Marta Chodyka[1]
Akademia Bialska im. Jana Pawła II, Biała Podlaska

https://doi.org/10.29316/9788368103373_7

CYBERODPORNOŚĆ SYSTEMÓW GRANICZNYCH

CYBER RESILIENCE OF BORDER SYSTEMS

Streszczenie

Celem rozdziału jest opracowanie i uzasadnienie referencyjnego modelu cyberodporności systemów granicznych (BORDER-CyRes), który integruje działania w obszarze prewencji, detekcji, reagowania i odtwarzania w wymiarze technicznym, organizacyjnym i proceduralnym. Problem badawczy sformułowano: w jaki sposób projektować i operacjonalizować cyberodporność systemów teleinformatycznych wspierających ochronę granic, aby zapewnić jednocześnie ciągłość odprawy, bezpieczeństwo informacji oraz skuteczną koordynację działań międzyinstytucjonalnych w warunkach rosnących zagrożeń cybernetycznych? Przyjęto hipotezę, że zastosowanie zintegrowanego modelu cyberodporności opartego na podejściu warstwowym, łączącego rozwiązania techniczne, organizacyjne i proceduralne oraz uwzględniającego wymagania regulacyjne i realne profile zagrożeń, umożliwia zwiększenie zdolności systemów granicznych do utrzymania funkcji krytycznych i szybkiego odtworzenia działania po incydencie. W badaniach zastosowano metody badawcze, w tym analizę normatywną aktów prawnych i standardów, analizę danych wtórnych i raportów dotyczących zagrożeń cybernetycznych oraz walidację

[1] https://orcid.org/0000-0002-8819-2451, e-mail: m.chodyka@dyd.akademiabialska.pl

scenariuszową modelu w odniesieniu do wybranych typów incydentów, takich jak ataki DDoS, ransomware oraz incydenty łańcucha dostaw. Uzyskane wyniki wskazują, że zaproponowany model cyberodporności umożliwia systematyczne projektowanie architektury bezpieczeństwa, usprawnienie procesów reagowania na incydenty oraz lepsze dopasowanie mechanizmów ochrony do specyfiki środowiska granicznego, co może wspierać zarówno praktykę operacyjną instytucji granicznych, jak i dalsze badania nad bezpieczeństwem infrastruktury krytycznej.

Słowa kluczowe: cyberodporność, ochrona granic, EES, interoperacyjność, SOC, CSIRT, NIS2, Zero Trust, reagowanie na incydenty

Abstract

The aim of the chapter is to develop and justify a reference model of cyber resilience for border systems (BORDER-CyRes), which integrates activities in the areas of prevention, detection, response, and recovery across the technical, organisational, and procedural dimensions. The research problem was formulated as follows: how to design and operationalise the cyber resilience of ICT systems supporting border protection to ensure the continuity of check-in, information security, and effective coordination of interinstitutional activities in the face of growing cyber threats? It was hypothesised that the use of an integrated cyber resilience model based on a layered approach, combining technical, organisational, and procedural solutions, and accounting for regulatory requirements and real-world threat profiles, enables border systems to maintain critical functions and quickly recover from incidents. The research used methods including normative analysis of legal acts and standards, analysis of secondary data and reports on cyber threats, and scenario validation of the model for selected incident types, such as DDoS attacks, ransomware, and supply chain incidents. The results indicate that the proposed cyber resilience model enables the systematic design of security architecture, the improvement of incident response processes, and the better adaptation of protection mechanisms to the specifics of the border environment, thereby supporting both the operational practice of border institutions and further research on the security of critical infrastructure.

Keywords: cyber resilience, border management, EES, interoperability, SOC, CSIRT, NIS2, Zero Trust, incident response

Wstęp

Cyfrowa transformacja zarządzania granicami zewnętrznymi UE materializuje się m.in. poprzez wdrażanie Systemu Wjazdu/Wyjazdu (EES) jako elementu „Smart Borders", zastępującego tradycyjne stemplowanie paszportów elektronicznymi zapisami oraz wykorzystującego dane biometryczne

w procesie kontroli. Równolegle rośnie rola systemów zarządzanych przez eu-LISA oraz komponentów interoperacyjności, które – łącząc wcześniej rozdzielone bazy – wzmacniają zdolność wykrywania oszustw tożsamości i zagrożeń bezpieczeństwa, ale jednocześnie zwiększają złożoność architektury oraz „promień rażenia" incydentów cybernetycznych. W praktyce oznacza to, że cyberincydent nie jest już problemem pojedynczej aplikacji „na granicy", lecz może obejmować: urządzenia i sensory w terenie (w tym OT), łączność i lokalne zasoby punktu odpraw, systemy krajowe i międzyresortowe, zależności usługowe i prawne wobec komponentów UE, partnerów (dostawcy urządzeń biometrycznych, integratorzy, operatorzy telekomunikacyjni, podmioty portowe i lotniskowe).

Problem badawczy niniejszego opracowania koncentruje się na tym, w jaki sposób projektować i operacjonalizować cyberodporność systemów teleinformatycznych wspierających ochronę oraz zarządzanie granicami, tak aby przy wysokiej presji czasowej i rygorystycznych wymogach dostępności usług (w szczególności w procesach odprawy) zapewnić jednocześnie bezpieczeństwo informacji, w tym ochronę danych biometrycznych, ciągłość świadczenia usług, interoperacyjność rozwiązań oraz skoordynowane reagowanie pomiędzy instytucjami, przy zachowaniu obowiązków raportowania i wymogów zarządzania kryzysowego. W tym kontekście rozdział odpowiada na trzy komplementarne pytania badawcze: po pierwsze, jakie mechanizmy techniczne i organizacyjne są krytyczne dla cyberodporności „systemu systemów" granicy w ujęciu cyklu prewencja–detekcja–reakcja–odtwarzanie, po drugie, w jaki sposób integrować workflow reagowania na incydenty w środowisku międzyinstytucjonalnym z wymaganiami raportowania oraz koordynacji na poziomie krajowym i unijnym, w tym z logiką ścieżki „24-72-30 dni", po trzecie, jakie mierniki oraz kryteria priorytetyzacji umożliwiają przełożenie danych o krajobrazie zagrożeń (m.in. kampanii DDoS, naruszeń danych, incydentów ransomware) na decyzje architektoniczne i operacyjne właściwe dla środowiska granicznego.

Celem badawczym jest opracowanie referencyjnego modelu cyberodporności systemów granicznych (BORDER-CyRes) oraz jego walidacja w oparciu o dane sektorowe i ponadsektorowe, a także scenariusze incydentów, prowadzące do sformułowania rekomendacji wdrożeniowych adresowanych do instytucji granicznych oraz ekosystemu podmiotów

współpracujących. Podjęcie tematu uzasadniają dane wskazujące na wysoką presję zagrożeń w administracji publicznej w UE: raporty ENISA konsekwentnie klasyfikują sektor publiczny jako jeden z najczęściej atakowanych, przy dominacji incydentów wpływających na dostępność (w szczególności kampanii DDoS) oraz istotnym udziale naruszeń danych. Ponieważ funkcje graniczne należą do obszarów o wysokiej krytyczności dla państwa, podatność ta ma wymiar nie tylko informacyjny, lecz także operacyjny, społeczny i polityczny – zakłócenia odpraw mogą prowadzić do powstawania kolejek i przerw w świadczeniu usług, generować konsekwencje reputacyjne, a także eskalować koszty i ryzyka wtórne, co wzmacnia potrzebę podejścia systemowego do cyberodporności w ujęciu międzyinstytucjonalnym.

Przegląd literatury

W literaturze inżynierii systemów pojęcie „systemu systemów" odnosi się do konfiguracji, w której spójne zdolności operacyjne powstają wskutek współdziałania wielu względnie autonomicznych systemów składowych, zarządzanych i rozwijanych niezależnie, a jednak powiązanych wspólną misją i zależnościami informacyjnymi oraz usługowymi. W tym ujęciu infrastruktura ICT granicy ma strukturę z natury rozproszoną i wielowarstwową: obejmuje warstwę brzegową (sensory oraz urządzenia rejestrujące i weryfikacyjne), warstwę lokalnej infrastruktury punktu granicznego (sieci, stanowiska odpraw, serwisy wspólne), warstwę centralnych systemów krajowych, a w warunkach europejskich również integrację z wielkoskalowymi systemami informacyjnymi oraz komponentami interoperacyjności (Wojciechowska-Filipek, Ciekanowski, 2019; Parlament Europejski i Rada UE, 2019). Taka topologia powoduje, że ryzyko cybernetyczne nie jest własnością pojedynczej aplikacji „na granicy", lecz ma charakter end-to-end: awaria lub kompromitacja jednego elementu może propagować się przez zależności transakcyjne, tożsamościowe i sieciowe, oddziałując na ciągłość odprawy i skuteczność realizacji zadań państwa (ENISA, 2024).

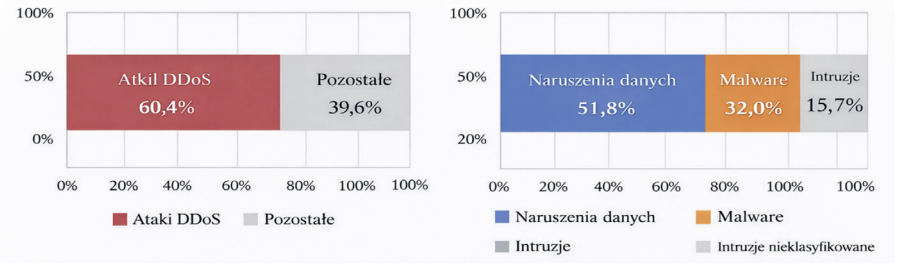
Istotnym tłem systemowym jest europejskie zintegrowane zarządzanie granicami, rozwijane m.in. w ramach mandatu Frontex, który wzmacnia wymiar współdziałania operacyjnego i informacyjnego pomiędzy podmiotami krajowymi oraz poziomem unijnym (Ciekanowski i in., 2022; Parlament Europejski i Rada UE, 2019). Równolegle eu-LISA pełni rolę agencji

odpowiedzialnej za operacyjne zarządzanie wybranymi wielkoskalowymi systemami IT w obszarze wolności, bezpieczeństwa i sprawiedliwości, co sprzyja odchodzeniu od modelu „silosowego" na rzecz ekosystemu integrującego systemy tożsamościowe i migracyjne w skali UE (Parlament Europejski i Rada UE, 2018c, Parlament Europejski i Rada UE, 2019b). W rezultacie interoperacyjność staje się nie tylko zagadnieniem integracji technicznej, lecz także trwałą własnością architektoniczną, która musi łączyć wymagania dostępności i wydajności operacyjnej z reżimami ochrony danych, kontroli dostępu oraz audytowalności działań (Parlament Europejski i Rada UE, 2019; ENISA, 2024). W tym sensie cyberodporność w środowisku granicznym powinna być projektowana jako zdolność ekosystemu do utrzymania kluczowych funkcji pomimo incydentów oraz do kontrolowanego odtwarzania i adaptacji, przy jednoczesnym zachowaniu spójności międzyinstytucjonalnej (ENISA, 2024). Dodatkową cechą infrastruktury granicznej jest współobecność komponentów klasy IT oraz OT (np. bramki i systemy kontroli dostępu, urządzenia peryferyjne, nadzoru wideo, a niekiedy także elementy łączności kryzysowej), co wymusza równoległe uwzględnienie odmiennych reżimów utrzymaniowych i modeli ryzyka (Ciekanowski, 2020; NIST, 2024). Z perspektywy praktyk bezpieczeństwa oznacza to konieczność łączenia mechanizmów typowych dla IT (np. zarządzanie tożsamością i dostępem, centralizacja i korelacja logów, detekcja i reakcja na stacjach roboczych) z wymaganiami charakterystycznymi dla OT, takimi jak twarde utwardzanie konfiguracji, dopuszczanie oprogramowania oparte o listy dozwolone, restrykcyjna kontrola łączności oraz podejście do aktualizacji uwzględniające krytyczność ciągłości działania (NIST, 2024, ENISA, 2024). W literaturze i zaleceniach podkreśla się przy tym, że w środowiskach, gdzie OT pełni funkcje krytyczne, priorytetem bywa bezpieczeństwo operacyjne i przewidywalność pracy systemu, co wymaga starannego projektowania segmentacji, izolacji domen oraz procedur reagowania tak, aby nie doprowadzić do niekontrolowanej degradacji procesów kluczowych (NIST, 2024).

Wdrażanie unijnego Systemu Wjazdu/Wyjazdu (EES) ma wymierny charakter operacyjny, ponieważ wiąże się z przejściem od tradycyjnych praktyk rejestracji do elektronicznego zapisu zdarzeń granicznych oraz wykorzystania danych biometrycznych w procesie kontroli (Parlament Europejski i Rada UE, 2017). W polskich realiach Straż Graniczna komunikuje

etapowe uruchamianie rozwiązań oraz stopniowe gromadzenie danych biometrycznych (wizerunek twarzy i odciski palców) w okresie przejściowym, co dodatkowo wzmacnia presję na dostępność usług w czasie odprawy (Straż Graniczna, 2025). Konsekwencje dla cyberodporności są wprost dwutorowe: po pierwsze, rośnie znaczenie zdolności do utrzymania ciągłości odprawy przy zakłóceniach i ograniczeniach przepustowości, a po drugie, wzmacnia się waga ochrony danych wrażliwych, w tym danych biometrycznych, których przetwarzanie w czasie rzeczywistym zwiększa wymagania dotyczące integralności, poufności oraz rozliczalności operacji (Parlament Europejski i Rada UE, 2017; ENISA, 2024; Straż Graniczna, 2025).

Dane sektorowe dla administracji publicznej UE – istotne także dla funkcji granicznych realizowanych przez podmioty publiczne – wskazują na dominację incydentów uderzających w dostępność usług. Analiza ENISA dla sektora administracji publicznej identyfikuje 586 publicznie raportowanych incydentów w okresie styczeń-grudzień 2024 i pokazuje, że ataki DDoS stanowią ponad 60% zdarzeń, co silnie akcentuje potrzebę odporności na zakłócenia dostępności usług (ENISA, 2026). W tej samej analizie, w grupie incydentów związanych z „intrusion-related" skutkami udanych włamań, największy udział mają naruszenia danych (51,8%), a następnie malware (~32%) oraz intruzje nieklasyfikowane (15,7%), co wzmacnia wniosek, że cyberodporność granicy nie może być redukowana do ochrony perymetrycznej, lecz wymaga dojrzałego zarządzania tożsamością, ciągłego monitoringu zdarzeń, detekcji nadużyć oraz zdolności odzyskiwania po naruszeniu – zwłaszcza przy przetwarzaniu danych wrażliwych (ENISA, 2026; NIST, 2024). Szersze ujęcie krajobrazu zagrożeń – obejmujące okres od około połowy 2023 do połowy 2024 – potwierdza utrzymywanie się priorytetów takich jak zagrożenia dla dostępności i ransomware oraz wskazuje na rolę czynników geopolitycznych i wzrost aktywności aktorów ukierunkowanych na efekt widoczności i zakłóceń (ENISA, 2024). Jest to spójne z tezą, że infrastruktury publiczne stanowią atrakcyjny cel zarówno dla hacktywizmu nastawionego na zakłócanie usług, jak i dla cyberprzestępczości (w tym ransomware) oraz podmiotów o charakterze państwowym, realizujących cele szpiegowskie (cyberespionage) (ENISA, 2024; Verizon, 2025). Incydenty przedstawione zostały na Rysunku 1.



a) b)

Rysunek 1. Incydenty cybernetyczne w sektorze administracji publicznej UE, styczeń – grudzień 2024, N = 586 z podziałem na a) incydenty na dostępność usług, b) incydenty „intrusion-related"

Źródło: opracowanie własne na podstawie ENISA, 2026.

Perspektywa ponadsektorowa dodatkowo wzmacnia znaczenie czynników organizacyjnych i łańcucha dostaw. W podsumowaniu raportu Verizon DBIR 2025 wskazano stabilny udział „czynnika ludzkiego" na poziomie około 60%, wzrost udziału naruszeń angażujących strony trzecie z 15% do 30% oraz wzrost udziału naruszeń o motywacji szpiegowskiej do 17% (Verizon, 2025). W kontekście systemów granicznych ma to szczególne znaczenie, ponieważ ekosystem techniczny granicy jest silnie zależny od dostawców urządzeń (w tym urządzeń biometrycznych), integratorów oraz operatorów usług infrastrukturalnych (łączność, serwis, oprogramowanie), a zatem ryzyko cybernetyczne ma w dużej mierze charakter współdzielony i łańcuchowy (Chodyka i in., 2025; Verizon, 2025; ENISA, 2024). Jednocześnie metryki czasu wykrycia (dwell time) wskazują, że w incydentach ransomware „okno czasowe" na przerwanie łańcucha zdarzeń może być operacyjnie krótkie, a wykrycie wewnętrzne potrafi być istotnie opóźnione, co podnosi wymagania wobec automatyzacji detekcji, segmentacji środowiska oraz gotowości do odtwarzania (Mandiant, 2025). W konsekwencji, wyniki analiz sektorowych i ponadsektorowych prowadzą do spójnego wniosku projektowego: cyberodporność systemów granicznych powinna w równym stopniu obejmować inżynierię dostępności (w tym odporność na przeciążenia i degradację), zarządzanie tożsamością i dostępem, obserwowalność zdarzeń oraz zdolności odtworzeniowe, jak i mechanizmy organizacyjne związane z zarządzaniem dostawcami, koordynacją międzyinstytucjonalną oraz gotowością proceduralną do działania pod presją czasu (ENISA, 2026; Verizon, 2025; Mandiant, 2025).

Metodologia

Badanie zrealizowano w paradygmacie design science research (DSR), ukierunkowanym na zaprojektowanie i ocenę artefaktu rozwiązującego problem praktyczno-inżynierski. Artefaktem jest referencyjny model cyberodporności systemów granicznych BORDER-CyRes, ujmowany jako spójny zestaw: konstruktów (role i zdolności), relacji (zależności warstw „systemu systemów"), mechanizmów technicznych i organizacyjnych oraz procedur operacyjnych (m.in. workflow reagowania i odtwarzania). Przyjęto iteracyjną logikę DSR (wymagania, projekt, walidacja) oraz triangulację przesłanek, aby model równoważył wymagania zgodności i interoperacyjności z realnym profilem zagrożeń i ograniczeniami wdrożeniowymi środowiska granicznego.

Przeprowadzono analizę normatywno-regulacyjną, wyprowadzając wymagania dla cyberodporności z obowiązków zarządzania ryzykiem i raportowania incydentów w logice 24-72-30 (Parlament Europejski i Rada UE, 2022) oraz z implementacyjnych wskazówek dot. środków zarządzania ryzykiem (ENISA, 2026). NIS2 przewiduje: early warning ≤24 h, incident notification ≤72 h, raport pośredni na żądanie CSIRT/organu oraz raport końcowy nie później niż 1 miesiąc po notyfikacji (plus szczególny reżim dla incydentów trwających). Równolegle uwzględniono ramy instytucjonalne i architektoniczne zarządzania granicami oraz interoperacyjności (w tym Frontex i eu-LISA) (Parlament Europejski i Rada UE, 2018a; Parlament Europejski i Rada UE, 2019), a także wymagania wynikające z EES w zakresie przetwarzania danych identyfikacyjnych i biometrycznych (Parlament Europejski i Rada UE, 2017) oraz krajowe uwarunkowania etapowego wdrożenia EES (Straż Graniczna, 2025). Rezultatem tego strumienia był zestaw wymagań zgodności obejmujący m.in. raportowanie, interoperacyjność, ochrona danych biometrycznych oraz ciągłość odprawy jako usługi krytycznej. Następnie wykonano syntetyczny przegląd ram praktyk, traktując cyberodporność jako cykl prewencji–detekcji–reakcji–odtwarzania. Do porządkowania rezultatów i mapowania zdolności użyto NIST CSF 2.0 (z uwzględnieniem specyfiki IT/OT), a do projektowania pokrycia detekcyjnego i reakcyjnego – taksonomii MITRE ATT&CK oraz zasad architektonicznych Zero Trust (NIST, 2024; MITRE, 2025; Rose i in., 2020). Priorytety modelu

skalibrowano następnie na podstawie danych wtórnych i metryk operacyjnych, zestawiając wnioski z raportów ENISA (w tym sektorowych dla administracji publicznej oraz horyzontalnych TL) (ENISA, 2024; ENISA, 2026) z danymi ponadsektorowymi (Verizon, 2025) oraz metrykami czasu wykrycia i dynamiki ransomware (Mandiant, 2025). W kolejnym kroku artefakt zwalidowano scenariuszowo (DDoS, ransomware, łańcuch dostaw), stosując BORDER-CyRes jako „szablon decyzyjny" i oceniając go kryteriami: RTO/RPO, MTTD/MTTR, zgodność z raportowaniem 24-72-30, minimalizacja ryzyka naruszeń danych (zwłaszcza biometrycznych) oraz wykonalność w rozproszonym środowisku IT/OT (Parlament Europejski i Rada UE, 2017; Parlament Europejski i Rada UE, 2022; NIST, 2024). Ograniczenia wynikają z charakteru danych wtórnych i zależności od praktyk raportowania (ENISA, 2024; ENISA, 2026). Zasady etyczne i ochrony danych zapewniono przez wykorzystanie informacji publicznych i zagregowanych oraz projektowanie scenariuszy bez przetwarzania rzeczywistych danych osobowych, w tym biometrycznych (Parlament Europejski i Rada UE, 2017; Straż Graniczna, 2025).

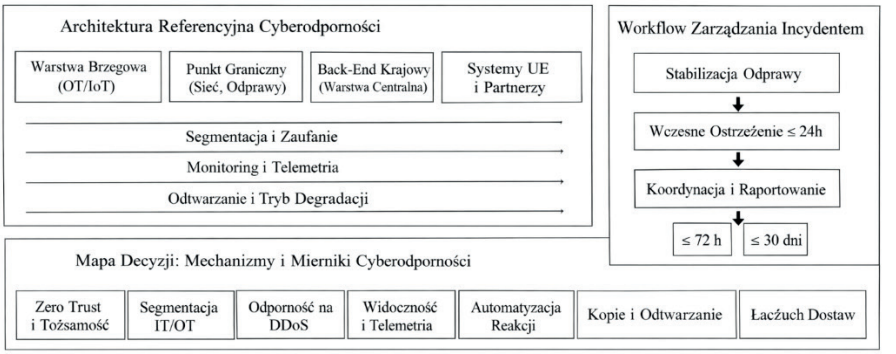
Wyniki

Wyniki prac projektowych w paradygmacie design science research materializują się w trzech komplementarnych artefaktach:

- architekturze referencyjnej cyberodporności,
- operacyjnym workflow zarządzania incydentem z mapowaniem na obowiązki raportowe oraz koordynację krajową i unijną,
- wdrożeniowej „mapie decyzji" w postaci zestawu mechanizmów wraz z miernikami i odniesieniami do ram referencyjnych.

Z perspektywy walidacji użyteczności, artefakty te zostały osadzone w realiach środowiska granicznego „systemu systemów" oraz zilustrowane na przykładzie drogowego przejścia granicznego Terespol–Brześć jako reprezentatywnego punktu odprawy ruchu osobowego, w którym priorytetem operacyjnym jest utrzymanie ciągłości odprawy przy jednoczesnej ochronie danych wrażliwych, w tym danych identyfikacyjnych i biometrycznych przetwarzanych w ramach EES (Elak i in., 2024; Parlament Europejski i Rada UE, 2017; Straż Graniczna, 2025).

W celu syntetycznego przedstawienia zależności pomiędzy trzema artefaktami modelu BORDER-CyRes – architekturą referencyjną, workflow reagowania na incydent oraz mapą decyzji wdrożeniowych – opracowano zintegrowany schemat koncepcyjny. Rysunek 2 przedstawia relacje pomiędzy warstwami techniczną, operacyjną oraz decyzyjno-wdrożeniową w ujęciu całościowym, ilustrując sposób przejścia od struktury systemu granicznego do mechanizmów reakcji oraz do zestawu mechanizmów i mierników implementacyjnych.



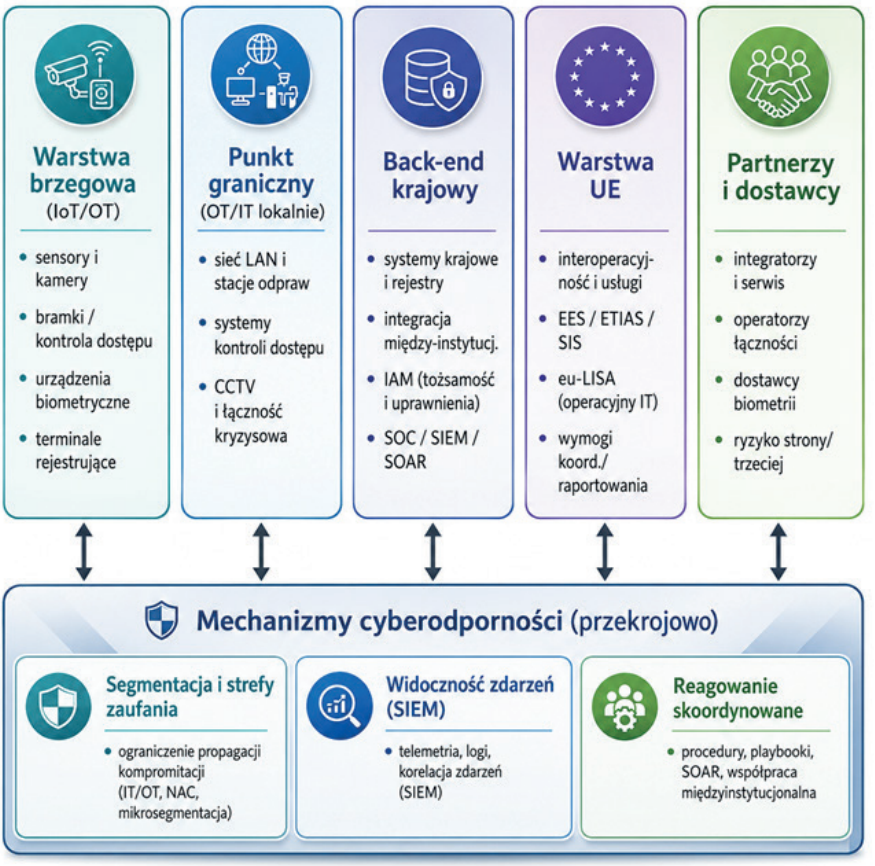
Rysunek 2. Relacje pomiędzy warstwą techniczną, operacyjną oraz decyzyjno-wdrożeniową

Źródło: opracowanie własne.

W części górnej przedstawiono architekturę referencyjną jako układ warstw: warstwę brzegową (OT/IoT), punkt graniczny (infrastruktura lokalna), warstwę centralną (back-end krajowy) oraz integrację z systemami UE i partnerami. W części środkowej zobrazowano workflow reagowania w logice „podwójnego rytmu", łączącej stabilizację operacyjną odprawy z równoległym uruchomieniem ścieżki raportowej 24-72-30. Część dolna przedstawia mapę decyzji – zestaw mechanizmów technicznych i organizacyjnych, które przekładają wnioski analityczne na działania wdrożeniowe. Takie trójwarstwowe ujęcie pozwala interpretować cyberodporność nie jako zbiór izolowanych zabezpieczeń, lecz jako powiązany system zależności pomiędzy architekturą, operacjami oraz governance. W instancji dla drogowego przejścia granicznego Terespol–Brześć oznacza to, że decyzje architektoniczne (np. segmentacja IT/OT) są bezpośrednio sprzężone z procedurami reagowania (np. izolacja segmentu w czasie ≤24 h) oraz z obowiązkami raportowymi

i koordynacyjnymi. W dalszej części rozdziału przedstawiono kolejno: architekturę referencyjną jako wynik pierwszy, workflow zarządzania incydentem jako wynik drugi oraz mapę decyzji i mechanizmy wdrożeniowe jako wynik trzeci.

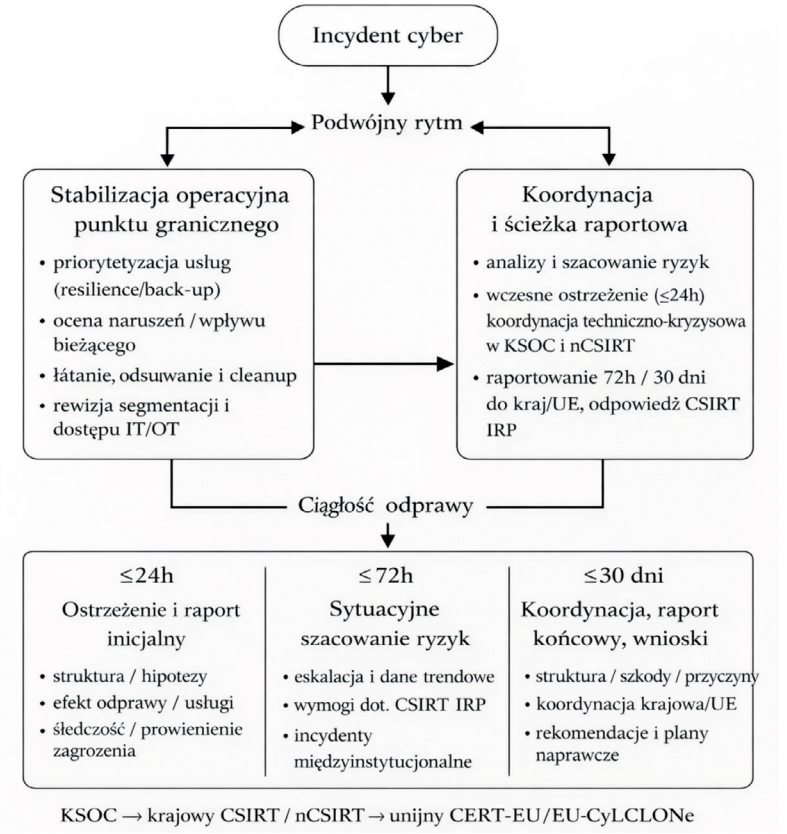
Pierwszym wynikiem jest architektura referencyjna, która traktuje granicę jako rozproszony ekosystem „end-to-end": od urządzeń i komponentów brzegowych (w tym OT/IoT), przez lokalną infrastrukturę punktu granicznego (sieć, stanowiska odpraw, usługi wspólne), po warstwę back-endu krajowego (tożsamość, monitoring, odtwarzanie), interoperacyjność i wielkoskalowe systemy UE oraz zależności partnerów i dostawców. Logika tej architektury została przedstawiona na Rysunku 3.



Rysunek 3. Ekosystem teleinformatyczny ochrony granic

Źródło: opracowanie własne.

Jej kluczowym założeniem jest projektowanie cyberodporności nie jako zbioru izolowanych kontroli, lecz jako własności systemu zdolnego do utrzymania funkcji krytycznych mimo incydentu oraz do kontrolowanego odtworzenia po zakłóceniu (NIST, 2024; NIST, 2021). W instancji dla drogowego przejścia granicznego Terespol–Brześć oznacza to, że krytyczne punkty kontrolne cyberodporności nie są skoncentrowane wyłącznie „w centrali", lecz rozkładają się wzdłuż całego łańcucha odprawy: od warstwy brzegowej (urządzenia weryfikacyjne i rejestracyjne, urządzenia wspierające kontrolę), przez segmentację i kontrolę dostępu w sieci lokalnej, po centralne zdolności IAM oraz SOC/SIEM/SOAR i mechanizmy odtwarzania. Szczególny nacisk położono na ograniczanie propagacji kompromitacji poprzez segmentację i strefy zaufania, zwiększanie obserwowalności poprzez telemetrię, logi i korelację, a także na zdolność do odtworzenia i pracy w trybie degradacji, co jest spójne z priorytetyzacją dostępności i ciągłości działania w środowiskach krytycznych (NIST, 2024, ENISA, 2024). Wymiar „end-to-end" obejmuje również zależności zewnętrzne: model zakłada, że ryzyko w punkcie granicznym jest współdzielone z dostawcami technologii, serwisu i łączności, a zatem musi być zarządzane w sposób systemowy (Verizon, 2025, ENISA, 2024). Uzasadnieniem tej części architektury są dane DBIR wskazujące na wzrost udziału naruszeń angażujących strony trzecie (z 15% do 30%), co przekłada się na konieczność formalizacji wymagań bezpieczeństwa wobec dostawców i kontroli kanałów serwisowych w środowiskach granicznych (Verizon, 2025). Drugim wynikiem jest workflow reagowania na incydent, który integruje logikę operacyjną odprawy z obowiązkami raportowania i koordynacji. Mechanizm ten został przedstawiony na Rysunku 4 i opiera się na założeniu „podwójnego rytmu" działań.

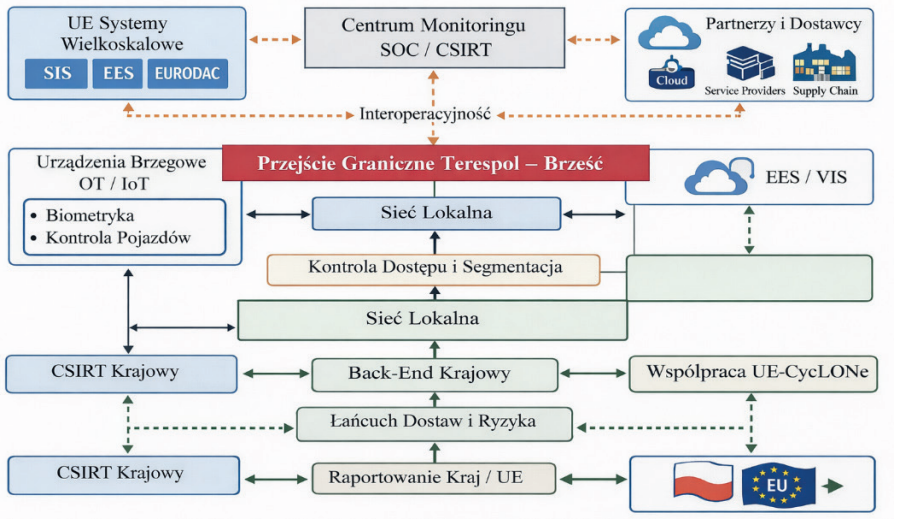


Rysunek 4. Mechanizm zarządzania incydentami cyber

Źródło: opracowanie własne.

Pierwszy rytm to natychmiastowa stabilizacja usług w punkcie granicznym, rozumiana jako utrzymanie ciągłości odprawy poprzez priorytetyzację usług, ograniczanie skutków, izolację segmentów oraz działania typu cleanup i przywracanie stanu operacyjnego. Drugi rytm to równoległe budowanie obrazu sytuacji oraz uruchomienie ścieżki eskalacyjno-raportowej w logice 24-72-30 dni, wymaganej przez NIS2 (Parlament Europejski i Rada UE, 2022). W konsekwencji etap „wczesne ostrzeżenie ≤24h" nie jest w modelu traktowany jako czynność następcza wobec działań technicznych, lecz jako proces uruchamiany równolegle, ponieważ w środowisku granicznym szybka eskalacja ma bezpośredni wpływ na zdolność do utrzymania odprawy oraz na ograniczenie ryzyka wtórnego. Dla drogowego przejścia granicznego Terespol–Brześć oznacza to, że decyzje o przejściu w tryb degradacji,

uruchomieniu łączy zapasowych, wdrożeniu reguł mitigacji DDoS czy izolacji segmentu nie są wyłącznie decyzjami lokalnymi. Wymagają one wczesnej koordynacji z właściwymi strukturami krajowymi (w tym SOC/CSIRT) oraz – w razie potrzeby – kanałami współpracy na poziomie UE, aby zapewnić spójność reakcji w ekosystemie interoperacyjnym (Parlament Europejski i Rada UE, 2022; ENISA, 2024; ENISA, 2026). Takie ujęcie jest szczególnie istotne w warunkach nadreprezentacji incydentów wpływających na dostępność (zwłaszcza DDoS) w sektorze administracji publicznej w UE, gdzie opóźnienie eskalacji może bezpośrednio przełożyć się na długotrwałe zakłócenie usług granicznych i utratę kontroli nad dynamiką incydentu (ENISA, 2024; ENISA, 2026). Logika workflow jest zgodna z podejściem do obsługi incydentów jako procesu obejmującego równolegle identyfikację, ograniczanie, usuwanie skutków i odtwarzanie, uzupełnionego o wymagania raportowe oraz zarządzanie informacją o incydencie (Nelson i in., 2025; Parlament Europejski i Rada UE, 2022). Trzecim wynikiem jest zestawienie danych i przesłanek, które uzasadniają priorytety mechanizmów cyberodporności, a następnie ich syntetyzacja w formie wdrożeniowej mapy decyzji. Mapa ekosystemu teleinformatycznego ochrony granic Terespol–Brześć przedstawiona została na Rysunku 5.



Rysunek 5. Ekosystem teleinformatyczny ochrony granic Terespol–Brześć

Źródło: opracowanie własne.

Dane sektorowe ENISA dla administracji publicznej UE wskazują dominację incydentów wpływających na dostępność (DDoS > 60% zdarzeń w analizowanym zbiorze), co wspiera priorytet inżynierii dostępności i odporności sieci, w tym zdolności do kontrolowanej degradacji usług (ENISA, 2026). Jednocześnie w grupie incydentów intrusion-related największy udział stanowią naruszenia danych (51,8%), co wzmacnia potrzebę wzmocnienia zarządzania tożsamością i dostępem oraz monitoringu i korelacji zdarzeń (ENISA, 2026; NIST, 2024). Wreszcie metryki czasu wykrycia i charakterystyka incydentów ransomware (dwell time) wskazują, że brak wykrycia wewnętrznego może oznaczać długotrwałą obecność intruza, co zwiększa ryzyko współwystąpienia zakłóceń operacyjnych i naruszeń danych, a tym samym uzasadnia nacisk na automatyzację reakcji, segmentację oraz gotowość odtworzeniową (Mandiant, 2025). W ujęciu instancji dla drogowego przejścia granicznego Terespol–Brześć priorytety te mają konsekwencje bezpośrednie: wysoka wrażliwość odprawy na niedostępność usług powoduje, że mechanizmy dostępności i degradacji muszą być projektowane „w pierwszej kolejności", a dopiero następnie uzupełniane o pełne spektrum kontroli poufności i integralności, jednocześnie przetwarzanie danych identyfikacyjnych i biometrycznych (EES) wymusza wzmocnienie rozliczalności dostępu i obserwowalności, ponieważ potencjalny wpływ naruszenia jest istotny zarówno prawnie, jak i operacyjnie (Parlament Europejski i Rada UE, 2017; ENISA, 2024; Straż Graniczna, 2025). Syntetycznym wyrazem trzeciego wyniku jest Tabela 1, przygotowana w wariancie dopasowanym do instancji Terespol.

Tabela 1. Mapa decyzji BORDER-CyRes – priorytetowe zdolności, minimalny zakres wdrożenia i mierniki (instancja: drogowe przejście graniczne Terespol–Brześć)

Priorytet	Zdolność (co)	Minimalny zakres wdrożenia (co konkretnie wdrożyć – MVP)	Jak mierzyć (2–3 wskaźniki)	Właściciel / warstwa	Odniesienia (skrót)
P1	Dostępność + „degraded border ops”	Ochrona anty-DDoS (np. rate-limiting/ scrubbing), redundancja łączy, procedura pracy w degradacji (minimalny zestaw funkcji odprawy, priorytety kolejek), test przełączenia	Dostępność usług (%), czas przełączenia (min), przepustowość w degradacji (% normy)	Centrala + przejście + operator łączności	ENISA PA TL, NIS2 (ciągłość)
P1	Tożsamość i dostępy uprzywilejowane	MFA dla operatorów i adminów, PAM dla kont uprzywilejowanych, zasada najmniejszych uprawnień, eliminacja kont współdzielonych	% kont uprzywilejowanych z MFA, liczba kont „shared”, czas odebrania uprawnień (h)	Back-end krajowy + stanowiska odpraw	NIST ZT, NIS2
P1	Segmentacja IT/OT + kontrola dostępu do sieci (NAC)	Podział na strefy (stanowiska odpraw, urządzenia brzegowe/biomet., strefa serwisowa), reguły komunikacji „tylko konieczne”, NAC dla urządzeń, szybka procedura izolacji segmentu	Liczba dozwolonych połączeń między strefami, czas izolacji segmentu (min), % urządzeń objętych NAC	Punkt graniczny (LAN) + centrala	NIST ZT, CIS v8
P1	Widoczność (logi + EDR) i korelacja zdarzeń	Centralizacja logów z przejścia, EDR na stacjach odpraw, spójne identyfikatory transakcji odprawy, korelacja w SIEM	Pokrycie logowania (% systemów krytycznych), MTTD (czas wykrycia), odsetek alarmów wysokiej trafności	SOC/SIEM (kraj) + przejście	NIST CSF 2.0
P1	Odtwarzanie po ransomware (kopie niezmienialne + obrazy stacji)	Kopie immutable (offline/odseparowane), testy odtworzeń, „golden images” stanowisk odpraw, runbook „clean restore”	RTO/RPO dla usług odprawy, % udanych testów odtworzeń, czas odtworzenia stanowiska (min/h)	Back-end krajowy + przejście	NIST 800-160, M-Trends

Priorytet	Zdolność (co)	Minimalny zakres wdrożenia (co konkretnie wdrożyć – MVP)	Jak mierzyć (2–3 wskaźniki)	Właściciel / warstwa	Odniesienia (skrót)
P2	Automatyzacja reakcji (playbooki)	Gotowe playbooki: blokada konta, izolacja hosta, odcięcie segmentu, reguły firewall, szybkie „zamrożenie zmian" na przejściu, półautomatyczna obsługa IOC	Czas od alarmu do akcji, % incydentów obsłużonych playbookiem, MTTR (czas przywrócenia)	SOC/CSIRT + lokalne procedury	NIST IR (800-61)
P2	Łańcuch dostaw i serwis (third-party)	Wymagania bezpieczeństwa w umowach, kontrola kanałów serwisowych, rejestr dostawców krytycznych, kontrola aktualizacji (okna serwisowe), SBOM tam, gdzie możliwe	% dostawców ocenionych, czas usunięcia podatności (dni), liczba incydentów third-party	Centrala + dostawcy	DBIR, ENISA
P2	Raportowanie i koordynacja (24h/72h/1 miesiąc)	Szablony zgłoszeń, jedno „case management", RACI (kto decyduje o degradacji/komunikuje/raportuje), ćwiczenia (DDoS, ransomware, supply chain)	Czas do „wczesnego ostrzeżenia" (h), kompletność zgłoszenia (% pól), liczba ćwiczeń/rok	Kierownictwo + CSIRT + przejście	NIS2, EU-CyCLON

Źródło: opracowanie własne.

Tabela ma charakter mapy decyzji wdrożeniowych. Zestawia priorytetowe zdolności cyberodporności w instancji dla drogowego przejścia granicznego Terespol–Brześć, definiując minimalny zakres wdrożeniowy (MVP) oraz mierniki umożliwiające weryfikację skuteczności. Priorytety P1 obejmują mechanizmy bezpośrednio warunkujące ciągłość odprawy i ograniczenie „blast radius", natomiast P2 uzupełniają zdolności automatyzacji, zarządzania dostawcami oraz zgodności raportowej i koordynacyjnej. Zastosowanie praktyczne modelu BORDER-CyRes w instytucji granicznej, w tym na przykładzie drogowego przejścia granicznego Terespol–Brześć, wymaga równoległego potraktowania trzech płaszczyzn: architektury technicznej, operacji bezpieczeństwa oraz governance i zgodności. W płaszczyźnie architektonicznej punktem startowym jest formalna identyfikacja usług krytycznych odprawy jako wątków misji (np. transakcja weryfikacji i transakcja rejestracji danych w logice EES) oraz ich zależności, a następnie przypisanie parametrów ciągłości RTO/RPO. Takie podejście jest spójne z definicją cyberodporności jako redukcji ryzyka misji zależnej od zasobów cybernetycznych i pozwala projektować mechanizmy degradacji w sposób kontrolowany, zamiast ad hoc (NIST, 2021; NIST, 2024). W płaszczyźnie operacyjnej kluczowe jest ustanowienie zdolności detekcji i reakcji (SOC/CSIRT) z automatyzacją playbooków oraz zapewnienie wysokiej jakości telemetryki z punktu granicznego. Presja czasowa obserwowana w incydentach ransomware oraz ryzyko długotrwałej obecności intruza uzasadniają inwestycje w skrócenie MTTD i MTTR oraz w możliwość szybkiej izolacji segmentu bez wywołania niekontrolowanej degradacji odprawy (Mandiant, 2025; Nelson i in., 2025). W płaszczyźnie zarządczej niezbędne jest zbudowanie schematu decyzyjnego i odpowiedzialności (RACI) dla działań krytycznych, w szczególności: kto podejmuje decyzję o przejściu w tryb „degraded border ops", kto raportuje incydent w logice 24-72-30, a kto odpowiada za komunikację do interesariuszy, co jest wymagane zarówno przez NIS2, jak i przez specyfikę środowiska międzyinstytucjonalnego (Parlament Europejski i Rada UE, 2022).

Wymiar międzyinstytucjonalny i transgraniczny stanowi w modelu odrębną oś ryzyka. Cyberodporność przejścia granicznego jest wrażliwa na „pęknięcia zaufania" między podmiotami o różnych mandatach, dojrzałości i kanałach komunikacji, co wzmacnia potrzebę standaryzacji wymiany

informacji oraz wspólnych ćwiczeń operacyjnych obejmujących zarówno DDoS, ransomware, jak i incydenty łańcucha dostaw (ENISA, 2024, ENISA, 2026). W ujęciu unijnym mechanizmy koordynacyjne (w tym EU-CyCLONe) wspierają zarządzanie dużymi incydentami i budowę wspólnej świadomości sytuacyjnej, natomiast w ujęciu praktycznym przekłada się to na konieczność posiadania „pakietu interoperacyjności cyber": uzgodnionych formatów IOC, bezpiecznych kanałów wymiany, zdefiniowanych punktów kontaktu oraz procedur szybkiego potwierdzania wpływu incydentu na ciągłość odprawy. Z perspektywy Terespola oznacza to, że gotowość do współdziałania musi obejmować zarówno warstwę techniczną (telemetria i wymiana IOC), jak i proceduralną (eskalacja i raportowanie), ponieważ incydent może oddziaływać wzdłuż zależności kraj-UE (Parlament Europejski i Rada UE, 2018b; Parlament Europejski i Rada UE, 2019a; Parlament Europejski i Rada UE, 2022).

Osadzenie w realiach Polski wymaga uwzględnienia krajowego systemu cyberbezpieczeństwa i relacji z CSIRT-ami poziomu krajowego, a także praktyk współpracy w incydentach krytycznych (Sejm Rzeczypospolitej Polskiej, 2018). W praktyce konsekwencją dla projektowania cyberodporności przejścia granicznego jest utrzymywanie stałych kanałów eskalacji i wymiany informacji o zagrożeniach, włączanie scenariuszy DDoS, ransomware i supply chain do cyklu ćwiczeń (w tym testów przełączenia na „degraded mode"), a także konsekwentne wzmacnianie ochrony tożsamości i kont uprzywilejowanych, co jest spójne zarówno z logiką Zero Trust (Rose i in., 2020), jak i z obserwacjami dotyczącymi czynnika ludzkiego i third-party w naruszeniach (Verizon, 2025). Dodatkowo, etapowe wdrażanie EES i związane z nim obciążenia operacyjne oraz przetwarzanie danych biometrycznych wzmacniają wymagania dotyczące dostępności, integralności i rozliczalności w okresie przejściowym, co powinno być uwzględnione w parametryzacji RTO/RPO i w projektowaniu trybów degradacji odprawy (Parlament Europejski i Rada UE, 2017; Straż Graniczna, 2025).

Wnioski

Rozdział odpowiada na problem projektowania i operacjonalizacji cyberodporności systemów granicznych w warunkach „systemu systemów", proponując i uzasadniając referencyjny model BORDER-CyRes.

Zasadniczym wkładem jest integracja trzech perspektyw: architektonicznej (warstwowy ekosystem end-to-end), operacyjnej (workflow reagowania w logice „podwójnego rytmu") oraz wdrożeniowej (mapa decyzji: mechanizmy–mierniki–ramy). Taka konstrukcja umożliwia przejście od opisu środowiska granicznego jako układu zależności kraj–UE–partnerzy do spójnego zestawu decyzji projektowych i operacyjnych, które mogą być mierzone i testowane w praktyce. W ujęciu aplikacyjnym kluczowym wnioskiem jest to, że cyberodporność przejścia granicznego – zilustrowana na przykładzie drogowego przejścia granicznego Terespol–Brześć wymaga traktowania ciągłości odprawy jako funkcji krytycznej, której utrzymanie musi być zapewniane równolegle z ochroną danych wrażliwych, w tym danych biometrycznych przetwarzanych w logice EES (European Commission, 2025; Parlament Europejski i Rada UE, 2017; Straż Graniczna, 2025). Oznacza to konieczność projektowania mechanizmów nie tylko w kategoriach prewencji, ale także jako zdolności do kontrolowanej degradacji i odtworzenia przy zachowaniu sterowności procesu odprawy. Priorytetyzację mechanizmów w modelu uzasadniają dane wskazujące na dominację incydentów wpływających na dostępność (w szczególności DDoS) w sektorze administracji publicznej UE oraz istotny udział naruszeń danych i incydentów ransomware, co potwierdza potrzebę równoczesnego wzmacniania odporności dostępnościowej, obserwowalności i gotowości odtworzeniowej (ENISA, 2024; ENISA, 2026; Mandiant, 2025). Drugim wnioskiem jest to, że skuteczna cyberodporność przejścia granicznego wymaga spójnego sprzężenia decyzji architektonicznych z procedurami operacyjnymi i obowiązkami raportowymi. Model pokazuje, że działania takie jak segmentacja IT/OT, wzmocnienie tożsamości i uprzywilejowanych dostępów czy automatyzacja reakcji nie mają wyłącznie charakteru „technicznego", determinują one wykonalność utrzymania odprawy w incydencie oraz zdolność do spełnienia wymogów raportowania i koordynacji, w tym sekwencji 24-72-30 dni (NIST, 2024; Parlament Europejski i Rada UE, 2022). W konsekwencji, etap „wczesnego ostrzeżenia ≤24h" powinien być interpretowany jako element równoległy wobec stabilizacji operacyjnej, ponieważ uruchomienie koordynacji i ścieżki raportowej wpływa na dostęp do zasobów reakcyjnych oraz na tempo działań systemowych (np. mitigacja, izolacja segmentu, przełączenia), a tym samym na ciągłość odprawy (Nelson i in., 2025; Parlament Europejski i Rada UE, 2022).

Kolejnym wnioskiem jest znaczenie ryzyka ekosystemowego, w szczególności zależności od podmiotów trzecich. W środowisku granicznym istotna część ryzyka ma charakter współdzielony z dostawcami technologii, integratorami i operatorami usług, co wzmacnia potrzebę ujęcia łańcucha dostaw jako pełnoprawnego obszaru cyberodporności, a nie komponentu pobocznego (Verizon, 2025; ENISA, 2024). Wymaga to formalizacji wymagań, kontroli kanałów serwisowych oraz testowania scenariuszy supply chain w cyklu ćwiczeń, zwłaszcza w punktach granicznych o wysokiej krytyczności operacyjnej.

Ograniczenia zaprezentowanego ujęcia wynikają, po pierwsze, z wykorzystania danych wtórnych, które odzwierciedlają obraz zagrożeń zależny od praktyk raportowania i dostępności informacji, co może wpływać na obserwowany rozkład klas incydentów (ENISA, 2024; ENISA, 2026). Po drugie, walidacja scenariuszowa – mimo że wzmacnia wykonalność wniosków – nie zastępuje weryfikacji wdrożeniowej w konkretnej architekturze organizacyjnej i technicznej (NIST, 2024). Dodatkowo, instancja dla przejścia Terespol–Brześć ma charakter referencyjny. Szczegółowe parametry (np. wartości RTO/RPO, progi przełączeń, docelowe mierniki MTTD/MTTR) wymagają doprecyzowania w oparciu o lokalne uwarunkowania przepustowości, topologii łączności, modelu odpowiedzialności oraz reżimu utrzymaniowego (NIST, 2021, NIST, 2024). Z perspektywy dalszych badań zasadne jest rozszerzenie walidacji o studia przypadków w różnych typach przejść (drogowych osobowych vs towarowych, lotniczych, kolejowych) oraz o pomiar dojrzałości wdrożeń w kategoriach NIST CSF 2.0 i Zero Trust, z jednoczesnym uwzględnieniem wymogów interoperacyjności i danych biometrycznych EES (NIST, 2024; Rose i in., 2020; Parlament Europejski i Rada UE, 2017). W kontekście NIS2 kierunkiem rozwojowym jest doprecyzowanie metryk i minimalnych artefaktów dowodowych (case management, logi, audyt integralności) tak, aby skracać czas uzyskania wiarygodnego obrazu sytuacji i wspierać koordynację kraj-UE w incydentach o dużej skali (Parlament Europejski i Rada UE, 2022; Nelson i in., 2025).

Literatura

1. Chodyka, M., Żurawski, S., Parczewska, W. (2025). Wpływ cyberzagrożeń na bezpieczeństwo granicy Rzeczypospolitej Polskiej. W: D. Brążkiewicz, M. Chodyka, T. Grudniewski, S. Żurawski (red.), *Wielowymiarowość środowiska bezpieczeństwa. Część druga* (s. 295-307). Wydawnictwo Akademii Bialskiej im. Jana Pawła II. https://doi.org/10.29316/9788368103236_188
2. Ciekanowski, Z. (2020). Straż graniczna w sytuacjach kryzysowych. W: Z. Ciekanowski (red.), *Państwo wobec zagrożeń* (s. 256-268). Wydawnictwo Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej. https://hdl.handle.net/20.500.13044/691
3. Ciekanowski, Z., Nowicka, J., Żurawski, S. (2022). Frontex w systemie zarządzania bezpieczeństwem granic Unii Europejskiej. *De Securitate et Defensione. O Bezpieczeństwie i Obronności, 8*(2), 176-186. https://doi.org/10.34739/dsd.2022.02.12
4. Elak, L., Oskierko, M., Żurawski, S. (2024). Ochrona granicy polsko-białoruskiej w obliczu wojny hybrydowej. *De Securitate et Defensione. O Bezpieczeństwie i Obronności, 10*(1), 81-95. https://doi.org/10.34739/dsd.2024.01.04
5. ENISA. (2024). *ENISA Threat Landscape 2024*. Pobrane z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (dostęp: 12.02.2026).
6. ENISA. (2025*). ENISA Sectorial Threat Landscape: Public Administration*. Pobrane z: https://www.enisa.europa.eu/publications/sectorial-threat-landscape-public-administration (dostęp: 12.02.2026).
7. European Commission. (2025). *Entry/Exit System (EES)*. Pobrane z: https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en (dostęp: 12.02.2026).
8. Mandiant. (2025). *M-Trends 2025 report.* Pobrane z : https://services.google.com/fh/files/misc/m-trends-2025-en.pdf#page=1&zoom=auto,-263,792 (dostęp: 12.02.2026).
9. MITRE. (2025). *MITRE ATT&CK knowledge base.*
10. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

11. Nelson, A., Rekhi, S., Souppaya, M., Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3
12. Parlament Europejski i Rada UE. (2017). *Rozporządzenie (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiające System Wjazdu/Wyjazdu (EES)* (Dz. Urz. UE L 327 z 9.12.2017).
13. Parlament Europejski i Rada UE. (2018a). *Rozporządzenie (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiające europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS)* (Dz. Urz. UE L 236 z 19.09.2018).
14. Parlament Europejski i Rada UE. (2018b). *Rozporządzenie (UE) 2018/1726 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości (eu-LISA)* (Dz. Urz. UE L 295 z 21.11.2018).
15. Parlament Europejski i Rada UE. (2018c). *Rozporządzenie (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych* (Dz. Urz. UE L 312 z 7.12.2018).
16. Parlament Europejski i Rada UE. (2019a). *Rozporządzenie (UE) 2019/817 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności systemów informacyjnych UE w dziedzinie granic i wiz* (Dz. Urz. UE L 135 z 22.05.2019).
17. Parlament Europejski i Rada UE. (2019b). *Rozporządzenie (UE) 2019/1896 z dnia 13 listopada 2019 r. w sprawie Europejskiej Straży Granicznej i Przybrzeżnej* (Dz. Urz. UE L 295 z 14.11.2019).
18. Parlament Europejski i Rada UE. (2022). *Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii* (Dz. Urz. UE L 333 z 27.12.2022).
19. Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020). *Zero trust architecture*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

20. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1
21. Sejm Rzeczypospolitej Polskiej. (2018). *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz. U. z 2018 r. poz. 1550).
22. Straż Graniczna. (2025). *Entry/Exit System (EES) – informacje i wdrożenie w Polsce*.
23. Verizon. (2025). *2025 Data Breach Investigations Report*. Pobrane z: https://www.verizon.com/business/resources/reports/dbir/ (dostęp: 12.02.2026).
24. Wojciechowska-Filipek, S., Ciekanowski, Z. (2019). *Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki – organizacji – państwa*. CeDeWu.