Marta CHODYKA

Akademia Bialska im. Jana Pawła II
ORCID: 0000-0002-8819-2451

Sławomir ŻURAWSKI

Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0001-9527-3391

Weronika PARCZEWSKA

Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego
ORCID: 0009-0005-8768-4736

https://doi.org/10.29316/9788368103236_18

WPŁYW CYBERZAGROŻEŃ NA BEZPIECZEŃSTWO GRANICY RZECZYPOSPOLITEJ POLSKIEJ

THE IMPACT OF CYBER THREATS ON THE SECURITY OF THE BORDER OF THE REPUBLIC OF POLAND

Streszczenie

Celem niniejszego rozdziału jest kompleksowa analiza wpływu cyberzagrożeń na bezpieczeństwo granicy Rzeczypospolitej Polskiej. W pierwszej części przedstawiono charakterystykę współczesnych cyberzagrożeń w kontekście ochrony granicy państwowej, w tym ich klasyfikację, mechanizmy działania oraz wybrane przypadki realnych incydentów. Część druga koncentruje się na identyfikacji

Abstract

The purpose of this chapter is to comprehensively analyze the impact of cyber threats on the security of the border of the Republic of Poland. The first part presents the characteristics of modern cyber threats in the context of state border protection, including their classification, mechanisms of action and selected cases of real incidents. The second part focuses on the identification of key vulnerabilities and

kluczowych podatności i wrażliwych komponentów infrastruktury granicznej RP – zarówno na poziomie systemów informatycznych, jak i organizacyjno-proceduralnym. Trzecia część poświęcona została analizie aktualnych i planowanych działań przeciwdziałających cyberzagrożeniom, zarówno w wymiarze krajowym, jak i międzynarodowym, z uwzględnieniem strategii, instrumentów prawnych, systemów reagowania oraz inicjatyw współpracy międzynarodowej. Zastosowana metodologia opiera się na analizie literatury przedmiotu, dokumentów strategicznych, raportów eksperckich oraz aktualnych doniesień medialnych i wyników badań naukowych. Rodział ma charakter przeglądowo-analityczny, ukierunkowany na ukazanie złożoności problematyki oraz potrzebę dalszego doskonalenia zdolności obronnych państwa w cyberprzestrzeni – zwłaszcza w obszarze ochrony granic.

Słowa kluczowe: cyberbezpieczeństwo, granica państwowa, wojna hybrydowa infrastruktura krytyczna, Straż Graniczna

sensitive components of the Polish border infrastructure – both at the level of IT systems and organizational and procedural. The third part is devoted to the analysis of current and planned activities counteracting cyber threats, both in the national and international dimension, taking into account strategies, legal instruments, response systems and international cooperation initiatives. The methodology used is based on the analysis of the literature on the subject, strategic documents, expert reports and current media reports and scientific research results. The chapter is of a review and analytical nature, aimed at showing the complexity of the issues and the need to further improve the state's defense capabilities in cyberspace – especially in the area of border protection.

Keywords: cybersecurity, state border, hybrid warfare, critical infrastructure, Border Guard

Wstęp

Współczesne środowisko bezpieczeństwa państwowego uległo głębokiej transformacji wskutek dynamicznego rozwoju technologii informacyjnych oraz rosnącego znaczenia cyberprzestrzeni jako nowego wymiaru działań wrogich. Coraz częściej granice państwowe nie są postrzegane jedynie jako fizyczna linia rozdziału terytoriów, lecz jako wrażliwe punkty styku systemów informacyjnych, infrastruktury krytycznej oraz sfery polityki bezpieczeństwa wewnętrznego i międzynarodowego. Cyberzagrożenia – obejmujące m.in. ataki na systemy teleinformatyczne, działania dezinformacyjne, manipulację danymi czy sabotaż infrastruktury cyfrowej – stają się narzędziem strategicznego oddziaływania, niejednokrotnie wykorzystywanym w ramach wojen hybrydowych, presji politycznej oraz operacji wywiadowczych.

Polska jako państwo graniczne Unii Europejskiej i NATO, stanowi kluczowy element wschodniej flanki Zachodu. Sytuacja geopolityczna – zwłaszcza w kontekście trwającej wojny rosyjsko-ukraińskiej, destabilizacji Białorusi oraz presji

migracyjnej – powoduje, że infrastruktura graniczna RP znajduje się w centrum zainteresowania nie tylko grup przestępczych, ale także wyspecjalizowanych podmiotów państwowych wykorzystujących środki cybernetyczne do realizacji celów politycznych i militarnych. Incydenty związane z ingerencją w systemy monitoringu, próby zakłócenia pracy przejść granicznych, manipulowanie bazami danych cudzoziemców czy dezinformacja w mediach społecznościowych wskazują na konieczność zintegrowanego podejścia do ochrony granic w ujęciu cyberbezpieczeństwa.

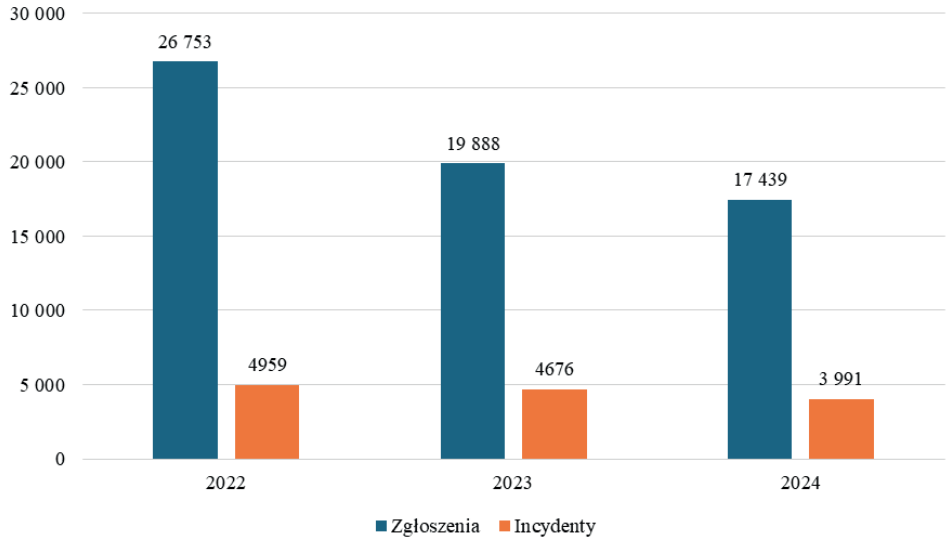
Charakterystyka cyberzagrożeń w kontekście ochrony granicy RP

Cyberzagrożenia wobec granicy państwowej to problem zarówno o charakterze krajowym, jak i międzynarodowym. Integracja technologii informacyjno-komunikacyjnych z systemami nadzoru granicznego powoduje, że każde naruszenie tych systemów może skutkować poważnymi zakłóceniami funkcjonowania kontroli granicznej oraz incydentami bezpieczeństwa[1].

W Polsce od 2015 r. nastąpił gwałtowny wzrost liczby zgłaszanych incydentów ICT[2]. W roku 2024 Zespół CSIRT GOV zarejestrował łącznie 17 439 zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego w swoim obszarze kompetencyjnym, spośród których 3 991 zostało zakwalifikowanych jako faktyczne incydenty bezpieczeństwa teleinformatycznego. Porównanie ostatnich lat przedstawiono na rysunku 1.

[1] R. Girod, *Border Security: Vulnerability and Emerging Global Security Threats*, Global Security and Intelligence Studies, Volume 8, Number 1, 2023, s. 222.

[2] M. Kamiński, Z. Śliwa, *Poland's Threat Assessment Deepened, Not Changed*, PRISM 10, no. 2, s. 135.



Rysunek 1. Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2022-2024
Źródło: raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku, s. 10.

Prezentowana statystyka obejmuje zgłoszenia oraz incydenty obsługiwane przez Zespół CSIRT GOV, z wyłączeniem zgłoszeń przekazywanych za pośrednictwem systemu ARAKIS GOV. Zaobserwowano spadek liczby zgłoszeń, co bezpośrednio wpłynęło na zmniejszenie liczby incydentów odnotowanych w 2024 roku. Zespół CSIRT GOV wskazuje, że na zaistniałą zmianę miało wpływ kilka kluczowych czynników:

- prowadzenie proaktywnych działań zwiększających świadomość użytkowników poprzez szkolenia – w 2024 roku przeszkolono oraz udzielono konsultacji około 1900 osobom, co stanowi znaczący wzrost względem roku 2023, kiedy to przeszkolono ok. 500 osób;
- systematyczne informowanie o zidentyfikowanych podatnościach w zakresie kompetencji Zespołu;
- bieżące wydawanie rekomendacji CSIRT GOV adekwatnych do poziomu zagrożenia CRP;
- regularna dystrybucja wskaźników kompromitacji dotyczących monitorowanych kampanii;
- cykliczne realizowanie ocen bezpieczeństwa systemów teleinformatycznych;
- wdrażanie przez instytucje rozwiązań bezpieczeństwa pozwalających skutecznie mitygować ataki już we wczesnych fazach.

Wszystkie wymienione działania przyczyniły się do skuteczniejszego przeciwdziałania zagrożeniom w obszarze cyberbezpieczeństwa[3]. W literaturze cyberzagrożenia tradycyjnie dzielą się na kilka kategorii:

- ransomware (zaszyfrowanie danych i żądanie okupu),
- phishing (manipulacja socjotechniczna celem uzyskania dostępu),
- DDoS (atak typu odmowa usługi),
- malware, kradzież danych,
- wycieki informacji oraz zagrożenia IoT (urządzeń podłączonych do sieci)[4].

Systemy kontroli granicznej stanowią infrastrukturę krytyczną – obejmują monitoring wizyjny (kamery CCTV), sieci komunikacyjne, bazy danych pasażerów, system Schengen (SIS), rejestry meldunkowe i systemy wspomagające Straż Graniczną[5]. Ich wsparcie i integracja w cyberprzestrzeni oznaczają, że są one celem potencjalnych cyberataków, a ich naruszenie może doprowadzić do utraty integralności danych, sabotowania przepływu informacji, a nawet paraliżu kontroli migracji[6].

W maju 2025 roku ukazały się doniesienia, że GRU (jednostka 26165, znana jako APT 28/Fancy Bear) próbowała włamać się do systemów kamer granicznych oraz kolejowej infrastruktury w Polsce, Rumunii, na Węgrzech i Słowacji, by zakłócić transport pomocy humanitarnej do Ukrainy. Wśród około 10 000 skompromitowanych kamer około 4 % znajdowało się w Polsce[7]. Równolegle raport Europolu z marca 2025 roku wskazuje, że aktorzy hybrydowi (w tym państwowi i przestępczy) działają wspólnie w celu destabilizacji UE: sabotaż, ataki cybernetyczne, dezinformacja i przemyt migrantów – jako elementy taktyki kumulatywnej niwelującej stabilność systemu państwowego[8].

---

3 Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku, s. 10.

4 M. Terlecka-Maciejewska, *Cybersecurity in polish security system*, Scientific Papers of Silesian University of Technology. Organization and Management, no. 198, 2024, s. 561-562.

5 J. Świerczyńska, *The importance of border surveillance and border traffic control at the eastern border of the Republic of Poland to the cross-border security of the European Union*, Central European Review of Economics & Finance, 44(3), 2023, s. 155.

6 M. Marczyk, M. Błachut, *Information security as part of Poland's security*, Scientific Journal of the Military University of Land Forces, Volume 54, Number 4(206), 2022, s. 610.

7 Russia accused of trying to hack border security cameras to disrupt Ukraine aid, The Guardian, https://www.theguardian.com/world/2025/may/21/russia-accused-trying-disrupt-aid-ukraine-hacking-border-crossings, [dostęp: 30.07.2025].

8 Russia using criminal networks to drive increase in sabotage acts, says Europol, Cybercrime, The Guardian, https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol, [dostęp: 30.07.2025].

Zagrożenia typu APT (Advanced Persistent Threat) są wyjątkowo niebezpieczne: to długotrwałe, ukierunkowane ataki na krytyczne systemy, często prowadzone przez państwowe służby wywiadowcze. W przypadku Polski znacząca część ruchu złośliwego pochodzi z rosyjskiego cybersfery. Dezinformacja i kampanie manipulacyjne skierowane są ku społeczności lokalnej i migrantom: celem jest zakłócenie przekazu instytucji państwowych, prowokowanie fake newsów dotyczących procedur granicznych i stanu bezpieczeństwa. Polska jest według rządu najbardziej atakowanym krajem w UE pod względem cyberataków i dezinformacji w związku z wyborami prezydenckimi w maju 2025 r.[9].

Na poziomie infrastruktury zagrożone są najbardziej takie elementy jak:

- Systemy CCTV na przejściach granicznych i przy szlakach transportowych;
- Systemy komunikacji danych i logistyki kolei przeładunkowej;
- Bazy danych dokumentów tożsamości i meldunkowe;
- System Schengen (SIS II) – choć stworzony z wysokim poziomem zabezpieczeń, może być podatny na ataki typu insider threat lub phishing celowany;
- Łączność sieciowa SG i innych służb, transport danych wrażliwych, systemy awaryjne.

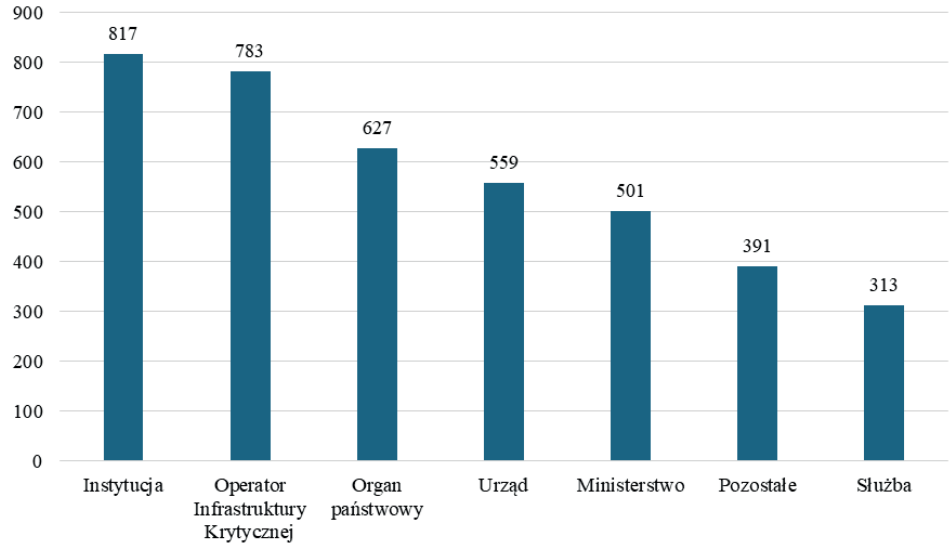
Przerwanie działania któregokolwiek z tych komponentów może prowadzić do zatrzymania kontroli ruchu, utraty danych dotyczących ruchu migracyjnego i ryzyka infiltracji osób nieuprawnionych. Wojna hybrydowa, stosowana przez państwa takie jak Rosja, łączy środki konwencjonalne i niekonwencjonalne – w tym cyberataki, dezinformację, manipulację migracyjną. Celem jest erozja zaufania instytucji, destabilizacja systemu i wyczerpanie odporności społecznej. Europol wskazuje, że przestępcze grupy funkcjonują jako „cienie", działając na rzecz państwowych aktorów hybrydowych – realizując ataki typu sabotaż, kradzież danych[10], co osłabia integralność funkcjonowania granic UE, w tym Polski.

Wzrost liczby incydentów w administracji rządowej powoduje potrzebę rozwoju mechanizmów detekcji, reakcji i koordynacji. Analizując podział incydentów na sektory, w 2024 roku najwięcej przypadków odnotowano w sektorze Instytucji oraz Operatorów Infrastruktury Krytycznej, tak jak w roku 2023. Kolejne miejsca pod względem liczby zarejestrowanych incydentów zajmowały sektory: Organ Państwowy, Urząd, Ministerstwo, Pozostałe oraz Służba. Poniżej na rysunku 2

[9] Poland 'most attacked' online by Russia, says minister, https://www.ft.com/content/e0e1a016-e4e0-4628-a0ac-c4a6e9d15db6, [dostęp: 30.07.2025].

[10] Russia using criminal networks to drive increase in sabotage acts, says Europol | Cybercrime | The Guardian, https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol, [dostęp: 30.07.2025].

przedstawiono liczbę incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa w 2024 roku z podziałem na sektory.



Rysunek 2. Liczba incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa w 2024 roku z podziałem na sektory

Źródło: raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku, s. 14.

Infrastruktura graniczna jako punkt krytyczny: chociaż dotąd atakowana rzadziej niż instytucje rządowe, struktura ta staje się coraz bardziej cyfrowa i podatna. Aspekty reputacyjne i polityczne: destabilizacja poprzez cyberprzestrzeń wpływa na zaufanie obywateli oraz relacje z UE i NATO.

Analiza literatury i dostępnych danych potwierdza, że cyberzagrożenia skierowane na infrastrukturę ochrony granicy RP są realne, coraz bardziej złożone i powiązane z działaniami hybrydowymi. Kluczowymi formami zagrożeń są APT, phishing, ransomware, sabotaż cyfrowy oraz kampanie dezinformacji. Konsekwencje takich ataków mogą przełożyć się na zakłócenia kontroli granicznej, manipulację danymi, destabilizację procedur migracyjnych i wzrost ryzyka przedostania się osób nieuprawnionych.

Wrażliwość i zagrożenia dla systemów granicznych RP

Wpływ cyberzagrożeń na bezpieczeństwo granicy Rzeczypospolitej Polskiej jest dzisiaj jednym z najważniejszych wyzwań strategicznych. Polska jako

zewnętrzna granica Unii Europejskiej, staje się celem zarówno tradycyjnych form przestępczości transgranicznej, jak i wyrafinowanych działań cybernetycznych, które mogą zakłócić funkcjonowanie systemów kontroli granicznych, logistykę transportową oraz wymianę informacji w ramach unijnych struktur.

W odniesieniu do specyfiki funkcjonowania granicy RP, zasadniczym zagrożeniem staje się nie tyle typowa przestępczość, co złożone działania hybrydowe. Raport Europolu z 2025 r. wskazuje, że państwowe struktury oraz powiązane z nimi organizacje przestępcze działają wspólnie, by realizować tzw. „shadow alliance" – sieć wykorzystującą zarówno sabotaż, cyberataki, jak i przemytnicze operacje migrantów, mając na celu destabilizację państw członkowskich UE, w tym Polski.

Rola infrastruktury transportowej jako elementu granicy państwowej jest szczególnie narażona na ataki. W 2023 r. zarejestrowano proste, choć skuteczne działania sabotażowe — nadanie przez radio niezaszyfrowanego sygnału STOP na częstotliwości 150 MHz spowodowało awaryjne zatrzymanie ponad 20 pociągów. Choć incydent wykorzystywał technologię analogową, jego skutki wskazują, jak niskim kosztem można sparaliżować kluczową infrastrukturę transportową, co ma bezpośrednie przełożenie na bezpieczeństwo graniczne[11].

Te działania ukazują, że systemy graniczne stanowią złożoną infrastrukturę cyberfizyczną, gdzie połączenie elementów IT i OT – kamery, systemy komunikacji, rejestry danych oraz urządzenia sterujące ruchem – stanowi potencjalne wektory ataku. Jak podkreślają badania nad systemami ICS i OT, wiele protokołów i urządzeń przemysłowych działa w systemach legacy, z niewystarczającym zabezpieczeniem, co czyni je atrakcją dla atakujących, którzy są w stanie wpływać na procesy fizyczne przez sieć[12].

W kontekście prawnym i administracyjnym, Polska podjęła działania mające na celu zbudowanie krajowego systemu cyberbezpieczeństwa. Strategia na lata 2019-2024 ustanowiła mechanizmy współpracy między Ministerstwem Cyfryzacji, ABW, NASK, CSIRT-ami oraz innymi instytucjami, które w kooperacji międzynarodowej – NATO czy UE – budują zdolności reagowania i wymiany informacji.

Niemniej skuteczność tych systemów w odniesieniu do ochrony granic zależy od możliwości monitorowania, wykrywania i szybkiego reagowania na incydenty specyficzne dla infrastruktury granicznej. Ogromna liczba zgłoszeń incydentów

[11] The Cheap Radio Hack That Disrupted Poland's Railway System, WIRED, https://www.wired.com/story/poland-train-radio-stop-attack, [dostęp: 30.07.2025].

[12] G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger, J. Benjamin, Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures, https://arxiv.org/abs/2109.03945, [dostęp: 30.07.2025].

ICT zgłaszanych do CSIRT GOV wskazuje wyraźnie na skalę wyzwania. Choć zdecydowana większość dotyczy infrastruktury administracyjnej, tempo wzrostu zagrożeń jasno sygnalizuje możliwość dotkliwego oddziaływania również na systemy graniczne, zwłaszcza że są one coraz bardziej cyfrowe i zintegrowane.

Wrażliwość systemów granicznych RP wynika z połączenia kilku czynników: rosnącej cyfryzacji, ekspozycji na ataki APT, słabości systemów OT oraz istnienia złożonych sojuszy hybrydowych działających w interesie obcych państw. Cyberprzestrzeń staje się areną bezpośrednich działań hybrydowych: sabotażu, dezinformacji, manewrów manipulacyjnych, co wymaga odpowiedzi strategicznej na poziomie narodowym i międzynarodowym.

Działania przeciwdziałające cyberzagrożeniom na granicy RP

W czwartej dekadzie XXI wieku Rzeczpospolita Polska realizuje kompleksową politykę cyberbezpieczeństwa ukierunkowaną również na ochronę granic państwowych. Ustawodawstwo uchwalone w 2018 roku wprowadziło ramy organizacyjne krajowego systemu cyberbezpieczeństwa, który obejmuje rozwój struktur takich jak CERT Polska (NASK), CSIRT-MON, ABW oraz Wojska Obrony Cyberprzestrzeni, odpowiedzialne za ochronę infrastruktury państwowej i militarnej

W ramach Strategii Cyberbezpieczeństwa RP na lata 2019-2024, jednym z pięciu celów strategicznych jest zwiększenie odporności systemów informacyjnych (publicznych, prywatnych i wojskowych), rozwój krajowego systemu wymiany informacji o zagrożeniach oraz podniesienie świadomości społecznej w zakresie cyberzagrożeń[13].

Centralną rolę operacyjną w detekcji i reagowaniu pełni CERT Polska – działający od 1996 r. z ramienia NASK ośrodek reagowania na incydenty komputerowe, stanowiący punkt kontaktowy dla administracji oraz współpracę z międzynarodowymi zespołami typu FIRST czy TERENA TF-CSIRT[14].

Na płaszczyźnie militarnej istotną rolę odgrywa Wojska Obrony Cyberprzestrzeni, utworzone w lutym 2022 roku jako komponent Sił Zbrojnych RP odpowiedzialny za ochronę cyfrową kraju, współpracujący z Narodowym Centrum Bezpieczeństwa Cyberprzestrzeni oraz NATO CCD COE. WOC posiada zdolności

[13] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.

[14] CERT Polska, https://cert.pl/o-nas, [dostęp: 30.07.2025].

zarówno obronne, jak i ofensywne, włączając w to wsparcie dla operacji stabilizacyjnych czy reagowania kryzysowego

Istotne znaczenie dla ochrony granic ma narodowe oraz międzynarodowe partnerstwo w dialogu o cyberbezpieczeństwie. Polska prowadzi aktywne działania w ramach współpracy z NATO, Unią Europejską, ENISA, CERT-EU oraz krajami Grupy Wyszehradzkiej i Wielkiej Brytanii. W marcu 2025 r. w Legionowie odbyła się konferencja CyberCo 2025 – spotkanie dowódców i ambasadorów cybernetycznych unijnych państw pod przewodnictwem Polski, skupione na współpracy cywilno-wojskowej i wymianie informacji o zagrożeniach mobilnych oraz nowych scenariuszach incydentów – z udziałem m.in. EDA, EUMS, EEAS i DG CNECT[15].

Rząd RP wspiera także tworzenie regionalnego Cybersecurity Platform w Europie Środkowej (CECSP), co sprzyja koordynacji i wymianie wiedzy między państwami członkowskimi[16]. Ponadto, w ramach polityki bezpieczeństwa granic wprowadzono program Tarcza Wschód (East Shield) – strategiczną inicjatywę obronną uruchomioną w 2024 roku, obejmującą modernizację infrastruktury przy granicy z Białorusią i obwodem kaliningradzkim, montaż elektronicznych systemów obserwacji (IMINT, SIGINT), środków walki elektronicznej, czujników antydronowych oraz analizę danych przy wsparciu sztucznej inteligencji — w tym szyfrowaną łączność transgraniczną i centra operacyjne[17].

W sferze edukacyjno-operacyjnej realizowane są ćwiczenia międzynarodowe, w tym symulacje incydentów i testy gotowości między państwami UE i NATO, co pozwala trenować procedury reagowania, komunikacji kryzysowej oraz interoperacyjność partnerów europejskich i wojskowych.

Działania przeciwdziałające cyberzagrożeniom na granicy RP opierają się na czterech filarach: (1) rozwój legislacji i ram organizacyjnych; (2) inwestycje w środkach technicznych – w tym Tarcza Wschód; (3) intensywna międzynarodowa współpraca i wymiana informacji; (4) szkolenia, ćwiczenia i budowanie cyberświadomości. Efektywność tych działań wymaga jednak dalszego wzmacniania mechanizmów szybkiej detekcji incydentów specyficznych dla systemów granicznych

[15] CyberCo25: Enhancing Civil-Military Cooperation, https://polish-presidency.consilium.europa.eu/en/news/cyberco25-enhancing-civil-military-cooperation, [dostęp: 30.07.2025].

[16] Wzmacnianie Europejskiego Systemu Odporności Cybernetycznej oraz Wspieranie Konkurencyjnego i Innowacyjnego Sektora Bezpieczeństwa Cybernetycznego – Cyberpolicy NASK, https://cyberpolicy.nask.pl/wzmacnianie-europejskiego-systemu-odpornosci-cybernetycznej-oraz-wspieranie-konkurencyjnego-i-innowacyjnego-sektora-bezpieczenstwa-cybernetycznego, [dostęp: 30.07.2025]

[17] L. Elak, M. Oskierko, S. Żurawski, *Ochrona granicy polsko-białoruskiej w obliczu wojny hybrydowej*, De Securitate et Defensione. O Bezpieczeństwie i Obronności, nr 1, 2024, s. 91.

(kamery CCTV, systemy SIS II, OT kontrolujące ruch graniczny), oraz praktycznego przetestowania procedur w warunkach ataków typu APT czy dezinformacji. Przyszłe badania powinny koncentrować się na ocenie skuteczności tych mechanizmów oraz możliwości przeciwdziałania hybrydowym kampaniom wymierzonym w granice RP.

Podsumowanie

W dobie intensywnej cyfryzacji funkcjonowania państwa oraz narastającej złożoności zagrożeń hybrydowych, bezpieczeństwo granic przestaje być wyłącznie kwestią fizycznej obecności sił porządkowych i infrastruktury technicznej. Coraz większe znaczenie mają aspekty związane z odpornością cyfrową systemów wykorzystywanych do nadzoru, kontroli i wymiany informacji transgranicznej. Jak wynika z przeprowadzonej analizy, cyberzagrożenia mogą prowadzić do głębokiego zakłócenia procedur granicznych, paraliżu administracji, manipulacji ruchem migracyjnym oraz rozprzestrzeniania dezinformacji mającej na celu destabilizację społeczną i polityczną.

Charakterystyka cyberzagrożeń wskazuje na ich różnorodność i dynamiczną ewolucję – od działań przestępczych po operacje prowadzone przez podmioty państwowe, wykorzystujące wyrafinowane techniki APT i inżynierii społecznej. Zidentyfikowane słabości w systemach informacyjnych i organizacyjnych służb granicznych Rzeczypospolitej Polskiej stanowią potencjalne punkty podatne na atak, zwłaszcza w kontekście rosnącej roli technologii cyfrowych w zarządzaniu ruchem granicznym. Szczególnym zagrożeniem pozostają zorganizowane działania hybrydowe, które łączą sabotaż fizyczny, operacje cybernetyczne oraz manipulację narracją medialną.

W odpowiedzi na te wyzwania państwo polskie podejmuje szereg działań, mających na celu zwiększenie odporności systemowej. Obejmują one rozwój struktur strategicznych i operacyjnych w ramach krajowego systemu cyberbezpieczeństwa, inwestycje w technologie monitoringu i analizy danych, a także rozbudowę współpracy międzynarodowej z partnerami z Unii Europejskiej i NATO. Szczególne znaczenie mają programy takie jak Tarcza Wschód oraz zaangażowanie Polski w regionalne i transnarodowe mechanizmy wymiany informacji i koordynacji reagowania na incydenty cybernetyczne.

Zapewnienie bezpieczeństwa granicy państwowej w XXI wieku wymaga zintegrowanego podejścia, które łączy działania fizyczne z zaawansowaną ochroną w cyberprzestrzeni. Niezbędne jest nie tylko utrzymywanie wysokiego poziomu

gotowości operacyjnej, lecz również ciągłe doskonalenie zdolności analitycznych, detekcyjnych i reagowania na zagrożenia cyfrowe. Rozdział potwierdza konieczność traktowania cyberbezpieczeństwa jako integralnej części polityki granicznej i narodowej strategii bezpieczeństwa.

Literatura

1. CERT Polska, https://cert.pl/o-nas, [dostęp: 30.07.2025].
2. CyberCo25: Enhancing Civil-Military Cooperation, https://polish-presidency.consilium.europa.eu/en/news/cyberco25-enhancing-civil-military-cooperation, [dostęp: 30.07.2025].
3. Elak L., Oskierko M., Żurawski S., *Ochrona granicy polsko-białoruskiej w obliczu wojny hybrydowej*, De Securitate et Defensione. O Bezpieczeństwie i Obronności, nr 1, 2024.
4. Girod R., *Border Security: Vulnerability and Emerging Global Security Threats*, Global Security and Intelligence Studies, Volume 8, Number 1, 2023.
5. Kamiński M., Śliwa Z., *Poland's Threat Assessment Deepened, Not Changed*, PRISM 10, no. 2, 2023.
6. Makrakis G. M., Kolias C., Kambourakis G., Rieger C., Benjamin J., *Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures*, https://arxiv.org/abs/2109.03945, [dostęp: 30.07.2025].
7. Marczyk M., Błachut M., *Information security as part of Poland's security*, Scientific Journal of the Military University of Land Forces, Volume 54, Number 4(206), 2022.
8. Poland 'most attacked' online by Russia, says minister, https://www.ft.com/content/e0e1a016-e4e0-4628-a0ac-c4a6e9d15db6.
9. Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 roku.
10. Russia accused of trying to hack border security cameras to disrupt Ukraine aid, The Guardian, https://www.theguardian.com/world/2025/may/21/russia-accused-trying-disrupt-aid-ukraine-hacking-border-crossings, [dostęp: 30.07.2025].
11. Russia using criminal networks to drive increase in sabotage acts, says Europol Cybercrime, The Guardian, https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol, [dostęp: 30.07.2025].
12. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.
13. Świerczyńska J., *The importance of border surveillance and border traffic control at the eastern border of the Republic of Poland to the cross-border security of the European Union*, Central European Review of Economics & Finance, 44(3), 2023.
14. Terlecka-Maciejewska M., *Cybersecurity in polish security system*, Scientific Papers of Silesian University of Technology, Organization and Management, no. 198, 2024.
15. The Cheap Radio Hack That Disrupted Poland's Railway System, WIRED, https://www.wired.com/story/poland-train-radio-stop-attack/, [dostęp: 30.07.2025].

16. Wzmacnianie Europejskiego Systemu Odporności Cybernetycznej oraz Wspieranie Konkurencyjnego i Innowacyjnego Sektora Bezpieczeństwa Cybernetycznego – Cyberpolicy NASK, https://cyberpolicy.nask.pl/wzmacnianie-europejskiego-systemu-odpornosci-cybernetycznej-oraz-wspieranie-konkurencyjnego-i-innowacyjnego-sektora-bezpieczenstwa-cybernetycznego, [dostęp: 30.07.2025].