Europejskiego. Działania organizacji polegały na tym, że przedstawiciele rosyjskich służb przekazywali pieniądze europejskim politykom, głównie reprezentującym skrajnie prawicowe i prorosyjskie partie. W związku z raportem BISu czeskie władze objęły dwie osoby – Wiktora Medwedczuka i Artioma Marczewskiego, oraz jedną firmę – Voice of Europe, sankcjami uzasadniając ich działania jako „promowanie interesów polityki zagranicznej Federacji Rosyjskiej oraz działań politycznych i propagandowych skierowanych przeciwko integralności terytorialnej, niezależności, stabilności i bezpieczeństwu Ukrainy" [11].

Kontrdziałania

1. W obliczu rosyjskiej inwazji na Ukrainę w 2022 r. doszło do dalszej redukcji rosyjskich dyplomatów na terenie Czech. Zamknięto oba rosyjskie konsulaty oraz z rosyjskiej ambasady wydalono wysoko postawionych przedstawicieli służb dyplomatycznych. Tym samym zmniejszyły się możliwości rosyjskiego wywiadu, który wcześniej wykorzystywał do swoich działań wewnętrznych przykrywkę zapewnioną przez pozycje w placówkach dyplomatycznych[12].

2. BIS prowadzi szeroko zakrojone działania wywiadowcze mające na celu monitorowanie i przeciwdziałanie rosyjskim działaniom hybrydowym, w tym przede wszystkim pod szczególnym nadzorem znajdują się osoby i działania powiązane z grupą GRU. Dodatkowo Służba zajmuje się również szerzeniem rzetelnych informacji na temat rosyjskiej działalności wewnątrz czeskich granic.

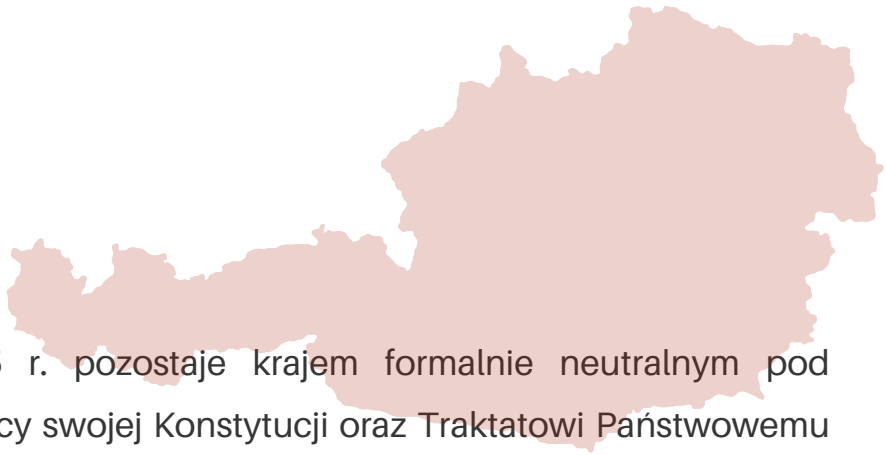
3. W ostatniej dekadzie relacje czesko-rosyjskie były napięte z powodu działań rosyjskich służb wywiadowczych w Czechach. Mimo tego, że Republika Czeska nie jest głównym celem rosyjskich działań hybrydowych to rosyjskie operacje obejmowały dezinformację, cyberataki i wpływanie na opinie publiczną w kontekście kryzysów międzynarodowych. Czechy rozpoznają Rosję jako zagrożenie oraz aktywnie podejmują kroki w celu zmniejszenia obecności rosyjskich dyplomatów i intensyfikacji działań kontrwywiadowczych, aby chronić swoje bezpieczeństwo i stabilność wewnątrz granic kraju.

Przypisy

[1] Rosyjskie zamachy w Czechach – kontekst krajowy, implikacje, perspektywy, Ośrodek Studiów Wschodnich, https://www.osw.waw.pl/pl/publikacje/analizy/2021-04-20/rosyjskie-zamachy-w-czechach-kontekst-krajowy-implikacje-perspektywy, dostęp: 28.07.2024.
[2] Report of the Security Information Service for 2015, Security Information Service Annual, 2016.
[3] Annual Report of the Security Information Service for 2016, Security Information Service, 2017.
[4] NATO znepokojují aktivity Ruska v Česku. Označilo je za zhoubné, strona internetowa Tn.nova.cz, https://tn.nova.cz/zpravodajstvi/clanek/553727-nato-znepokojuji-aktivity-ruska-v-cesku-oznacilo-je-za-zhoubne, dostęp: 28.07.2024.
[5] Statement of the MFA on the Cyberattacks Carried by Russian Actor APT28 on Czechia, strona internetowa Ministry of Foreign Affairs of the Czech Republic, https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_of_the_mfa_on_the_cyberattacks.html, dostęp: 17.07.2024.
[6] Annual Report of the Security Information Service for 2018, Security Information Service, 2019.
[7] Ruské weby sbírají ‚kliky' v Česku. Dezinformační stránky ale na vrchních příčkách vůbec nejsou, strona internetowa Lidovky.cz, https://www.lidovky.cz/domov/ruske-weby-sbiraji-kliky-v-cesku-dezinformacni-stranky-ale-na-vrchnich-prickach-vubec-nejsou.A190816_190321_ln_noviny_rkj, dostęp: 17.07.2024.
[8] Rusko se pokusilo zabránit zvolení Petra Pavla. Šířilo o něm lživé video, soudí ministerstvo vnitra, strona interntowa Forum.24.cz, https://www.forum24.cz/rusko-se-pokusilo-zabranit-zvoleni-petra-pavla-sirilo-o-nem-lzive-video-soudi-ministerstvo-vnitra, dostęp: 18.07.2024.
[9] Souhrn poznatků k českým prezidentským volbám 2023, strona internetowa Ministerstvo Vnitra ČR, https://www.mvcr.cz/chh/clanek/souhrn-poznatku-k-ceskym-prezidentskym-volbam-2023.aspx, dostęp: 17.07.2024.
[10] Telegram je nový dark web. Pro Čechy jde téměř o neomezenou cestu ke konspiračním teoriím, strona internetowa Hlidacipes.org, https://hlidacipes.org/telegram-je-novy-dark-web-pro-cechy-jde-temer-o-neomezenou-cestu-ke-konspiracnim-teoriim/, dostęp: 18.07.2024.
[11] Czechy ujawniają sieć szpiegowską Rosji w UE. Przeszukania także w Polsce, strona internetowa Euractiv.pl, https://www.euractiv.pl/section/polityka-zagraniczna-ue/news/czechy-ujawniaja-siec-szpiegowska-rosji-w-ue-przeszukania-takze-w-polsce/, dostęp: 28.07.2024.
[12] Annual Report of the Security Information Service for 2022, Security Information Service, 2023.

Austria

Martyna Dorda



Republika Austrii od 1955 r. pozostaje krajem formalnie neutralnym pod względem militarnym na mocy swojej Konstytucji oraz Traktatowi Państwowemu (niem. Die Unterzeichnung des Staatsvertrags). Współcześnie neutralność ta staje się coraz bardziej problematyczna w utrzymaniu wobec wydarzeń na arenie międzynarodowej[1]. W ostatnich dekadach Austria utrzymywała z Rosją dobre relacje w szczególności pod względem ekonomicznym oraz przemysłowym – m.in. podpisanie w 2018 r. wydłużenia rosyjskich dostaw gazu Gazpromu do Austrii aż do 2040 r. Dodatkowo, pod względem politycznym, w 2016 r. lider partii Freiheitliche Partei Österreichs (FPÖ – pl. Wolnościowa Partia Austrii) podpisał porozumienie dotyczące kooperacji z panującą partią rosyjską Единая Россия, Jedinaja Rossija (pl. Jedna Rosja). Wobec rosyjskiej inwazji na Ukrainę w 2022 r., Austria pozornie pozostała neutralna szczególnie pod względem militarnym, z częścią polityków FPÖ nawołującą wręcz do całkowitego odcięcia się od tych wydarzeń, lecz jako państwo członkowskie Unii Europejskiej (UE) nałożyła na Rosję sankcje proponowane przez Wspólnotę[2]. Rząd austriacki uznał również część rosyjskich dyplomatów jako person non grata oraz w późniejszych miesiącach 2022 r. i 2023 r. wydalił aż 8 dyplomatów za zachowania niezgodne z ich statusem dyplomatycznym[3]. Pomimo tego Austria pozostaje z Rosją w ścisłych relacjach gospodarczych i przemysłowych pod względem importu rosyjskiego gazu oraz z austriackimi przedsiębiorstwami nadal operującymi w Rosji.

Rosja podejmowała działania hybrydowe wobec Austrii jeszcze długo przed 2022 r., szczególnie w 2014 r. przed samą aneksją przez rosyjskie wojska terenów Krymu, w przestrzeni internetowej pojawiały się coraz to częstsze kampania promujące ambicje dotyczące Wielkorosji.

1

Po 2014 r. rosyjskie działania hybrydowe w Austrii były szczególnie widoczne w postaci cyberataków. W maju 2023 r. po wycieku tzw. „Vulkan files”[4] Bundesministerium für Inneres (BMI – pl. Ministerstwo Spraw Wewnętrznych) wydało ogłoszenie, że od rozpoczęcia się inwazji rosyjskiej na Ukrainę zarejestrowało zwiększoną liczbę rosyjskich ataków cybernetycznych. Pomimo informacji zawartych w „Vulkan files” na temat rosyjskich strategii prowadzenia kampanii dezinformacyjnych oraz ataków hakerskich grupy Sandworm, ministerstwo zaznaczyło że nie znajdują się tam żadne dokładniejsze informacje, które byłby pomocne oraz ogłosiło że: „Firmy i władze muszą w dalszym ciągu inwestować w swoje bezpieczeństwo IT i chronić się przed potencjalnymi atakami” (tł. własne)[5].

2

Austriackie strony internetowe nie są tak częstym celem rosyjskich fabryk trolli czy botów, lecz nadal w przestrzeni wirtualnej pojawiają się portale, które szerzą prorosyjską dezinformację. Przykładem tego może być „Ukrainian Expat”, który pojawia się w ukierunkowanych reklamach użytkowników w okolicach Wiednia, obserwujących autentyczne portale informacyjne na serwisie X (uprzednio Twitter). Rzekoma autorka bloga „Anna” jest rosyjskojęzyczną Ukrainką, która obecnie mieszka w Serbii i chce krytycznie zaangażować się w wydarzenia w swojej ojczyźnie. Autorka używa rosyjskiego języka propagandowego, pisząc m.in. o „prześladowaniach etnicznych Rosjan” na Ukrainie od czasu wojny w Donbasie w 2014 r. Kod źródłowy bloga pokazuje, że wykorzystuje on tzw. „wtyczkę geotargetingową” – oznacza to, że treść targetowane są dopasowywane do lokalizacji odbiorcy[6]. Tego typu konta są notorycznie zawieszane lub znikają z portali internetowych, po to aby ponownie pojawić się w nowej odsłonie po jakimś czasie.

3 Jan Marsalek – z pochodzenia Austriak, był kluczową postacią w jednym z największych skandali finansowych w historii Niemiec. Jako członek zarządu Wirecard, był odpowiedzialny za międzynarodowe operacje firmy, w tym nadzór nad finansami w regionie Azji-Pacyfiku, gdzie doszło do oszustw finansowych na ogromną skalę. Firma ogłosiła bankructwo w 2020 r., kiedy okazało się, że brakuje w jej bilansach 1,9 mln euro. Marsalek był podejrzany o udział w fałszowaniu ksiąg i wyprowadzaniu funduszy. Po ujawnieniu skandalu Marsalek zbiegł, uważa się, że ukrywał się w Rosji lub na Białorusi, gdzie utrzymywał kontakty z rosyjskimi służbami wywiadowczymi. W 2023 r. Wall Street Journal opublikował artykuł ogłaszający, że Marsalek przez niemal dekadę działał jako agent rosyjskiego wywiadu, m.in. wspierając Grupę Wagnera i przekazując Moskwie informacje na temat niemieckich służb wywiadowczych. Zachodnie służby uważają, że podczas kierowania Wirecard, pomagał w organizowaniu płatności rosyjskich służb wywiadu wojskowego (GRU) i zagranicznego (SWR), a także przekazywał im informacje na temat klientów spółki, do których zaliczały się niemieckie służby wywiadowcze i Federalny Urząd Śledczy (BKA). Dodatkowo jest również oskarżany o zaangażowanie w rekonfigurację biznesowego imperium Prigożyna w Afryce.

4 Austria rozpoznaje dezinformację jako jedną z technikach działań hybrydowych Rosji. Po inwazji na Ukrainę wraz z innymi krajami UE podjęła decyzję wobec wstrzymaniu działalności nadawczej rosyjskich mediów państwowych na swoim terytorium. Jeszcze przed tym rosyjskie portale szerzyły wiadomości mające na celu kontrolę narracji wobec rosyjskich działań imperialistycznych, m.in. dotyczyły one poniższych tematów:

- Ukazywanie Rosji i Ukrainy jako historycznie jedno państwo,
- Rzekome narażenie populacji rosyjskojęzycznej w Donbasie na okrucieństwa ze strony Ukraińców,

Nazywanie inwazji oraz wojny „Operacją specjalną" mającą na celu denazyfikację Ukrainy[7].

Kontrdziałania

1. Z racji rosnących globalnych zagrożeń oraz rosyjskich działań hybrydowych rząd austriacki podjął decyzje o pierwszej od 10 lat zmianie ich die nationale Cyber-Sicherheitsstrategie (ÖSS – pl. Strategia bezpieczeństwa cybernetycznego). Obecnie cyberbezpieczeństwo Austrii skupia się na wczesnym wykrywaniu zagrożeń i niedopuszczaniu do ichrozwoju[8].

2. Austriacka Minister Obrony Klaudia Tanner chce wzmocnić obronę kraju nie tylko w kontekście ataków militarnych, lecz również hybrydowych[9]. Podobne stanowisko zajmuje dokument stanowiący austriacką analizę polityki bezpieczeństwa międzynarodowego Risikobild 2024 – Welt aus den Fugen[10].

3. Austriackie instytucje zarówno rządowe jak i te pochodzące z trzeciego sektora prowadzą research oraz badania dotyczące hybrydowych działań Rosji, zajmują się publikacją tematycznych raportów oraz prowadzą fact-checking wobec dezinformacji. M.in. Austrian Center for Intelligence, Propaganda and Security Studies (ACIPSS), czy też Austria Instituts für Europa- und Sicherheitspolitik (AIES).

Pomimo militarnej neutralności Austrii i wewnętrznych sporów dotyczących postawy jaką kraj powinien przyjąć w obliczu rosyjskiej agresji, rząd austriacki jest wyraźnie świadomy hybrydowych zagrożeń, które stwarza dla niego Rosja. Jednakże władze austriackie nadal importują rosyjski gaz oraz pozwalają na prowadzenie działalności gospodarczej w Rosji, mimo podjęcia działań takich jak wydalenia rosyjskich dyplomatów czy nałożenie sankcji. Tym samym w polityce austriackiej wobec Rosji wybija się wyraźny dualizm oraz brak konsekwentnych działań.

Przypisy

[1] D. Imwinkelried, Wehe den Kritikern, die Österreichs Neutralität infrage stellen, strona internetowa NZZ.ch, https://www.nzz.ch/international/oesterreich-der-ukraine-krieg-und-die-neutralitaet-ld.1733922, dostęp: 18.07.2024 r.

[2] Auswirkungen des Konflikts in der Ukraine auf Österreich, strona internetowa verteidingungspolitik.at, https://verteidigungspolitik.at/auswirkungen-des-konflikts-in-der-ukraine-auf-%C3%96sterreich, dostęp: 18.07.2024 r.

[3] Österreich weist zwei russische Diplomaten aus, strona internetowa Zeit.de, https://www.zeit.de/politik/ausland/2024-03/oesterreich-russland-diplomaten-ausgewiesen-spionage, dostęp: 28.07.2024 r.

[4] 'Vulkan files' leak reveles Putin's global and domestic cyberwarfare tactics, strona internetowa The Guardian, https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics, dostęp: 29.07.2024 r.

[5] Innenministerium: Vermehrt russische Cyberangriffe, strona internetowa Saltsburgen Nachrichten, https://www.sn.at/politik/innenpolitik/innenministerium-vermehrt-russische-cyberangriffe-136440850, dostęp: 29.07.2024 r.

[6] J. Denkmayr, J. Melchar, Russische Fake News erreichen Österreich, stona interntowa Kleine Zeitung, https://www.kleinezeitung.at/politik/aussenpolitik/18219147/mutmassliche-russische-fake-news-nun-auch-in-oesterreich, dostęp: 29.07.2024 r.

[7] M. Zinkanell, Die russische hybride Kriegsführung. Im Kontext des Angriffskriegs gegen die Ukraine, AIES Austrian Institute for European and Security Policy STUDY, Bundesministrum Landesverteiding, Nr 2023/3, 2023.

[8] Bundeskazleramt, Österreichische Sicherheitsstrategie, strona internetowa bundeskazleramt.gv.at, https://www.bundeskanzleramt.gv.at/themen/sicherheitspolitik/sicherheitsstrategie.html, dostęp: 29.07.2024 r.

[9] L. Mahnke, Risiko „sehr hoch": Österreich warnt vor Angriff aus Russland, strona internetowa Merkur.de, https://www.merkur.de/politik/konfliktherde-oesterreich-bundesheer-bericht-risikobild-warnung-frieden-krieg-verteidigung-zr-92804346.html, dostęp: 29.07.2024 r.

[10] Bundesministerium für Landesverteidigung (BMLV), Risikobild 2024 – Welt aus den Fugen, 2024.

Estonia

Antonina Sołtysiak

Estonię łączy z Federacją Rosyjską nie tylko granica licząca prawie 300 kilometrów, ale także liczna mniejszość rosyjska stanowiąca ¼ całej ludności. Do tego dochodzi również rozległa historia obu krajów, która sięga I wojny światowej. Dziś środki wpływu stosowane przez Rosję różnią się jednak od tych używanych ponad 100 lat temu. Wraz z rozwojem technologicznym na świecie, popularność zaczęły zyskiwać ataki cybernetyczne. Zwłaszcza w Rosji wykształcili się najlepsi hakerzy, którzy często bezproblemowo mogli naruszać pracę, m.in. stron rządowych wielu państw. Estonia nie była tutaj wyjątkiem, lecz w tym wypadku doszedł również fakt wspólnej historii z czasów sowieckich. Ten aspekt często stawał się kością niezgody oraz wystarczającym powodem na atak na kraj bałtycki. Zarzewiem przyszłych cyberataków stały się wydarzenia z 2007 roku, gdy Rosja po raz pierwszy zaatakowała przestrzeń internetową Estonii.

Estonia w celu zapobiegnięcia przyszłym podobnym incydentom, szybko rozwinęła swój system ochrony komputerowej. Dziś, jest uważana za kraj wysoko rozwinięty pod tym względem i odporny na wszelkie ataki zewnętrzne. Należy również wspomnieć, iż w 2008 roku w Tallinie powstało Centrum Doskonalenia Obrony Cybernetycznej NATO. To Estonia jest dzisiaj liderem w Europie, jeśli chodzi o system ochrony. Okazało się to bardzo ważne przede wszystkim po wybuchu wojny w Ukrainie. Rosja od tego momentu prowadziła działania nie tylko na froncie, ale też w państwach otwarcie wspierających Kijów. Działania hybrydowe stały się dziś przykrą codziennością, jednak Estonia dobrze sobie z nimi radzi. Mimo iż ataków jest dużo, nie wpływają one na życie Estończyków. Są one na bieżąco odpierane i dzięki temu wręcz niewidoczne.

Kwiecień 2007- Po decyzji rządu estońskiego o przeniesieniu pomnika żołnierza sowieckiego z centrum Tallina na cmentarz wojskowy rozpoczęły się liczne protesty prorosyjskich aktywistów. Dzień później, 27 kwietnia doszło do zmasowanych cyberataków przede wszystkim na strony rządowe oraz publiczne. Ataki trwały 22 dni. Polegały głównie na ograniczeniu dostępu, bądź zalewania stron spamem. W odpowiedzi, rząd Estonii zamknął granice cyfrowe państwa oraz ograniczył ruch na swoich stronach internetowych. Był to pierwszy tak poważny cyberatak na bezpieczeństwo estońskie[1].

Sierpień 2022- Zmasowany atak na ok. 200 stron rządowych i prywatnych instytucji. Było to spowodowane decyzją o przeniesieniu zabytkowego czołgu sowieckiego Tu-34 z centrum miasta Narva do Estońskiego Muzeum Wojskowego. Spotkało się to (podobnie jak w 2007 roku) z niezadowoleniem przede wszystkim mniejszości rosyjskiej, która uważa, że w ten sposób Tallin chciał "zamazać" kawałek historii. W związku z tym, rosyjska grupa Killnet przeprowadziła atak, który jednak nie wyrządził znacznych szkód, jedynie utrudnił dostęp do wielu stron internetowych i naruszył przepływ danych[2].

Wrzesień 2023 - Atak DDoS (Distributed Denial-of-Service) na stronę internetową estońskiego przewoźnika kolejowego Elron. W czasie ataku, strona nie działała przez 24 godziny, co uniemożliwiło zakup biletów zarówno przez Internet, jak i w pociągu[3].

Marzec 2024 - Atak rosyjskich hakerów na rządowe strony Estonii, m.in. na Zarządu Policji i Służby Granicznej (The Police and Border Guard Board), Urzędu Celno-Skarbowego (The Tax and Customs Board) oraz na Ministerstwo Sprawiedliwości. Trwający dwa dni atak znacznie utrudnił dostęp do wielu stron urzędowych, na których można załatwiać wiele podstawowych spraw, np. składać dokumenty. Estonia jednak dzięki swoim rozwiniętym środkom ochrony komputerowej, szybko poradziła sobie z problemem, a atak nie wyrządził żadnych trwałych szkód w systemie[4].

Kontrdziałania

1. Utworzenie “ambasady danych” Estonii w Luksemburgu[5].

2. Rząd Estonii przez lata inwestował i dbał o edukację oraz programy dla dzieci, które zaznajamiały je z technologią. Takie programy również funkcjonują dla starszych osób. Tallin stawia na edukację i przygotowanie społeczeństwa na szybkie wykrywanie manipulacji oraz radzenie sobie z nią[6].

3. Utworzenie Estońskiego Departamentu Systemu Informacji (RIA).

Przypisy

[1] How a cyber attack transformed Estonia, BBC News, https://www.bbc.com/news/39655415, dostęp: 29.07.2024.

[2] Estonia repels cyberattacks claimed by Russian hackers, Al Jazeera, https://www.aljazeera.com/news/2022/8/18/estonia-says-it-repelled-cyber-attacks-claimed-by-russian-group, dostęp: 29.07.2024.

[3] RIA on Elron cyberattack: It is likely that it will happen again, ERR News, https://news.err.ee/1609108433/ria-on-elron-cyberattack-it-is-likely-that-it-will-happen-again, dostęp: 29.07.2024.

[4] Massive cyberattack on Estonian gov't institutions, TVP World, https://tvpworld.com/76379715/estonian-govt-institutions-targeted-in-largest-cyber-attack-in-countrys-history, dostęp: 29.07.2024.

[5] Data Embassy- e- Estonia, e- Estonia, https://e-estonia.com/solutions/e-governance/data-embassy/, dostęp: 29.07.2024.

[6] How Russian threats in the 2000s turned Estonia into the go-to expert on cyber defense, CNN Business, https://edition.cnn.com/2021/06/18/tech/estonia-cyber-security-lessons-intl-cmd/index.html, dostęp: 29.07.2024.

Sfinansowano ze środków
Narodowego Instytutu Wolności w ramach programu
Korpus Solidarności – Wsparcie organizacji wolontariatu w NGO.

KOMITET DO SPRAW POŻYTKU PUBLICZNEGO

NIW
Narodowy Instytut Wolności
Centrum Rozwoju Społeczeństwa Obywatelskiego

Program Wspierania i Rozwoju Wolontariatu Długoterminowego na lata 2018–2030
Korpus Solidarności