Przegląd Bezpieczeństwa Wewnętrznego
2026, nr 34, s. 205–223

https://doi.org/10.4467/20801335PBW.26.010.23372

ARTYKUŁ

Łączność w ramach administracji państwowej jako fundament odporności państwa na przykładzie Polski[1]

Communications within the state administration as the foundation of a nation's resilience: the case of Poland

DAVID CYBULSKI

Akademia Sztuki Wojennej

https://orcid.org/0009-0003-9195-4407

Abstrakt

Celem artykułu jest przedstawienie roli oraz stanu łączności między organami współczesnej administracji Rzeczypospolitej Polskiej. Zostały omówione aspekty prawne, organizacyjne i techniczne problematyki łączności w ramach tej administracji. Wskazano poważne braki w funkcjonowaniu dotychczasowych systemów łączności w cywilnych strukturach państwa, co może przekładać się na zdolności Polski do sprawnego reagowania na zagrożenia bezpieczeństwa narodowego. Podstawowym problemem jest brak ujednoliconego podejścia państwa do funkcjonowania komunikacji między

[1] Artykuł powstał na podstawie pracy magisterskiej pt. *Łączność i komunikacja administracji państwa w sytuacji zagrożenia bezpieczeństwa narodowego: na przykładzie Polski*, obronionej na Wydziale Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego. Autor wykorzystał fragmenty rozdziałów I, II i IV. Praca została nagrodzona w XV edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

jednostkami administracji publicznej, w szczególności organami bezpieczeństwa, służbami ratunkowymi. Konieczne jest tym samym pilne dokonanie modernizacji podsystemu łączności państwowej do celów zarządzania kryzysowego w kontekście współczesnych wyzwań.

Słowa kluczowe komunikacja elektroniczna, łączność, łączność awaryjna, zarządzanie kryzysowe, System Bezpiecznej Łączności Państwowej

Abstract The purpose of this article is to present the role and current state of communications among the agencies of the modern administration of the Republic of Poland. The article addresses legal, organisational, and technical aspects of communication within the state administration. It highlights serious systemic deficiencies related to the functioning of existing communication systems in the civilian structures of the state, which may affect Poland's ability to respond effectively to emerging threats to national security. The fundamental problem here is the lack of a unified state perspective on the establishment and operation of communication between its various components, namely security agencies, emergency services, and public administration. It is therefore necessary to urgently modernise the state communications subsystem for crisis management purposes in the context of contemporary challenges.

Keywords electronic communication, telecommunications, emergency communications, crisis management

Wprowadzenie

Współczesne środowisko bezpieczeństwa narodowego charakteryzuje się ewoluującymi zagrożeniami, w tym cyberatakami, terroryzmem, a także działaniami o charakterze hybrydowym. W takich warunkach klasyczne, liniowe modele zarządzania kryzysowego okazują się niewystarczające, a zdolność państwa do skutecznego reagowania jest w coraz większym stopniu uzależniona od jakości przepływu informacji między kluczowymi uczestnikami systemu bezpieczeństwa. Szczególne znaczenie w tym kontekście zyskuje podsystem łączności, który nie tylko stanowi techniczne zaplecze dla działań administracji publicznej, służb ratowniczych i podmiotów odpowiedzialnych za ochronę infrastruktury krytycznej, lecz także odpowiada za sprawne działanie całego systemu zarządzania kryzysowego.

Cyfryzacja administracji oraz rosnąca złożoność środowiska zagrożeń sprawiają, że skuteczna i bezpieczna wymiana informacji staje się warunkiem sine qua non przeciwdziałania incydentom mającym wpływ na funkcjonowanie państwa, zarówno o charakterze fizycznym, jak i cyfrowym. Jednocześnie wiele dokumentów, np. informacje pokontrolne NIK, wskazuje, że obecne systemy łączności w administracji publicznej często nie są w pełni dostosowane do jej współczesnych realiów operacyjnych i technologicznych. Przejawia się to m.in. w rozdrobnieniu rozwiązań telekomunikacyjnych, braku jednolitej architektury wymiany informacji, niedostatkach interoperacyjności, a także w znacznej podatności na błędy projektowe czy błędy popełnione przez człowieka.

Problem badawczy to pytanie: w jakim stopniu obecny podsystem łączności administracji państwowej jest odporny na aktualne zagrożenia dla bezpieczeństwa narodowego oraz jakie kierunki zmian mogą zwiększyć jego efektywność? Odpowiedź na to pytanie wymaga potraktowania łączności jako złożonego systemu społeczno-technicznego, w którym ramy prawne, rozwiązania organizacyjne, technologie i kompetencje użytkowników wzajemnie się warunkują. Hipoteza przyjęta w artykule zakłada, że istniejący system łączności administracji państwowej – budowany przez lata w sposób resortowy (jedynie pod zapotrzebowanie danego resortu) i fragmentaryczny – nie zapewnia w wystarczającym stopniu spójności i odporności na współczesne zagrożenia oraz że możliwe jest wskazanie realistycznych kierunków jego optymalizacji.

W artykule dokonano przeglądu ram normatywnych funkcjonowania łączności na potrzeby bezpieczeństwa narodowego, obejmujących zarówno ustawy, jak i rozporządzenia wykonawcze oraz wybrane dokumenty strategiczne. Ponadto zidentyfikowano i sklasyfikowano główne kategorie ryzyka – od błędów planistycznych i projektowych, przez problemy eksploatacyjne i ograniczenie suwerenności technologicznej, aż po zagrożenia cyberbezpieczeństwa. Następnie zaproponowano kierunki modernizacji, obejmujące zarówno integrację funkcjonujących systemów, jak i potencjał nowych technologii oraz koncepcję zintegrowanego podsystemu łączności państwa.

Zastosowano takie metody, jak: analiza aktów prawnych, przegląd literatury z zakresu bezpieczeństwa narodowego i telekomunikacji oraz analiza dokumentacji technicznej wybranych systemów. Wskazano także przykłady rozwiązań wdrożonych we Francji i Australii. Wykorzystano również analizę systemową, pozwalającą potraktować podsystem łączności jako element większej całości – narodowego systemu bezpieczeństwa – oraz ocenić jego funkcjonowanie w kategoriach spójności, redundancji i odporności. Zakres analizy celowo został ograniczony do rozwiązań komunikacyjnych w administracji państwowej, z wyłączeniem komunikacji

masowej między obywatelami oraz wojskowej, co umożliwia pogłębione ujęcie problematyki z perspektywy instytucji państwa.

Artykuł wpisuje się w szerszy nurt badań nad modernizacją systemów bezpieczeństwa państwa w warunkach transformacji cyfrowej i nasilających się napięć geopolitycznych. Wskazuje, że problematyka łączności – często postrzegana jako domena techniczna – powinna być traktowana jako strategiczny element bezpieczeństwa narodowego, wymagający spójnej polityki publicznej oraz świadomych decyzji inwestycyjnych. Proponowane wnioski i rekomendacje mogą stanowić punkt wyjścia zarówno do dalszych badań naukowych, jak i do prac koncepcyjnych związanych z aktualizacją krajowego podsystemu łączności administracji państwowej na potrzeby zarządzania kryzysowego.

Ramy prawne

Zapewnienie ciągłej i niezawodnej wymiany informacji uznano w Polsce za jeden z filarów bezpieczeństwa narodowego i sprawnego działania administracji publicznej, zwłaszcza w sytuacjach kryzysowych, nadzwyczajnych czy zagrożenia konfliktem zbrojnym. W efekcie stworzono rozbudowany system aktów prawnych, które regulują budowę, funkcjonowanie i ochronę systemów wchodzących w skład podsystemu łączności państwa, obejmujących zarówno systemy rządowe, jak i ogólnodostępne systemy komercyjne, mogące pełnić funkcję łączności zapasowej dla organów państwa.

W *Ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* wybrane systemy łączności i sieci teleinformatyczne zaliczono do infrastruktury krytycznej (art. 3 pkt 2 lit. b i c). Ustawa nakłada obowiązek opracowania i aktualizowania planów zarządzania kryzysowego, które muszą uwzględniać również kwestie teleinformatyczne i łączności (art. 6 ust. 5b), oraz ustanawiania zasady obiegu informacji w krajowym systemie zarządzania kryzysowego (art. 11 ust. 2 pkt 8). Ustawa wyraźnie wskazuje, że systemy łączności będące częścią infrastruktury krytycznej – zarówno rządowe, jak i część systemów komercyjnych – podlegają szczególnej ochronie przed zagrożeniami.

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych reguluje ochronę infrastruktury teleinformatycznej przed zdarzeniami o charakterze terrorystycznym oraz zasady wymiany informacji między organami administracji publicznej i służbami w razie wystąpienia takich zagrożeń. Przewiduje ona m.in. możliwość czasowego dostosowywania i montażu przewodowych i bezprzewodowych instalacji łączności na potrzeby zabezpieczenia wydarzenia o podwyższonym ryzyku, z pewnymi odstępstwami od prawa budowlanego, tak aby zapewnić łączność

właściwym służbom (art. 13). Ustawa wprowadza również system stopni alarmowych i stopni alarmowych CRP (dotyczących cyberprzestrzeni RP), ogłaszanych zarządzeniem Prezesa Rady Ministrów. Dla podsystemu łączności istotne z punktu widzenia powyższych stopni są takie zadania, jak m.in.: informowanie podległego personelu, weryfikacja działania środków łączności, wzmożone monitorowanie systemów teleinformatycznych i integralności komunikacji elektronicznej, zapewnienie dyżurów administratorów i osób decyzyjnych, przegląd zapasowej infrastruktury teleinformatycznej oraz realizacja planów postincydentalnych przy najwyższych stopniach zagrożenia terrorystycznego[2].

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny kompleksowo opisuje zadania państwa w zakresie bezpieczeństwa militarnego, w tym kwestie organizacji łączności na potrzeby obronności. Jednym z centralnych elementów ustawy jest wojskowy system telekomunikacyjny (art. 17), który łączy Siły Zbrojne RP i resort obrony z innymi organami administracji publicznej oraz – w razie potrzeby – z organizacjami społecznymi służącymi obronności[3]. Ma on zapewniać funkcjonowanie systemu kierowania bezpieczeństwem narodowym oraz sprawne działanie państwa w czasie wojny, zagrożenia zewnętrznego i poważnych kryzysów, co wymaga od systemów łączności m.in. skalowalności i wysokiej żywotności, czyli zachowania integralności i dostępności w skrajnych warunkach. Ustawa przewiduje także możliwość militaryzacji wybranych podmiotów o kluczowym znaczeniu dla obronności, w tym przedsiębiorców telekomunikacyjnych. W praktyce oznacza to, że np. operator telefonii komórkowej może zostać objęty reżimem wojskowym, aby w razie zagrożenia zapewnić dostępność jego sieci na potrzeby administracji państwowej i sił zbrojnych.

Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej porządkuje zasady funkcjonowania rynku telekomunikacyjnego i komunikacji elektronicznej. Nakłada jednocześnie obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Zobowiązuje przedsiębiorców telekomunikacyjnych do opracowania planów działania w sytuacjach szczególnych zagrożeń i utrzymywania ciągłości świadczenia usług, a Prezesowi Urzędu Komunikacji Elektronicznej (UKE) przyznaje uprawnienia do nakładania na nich określonych obowiązków, np. w zakresie utrzymania działania sieci. Istotny z punktu widzenia podsystemu łączności państwa jest nałożony na przedsiębiorców obowiązek świadczenia usług na rzecz organów państwowych w razie szczególnego zagrożenia

[2] *Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP.*

[3] *Rozporządzenie Ministra Obrony Narodowej z dnia 20 kwietnia 2022 r. w sprawie działania wojskowego systemu telekomunikacyjnego.*

bezpieczeństwa, stanów nadzwyczajnych czy wojny. Ustawa zobowiązuje także operatorów do przekazywania Prezesowi UKE informacji o posiadanej infrastrukturze telekomunikacyjnej potrzebnej do przygotowania systemów łączności służących obronności i bezpieczeństwu, co umożliwia władzom państwowym planowanie wykorzystania potencjału sieci publicznych jako elementu systemu bezpieczeństwa.

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz *Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym* (art. 21 pkt 6) przyznają władzom państwowym prawo do czasowego ograniczania praw i wolności obywatelskich, w tym swobody korzystania z systemów łączności. Pozwala to na redukowanie lub wyłączanie części usług dla ogółu użytkowników, aby zapewnić administracji państwowej, wojsku i służbom priorytetowy dostęp do łączności. Dzięki tym regulacjom możliwe jest również sięgnięcie po komercyjne systemy łączności jako łącza zapasowe, z jednoczesnym ograniczeniem ich publicznego obciążenia w taki sposób, aby w krytycznym momencie nie doszło do przeciążenia infrastruktury.

Obowiązująca od 2025 r. *Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej* wypełnia dotychczasową lukę regulacyjną w obszarze obrony cywilnej i porządkuje system ochrony ludności w sytuacjach pokoju, kryzysu i wojny. Określa ona m.in. infrastrukturę niezbędną do realizacji zadań ochrony ludności, w tym infrastrukturę łączności i systemy teleinformatyczne jako podstawowy warunek efektywnej koordynacji działań różnych szczebli administracji. Na podstawie art. 71 wyodrębniono katalog narzędzi komunikacyjnych tworzących system komunikacji administracji państwowej: syreny alarmowe i urządzenia nagłaśniające, systemy ostrzegania (w tym Regionalny System Ostrzegania), dzienniki lokalne i ogólnopolskie, radio i telewizję, system ALERT RCB, ostrzeżenia wysyłane w ramach technologii cyfrowych oraz oficjalne serwisy informacyjne administracji.

Jednym z centralnych projektów przewidzianych w ustawie o ochronie ludności i obronie cywilnej jest System Bezpiecznej Łączności Państwowej (SBŁP), nadzorowany przez ministra właściwego do spraw wewnętrznych (art. 15 ust. 1 pkt 24). System ma stanowić zintegrowaną, bezpieczną i o wysokiej dostępności platformę łączności dla najważniejszych organów państwa, służb ratowniczych, podmiotów ochrony ludności i sił zbrojnych, łącząc różne dotychczasowe systemy resortowe przez odpowiednie interfejsy i standardy. W ustawie wyróżniono kilka funkcjonalnych wariantów SBŁP: system jawny (SBŁP-J), system wielopunktowej wideokonferencji (SBŁP-V), radiowy system mobilny (SBŁP-M), system radiowej łączności trankingowej (SBŁP-T) oraz system łączności satelitarnej (SBŁP-S). Wszystkie te moduły mają zapewniać szyfrowanie end-to-end oraz spełniać określone przez

Radę Ministrów minimalne wymagania bezpieczeństwa teleinformatycznego, adekwatne do poziomu zagrożeń (art. 78 pkt 2).

Dodatkowo *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* reguluje zasady przetwarzania informacji klauzulowanych w systemach teleinformatycznych. Dla podsystemu łączności oznacza to konieczność projektowania oddzielnych, akredytowanych systemów dla komunikacji niejawnej, takich jak systemy niejawnej łączności stacjonarnej (SBŁP-N), a częściowo również SBŁP-M i SBŁP-S. Przetwarzanie informacji niejawnych jest dopuszczalne wyłącznie w systemach do tego dostosowanych, w tym specjalnie akredytowanych przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego. To powoduje, że dystrybucja danych, np. wywiadowczych czy informacji operacyjnych, staje się logistycznie trudniejsza, równocześnie jednak zwiększa ochronę przed ich przechwyceniem. Wymusza też tworzenie wyspecjalizowanych sieci i urządzeń końcowych dla uprawnionych użytkowników.

Analiza zagrożeń dla podsystemu łączności

Podsystem łączności administracji państwowej stanowi jeden z filarów zarządzania kryzysowego oraz szeroko rozumianego systemu bezpieczeństwa narodowego. Jest kluczem do efektywnego zarządzania siłami i środkami zarówno w wymiarze prewencyjnym, jak i na etapie reagowania na sytuacje kryzysowe, w których przekaz informacji za pomocą technicznych środków łączności pozostaje podstawowym kryterium zintegrowanego zarządzania zasobami[4]. Jednocześnie brakuje alternatyw dla współczesnych systemów teleinformatycznych, co sprawia, że konieczność priorytetyzacji przez państwo rozwoju, utrzymania i zabezpieczenia tych systemów jest bezdyskusyjna. Bez odpowiednich rozwiązań technologicznych nawet najlepiej przygotowana i wyspecjalizowana administracja nie będzie zdolna do skutecznego wykonywania swoich zadań, ponieważ nie będzie miała narzędzi do sprawnej koordynacji działań na poziomach taktycznym, operacyjnym i strategicznym, co grozi pogłębieniem kryzysu.

Znaczenie systemów łączności dla bezpieczeństwa narodowego potwierdzają dokumenty strategiczne, w tym Strategia Bezpieczeństwa Narodowego z 2020 r. Wskazano w niej, że sieci łączności satelitarnej i mobilnej stanowią podstawę wymiany informacji i są kluczowym elementem zasobów bezpieczeństwa narodowego

[4] J. Pilżys, *Zarządzanie systemami łączności i transmisją danych w sytuacjach kryzysowych*, „Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" 2015, t. 8, nr 1, s. 45.

oraz gotowości państwa na wypadek sytuacji kryzysowych[5]. Systemy łączności zostały zaliczone do krajowej infrastruktury krytycznej, a dokument strategiczny akcentuje potrzebę dalszego rozwoju bezpiecznych, nowoczesnych sieci telekomunikacyjnych.

Dotychczasowy rozwój podsystemu łączności w Polsce miał charakter rozproszony i resortowy. Brak całościowego, odgórnego programu budowy jednolitego systemu łączności państwowej sprawił, że poszczególne organy i służby tworzyły własne rozwiązania na miarę bieżących potrzeb i możliwości. W rezultacie funkcjonują systemy, które często nie są ze sobą zintegrowane ani technicznie, ani organizacyjnie[6]. Wymiana informacji między resortami, służbami, a nawet na różnych poziomach administracji publicznej (centralnym, wojewódzkim, powiatowym i gminnym) jest utrudniona. System zarządzania kryzysowego i system kierowania bezpieczeństwem narodowym mają wprawdzie formalnie określoną strukturę hierarchiczną, jednak brak jednolitych środków łączności zarówno w pionie, jak i w poziomie powoduje ryzyko paraliżu decyzyjnego, powielania zadań oraz rozproszenia wysiłków w sytuacji realnego zagrożenia. Wskazuje na to również Najwyższa Izba Kontroli, która w licznych raportach z kontroli zwracała uwagę na problem braku jednolitego cyfrowego systemu łączności radiowej dla służb ratowniczych i struktur zarządzania kryzysowego. Oceniała, że to negatywnie oddziałuje na przepływ informacji i skuteczność działań[7].

Ważnym elementem kształtowania każdego systemu teleinformatycznego jest jego właściwe zaplanowanie i zaprojektowanie. Standardy z obszaru inżynierii systemów i oprogramowania, takie jak norma ISO/IEC/IEEE 24748-1, wyróżniają pełen cykl życia systemu: planowanie, projektowanie, budowę, użytkowanie, doskonalenie i ostatecznie wycofanie z eksploatacji[8]. Każdy z tych etapów jest ze sobą ściśle powiązany, a błędy popełnione w fazie planistycznej mogą się kumulować w kolejnych fazach projektu. W przypadku systemów o znaczeniu państwowym, szczególnie tych o zasięgu krajowym, błędne założenia, niedoszacowanie kosztów i terminów, wybór niewłaściwych partnerów, pominięcie analizy rzeczywistych potrzeb użytkowników czy rezygnacja z wbudowania redundancji mogą doprowadzić do sytuacji, w której system nie będzie spełniał swojej podstawowej funkcji.

---

5 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*, Warszawa 2020, s. 8.

6 M. Gawroński, *Systemy teleinformatyczne wspomagania kierowania systemem bezpieczeństwa narodowego*, „Wiedza Obronna" 2014, nr 2–3, s. 61–63.

7 Najwyższa Izba Kontroli, *Informacja o wynikach kontroli: Organizacja i przygotowanie do działań ratowniczych na autostradach i drogach ekspresowych*, 2017 r., s. 11.

8 ISO/IEC/IEEE 24748-1 – Systems and software engineering – Life cycle management – Part 1: Guidelines for life cycle management.

Przykładem takich zaniedbań jest pożar Mostu Łazienkowskiego w Warszawie w 2015 r. Spowodował zniszczenie kluczowych łączy światłowodowych, co doprowadziło do czasowego odcięcia od sieci części instytucji centralnych, w tym resortu obrony[9]. Z kolei ogólnokrajowe awarie systemów dyspozytorskich Centrów Powiadamiania Ratunkowego w 2021 r. i 2024 r. doprowadziły do sytuacji, w której dyspozytorzy nie byli w stanie przydzielać zadań zespołom ratownictwa medycznego w standardowy sposób, a rozwiązaniem było ręczne zapisywanie zgłoszeń[10]. Zdarzenia te mogły mieć znacznie łagodniejszy przebieg, gdyby już na etapie projektowania przewidziano obowiązek redundancji niezależnych kanałów, alternatywnych tras transmisyjnych oraz procedur przełączenia między nimi.

Równie istotny jest sposób eksploatacji systemów łączności. Etap użytkowania nie kończy cyklu życia systemu – to właśnie w codziennej pracy jest on weryfikowany przez użytkowników końcowych, a równocześnie są gromadzone doświadczenia niezbędne do jego dalszego doskonalenia. Kluczową rolę odgrywa przygotowanie użytkowników. Jeżeli nie zostaną właściwie przeszkoleni, a interfejs systemu okaże się zbyt skomplikowany lub nieintuicyjny, istnieje ryzyko, że w praktyce będą oni obchodzić przewidziane rozwiązania i sięgać po kanały pozasystemowe. Dążenie przez użytkownika do wygody w obszarze łączności może prowadzić np. do wykorzystywania popularnych komunikatorów internetowych, które nie są przystosowane do wymiany informacji niejawnych czy informacji na temat sytuacji kryzysowych. W ostatnich latach odnotowano przykłady wykorzystania komercyjnych aplikacji do przekazywania wrażliwych informacji m.in. w administracjach amerykańskiej oraz w polskiej, w których istotne decyzje były konsultowane z użyciem ogólnodostępnych usług[11]. Takie praktyki podważają poziom bezpieczeństwa informacji i pokazują, że systemy łączności muszą być projektowane z uwzględnieniem nie tylko wymagań technicznych i norm bezpieczeństwa, lecz także ergonomii, łatwości obsługi i nawyków użytkowników.

---

[9] M. Gąsior, *W pożarze mostu spłonęły łącza MON. Kilka instytucji bez dostępu do internetu*, naTemat, 15 II 2015 r., https://natemat.pl/133507,w-pozarze-mostu-splonely-lacza-mon-kilka-instytucji-bez-dostepu-do-internetu [dostęp: 18 III 2026].

[10] *Drugi dzień z awarią systemu ratownictwa medycznego. Ministerstwo uspokaja*, TVN24, 15 V 2021 r., https://tvn24.pl/polska/awaria-systemu-ratownictwa-medycznego-st5095494 [dostęp: 18 III 2026]; *Ogólnopolska awaria Centrum Powiadamiania Ratunkowego 112*, Onet, 16 XII 2024 r., https://wiadomosci.onet.pl/kraj/awaria-centrum-powiadamiania-ratunkowego-112/bltrlw7 [dostęp: 18 III 2026].

[11] J. Goldberg, *The Trump Administration Accidentally Texted Me Its War Plans*, The Atlantic, 24 III 2025 r., https://www.theatlantic.com/politics/archive/2025/03/trump-administration-accidentally-texted-me-its-war-plans/682151/ [dostęp: 18 III 2026]; Z. Wanat, *Leaked email scandal engulfs Poland's political elite*, Politico, 24 VI 2021 r., https://www.politico.eu/article/leaked-email-scandal-engulfs-poland-political-elite-mails-hacking/ [dostęp: 18 III 2026].

Warunkiem poprawnej eksploatacji są szczegółowe procedury operacyjne oraz regularne ćwiczenia. Procedury powinny precyzyjnie opisywać czynności użytkowników i administratorów, a także zawierać plany awaryjne, tryby postępowania w razie utraty części infrastruktury czy wystąpienia incydentów bezpieczeństwa. Ćwiczenia – zarówno symulacje sytuacji kryzysowych, jak i testy obciążeniowe – pozwalają zweryfikować założenia projektowe, wykryć wąskie gardła oraz utrzymać na odpowiednim poziomie kompetencje personelu. Brak ćwiczeń lub ich pobieżny charakter prowadzi do stopniowej utraty umiejętności korzystania z systemów w sytuacjach niestandardowych. To oznacza, że w chwili realnego kryzysu personel może spontanicznie sięgnąć po nieautoryzowane narzędzia, czym narazi bezpieczeństwo informacji i ciągłość działania instytucji.

W wymiarze organizacyjnym szczególnego znaczenia nabiera zagadnienie suwerenności technologicznej. Korzystanie z rozwiązań sprzętowych i programowych pochodzących z państw trzecich, stwarza ryzyko utraty kontroli nad kluczowymi parametrami bezpieczeństwa informacji: poufnością, integralnością i dostępnością. Przykłady takich zagrożeń obejmują zarówno rekomendacje władz[12], aby w systemach krytycznych nie stosować niektórych zagranicznych produktów bezpieczeństwa, jak i przypadki wykrycia backdoorów (pol. tylnych furtek) w urządzeniach i oprogramowaniach[13] wykorzystywanych do przetwarzania danych wrażliwych. Informacje o możliwości zdalnej ingerencji w zaawansowane systemy wojskowe czy o eksfiltracji danych medycznych z wykorzystaniem luk w urządzeniach monitorujących pokazują, że brak pełnej kontroli nad technologią może zostać wykorzystany do wywierania presji politycznej, destabilizacji systemów ochrony zdrowia czy zakłócenia działania sił zbrojnych. W przypadku Polski istnieje ryzyko braku dostępu do ponadnarodowych źródeł danych, np. NATO i Unii Europejskiej czy własnych systemów rozlokowanych poza terytorium kraju (placówki dyplomatyczne, konstelacje satelitarne). Racjonalnym rozwiązaniem jest budowa nadmiarowych, niezależnych torów łączności oraz rozwój krajowego potencjału w zakresie projektowania i produkcji systemów łączności, co pozwoli w większym stopniu uniezależnić się od zagranicznych dostawców i ograniczy możliwość szantażu technologicznego.

Pod względem technicznym bezpieczeństwo i odporność podsystemu łączności opierają się na zapewnieniu określonych atrybutów bezpieczeństwa informacji. Normy z rodziny ISO/IEC 27000 i pokrewnych wyróżniają w tym zakresie przede wszystkim poufność, integralność i dostępność, a także autentyczność,

[12] *Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa z dnia 30 maja 2022 r.* (DC.WFKSC.7250.1.2022), Kancelaria Prezesa Rady Ministrów, 2022 r., s. 1.

[13] *Contec CMS8000 Contains a Backdoor*, CISA 2025, s. 1 i nast.

rozliczalność, aktualność i kompletność danych[14]. W kontekście łączności państwowej oznacza to, że informacje muszą być dostępne dla uprawnionych podmiotów wtedy, kiedy są potrzebne, nie mogą być zmieniane lub niszczone w sposób nieautoryzowany, muszą pochodzić z wiarygodnych źródeł, a każde działanie na nich powinno być możliwe do przypisania do konkretnego użytkownika lub procesu. Dodatkowo informacje wykorzystywane w procesie decyzyjnym muszą być aktualne oraz kompletne, aby umożliwić ich przetworzenie w rzetelną wiedzę operacyjną. Brak któregokolwiek z tych atrybutów może prowadzić do błędnych decyzji, opóźnień lub całkowitego paraliżu działań.

Ponadto poważnym wyzwaniem jest zapewnienie interoperacyjności i kompatybilności stosowanych rozwiązań. Poszczególne służby i instytucje państwowe korzystają z wielu systemów, częstotliwości, protokołów i standardów, które nie zawsze są ze sobą spójne. Brak ogólnokrajowych standardów dla łączności kryzysowej i wspólnej platformy wymiany informacji powoduje, że w sytuacjach wymagających współdziałania mogą pojawić się opóźnienia, nieporozumienia i przerwy w przepływie danych[15]. Rozdrobnienie systemów zwiększa też skalę ataku – utrzymywanie wielu niespójnych rozwiązań utrudnia skuteczne zabezpieczenie i monitoring tych systemów. W obliczu rosnącej liczby cyberataków, w tym ze strony zaawansowanych, sponsorowanych przez państwa grup APT (ang. *advanced persistent threats*), konieczne staje się podejście, w którym bezpieczeństwo łączności postrzegane jest jako element konstytucyjnego obowiązku państwa w zakresie zapewnienia bezpieczeństwa obywateli, a nie jako koszt. Wymaga to stosowania silnego szyfrowania end-to-end, konsekwentnej aktualizacji oprogramowania, segmentacji sieci, stosowania zasady najmniejszych uprawnień (ang. *principle of least privilege*) oraz rozwiązań silnego, najlepiej wieloskładnikowego uwierzytelniania użytkowników.

Wszystkie wskazane zagrożenia prowadzą do jednoznacznego wniosku, że Polska powinna konsekwentnie rozwijać spójny, jednolity podsystem łączności państwa, integrujący istniejące systemy resortowe i zapewniający bezpieczną, odporną i efektywną wymianę informacji na wszystkich poziomach zarządzania i współpracy. Oznacza to odejście od modelu wyspowego na rzecz świadomie zaprojektowanej, skalowalnej i redundantnej architektury, opartej na narodowych kompetencjach technologicznych i wspólnych standardach. Tylko w ten sposób

[14] PN-EN ISO/IEC 27000 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia, Polski Komitet Normalizacyjny, Warszawa 2012, s. 14, 17.

[15] M. Bieńkowski, *Funkcjonowanie systemu ochrony ludności w Polsce*, „Kontrola Państwowa" 2019, nr 5, s. 60–62.

można zagwarantować, że w sytuacjach kryzysowych, w tym w warunkach działań hybrydowych czy konfliktów zbrojnych, aparat państwowy będzie w stanie skutecznie realizować swoje zadania i chronić bezpieczeństwo obywateli.

Możliwości rozwiązania impasu komunikacyjnego

Obecnie w Polsce różne instytucje i resorty korzystają z własnych, często dublujących się rozwiązań (np. dwóch systemów mobilnej łączności niejawnej – CATEL i SKR-Z czy kilku środowisk poczty elektronicznej dla tych samych poziomów tajności – CATEL i System Niejawnej Poczty Internetowej OPAL), które nie są kompatybilne. Brak jednolitego systemu i wspólnych standardów powoduje, że wymiana informacji pomiędzy systemami często odbywa się ręcznie, co wydłuża czas reakcji na zdarzenia kryzysowe i zwiększa ryzyko błędu.

Brak jednolitości systemów generuje również koszty i ryzyka na kilku poziomach. Po pierwsze, zwielokrotniają się nakłady inwestycyjne – państwo finansuje wiele równoległych projektów, co obciąża budżet i ogranicza środki na modernizację infrastruktury czy innowacje. Po drugie, rozproszenie systemów poszerza wektor ataku: każdą nową platformę trzeba osobno nadzorować, aktualizować, testować i zabezpieczać, co utrudnia zarządzanie podatnościami w skali całej administracji. Po trzecie, wymusza to utrzymywanie dużej liczby specjalistów w wielu instytucjach – poszczególne jednostki muszą dysponować własnym zespołem utrzymania i bezpieczeństwa, co nie tylko podnosi koszty, lecz także prowadzi do sytuacji, w której wzrost zatrudnienia w danej instytucji następuje kosztem osłabienia innej. W tym kontekście coraz wyraźniej zarysowuje się potrzeba wypracowania nowego, zintegrowanego podejścia, które z jednej strony pozwoli zachować elastyczność i sprostać specyficznym wymaganiom różnych instytucji, z drugiej zaś zapewni spójność i interoperacyjność całego podsystemu łączności państwa.

Jedną z możliwości jest przyjęcie architektury warstwowej, inspirowanej europejskimi ramami interoperacyjności[16]. W takim modelu poszczególne instytucje mogłyby nadal korzystać z właściwych interfejsów i aplikacji (np. różnych komunikatorów, platform wideokonferencyjnych czy systemów telefonii IP), lecz cała wymiana danych odbywałaby się za pośrednictwem wspólnej warstwy transportowej i semantycznej (tabela 1). Funkcje komunikacyjne byłyby odseparowane od używanego medium – ta sama rozmowa czy komunikat przechodziłyby przez sieć komórkową, światłowód, radio lub satelitę, przy zachowaniu jednolitych standardów

[16] *Europejskie Rady Interoperacyjności*, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/ia/europejskie-ramy-interoperacyjnosci [dostęp: 30 III 2026].

szyfrowania i metadanych. Kluczowe byłoby wdrożenie translatorów protokołów działających w czasie rzeczywistym, które automatycznie konwertowałyby komunikaty między różnymi formatami i protokołami bez utraty informacji o nadawcy, odbiorcy, klauzuli tajności czy priorytecie wiadomości. Uzupełnieniem tego podejścia byłyby inteligentne mechanizmy routingu, wybierające optymalny kanał transmisji w zależności od kontekstu – ważności komunikatu, dostępnych łączy, obciążenia sieci czy rodzaju urządzenia, jakim dysponuje odbiorca.

Tabela 1. Koncepcja rozwoju systemu zintegrowanej łączności państwowej.

Warstwa	Opis	Przykładowe standardy
Aplikacyjna	Narzędzia dostosowane do potrzeb instytucji	Threema OnPrem dla urzędów, Matrix dla organów bezpieczeństwa
Semantyczna	Słowniki, translatory i schematy wymiany danych	XML GovCore, JSON-LD z ontologiami EU Vocab
Transportowa	Uniwersalne protokoły szyfrowanej komunikacji	TLS 1.3, QUIC, SCIP dla głosu
Fizyczna	Neutralna technologicznie infrastruktura sieciowa	SD-WAN, 5G NSA, sieci kampusowe

Źródło: opracowanie własne.

Inspiracji dla takiego podejścia dostarczają rozwiązania wdrożone w innych państwach. Francuski system Tchap, uruchomiony w 2019 r., opiera się na otwartym, zdecentralizowanym protokole Matrix, co pozwala budować federacyjną architekturę komunikacyjną – każdy resort czy agencja może utrzymywać własny serwer, zachowując kontrolę nad danymi, a jednocześnie pozostaje w bezpiecznym kontakcie z innymi jednostkami administracji[17]. Protokół Matrix umożliwia też tworzenie tzw. mostów do innych platform (np. XMPP, IRC, Slack), co ułatwia bezpieczny kontakt z partnerami zewnętrznymi przy zachowaniu standardów bezpieczeństwa i zgodności z regulacjami, takimi jak rozporządzenie eIDAS[18]. System

[17] C. Dussutour, *French government launches in-house developed messaging service, Tchap*, European Commission, 10 XII 2021 r., https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/french-government-launches-house-developed-messaging-service-tchap [dostęp: 19 III 2026].

[18] eIDAS (ang. *Electronic IDentification, Authentication and Trust Services*) – jednolity standard identyfikacji elektronicznej i usług zaufania Unii Europejskiej działający na podstawie *Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji*

Tchap oferuje m.in. szyfrowanie end-to-end, integrację z państwowym systemem tożsamości elektronicznej oraz mechanizmy automatycznego usuwania wiadomości. Jego skuteczność została potwierdzona podczas XXXIII Letnich Igrzysk Olimpijskich w Paryżu, kiedy znacznie wzrosła liczba użytkowników, wysyłanych komunikatów i tworzonych pokoi roboczych (chatów wieloosobowych) na potrzeby koordynacji bezpieczeństwa i logistyki[19].

Kolejnym przykładem rozwiązania ukierunkowanego na bezpieczną integrację komunikacyjną rozproszonej struktury rządowej jest australijski GovLINK. System zarządzany przez Department of Finance tworzy szyfrowane środowisko wymiany informacji między agencjami federalnymi, stanowymi oraz wybranymi partnerami publicznymi i prywatnymi[20]. Bazuje na federacyjnej architekturze i wspólnych standardach bezpieczeństwa (np. S/MIME, X.509), co pozwala agencjom zachować własne systemy i równocześnie korzystać z jednolitych mechanizmów uwierzytelniania, szyfrowania i podpisu elektronicznego.

Oba przykłady pokazują, że otwarte protokoły, federacyjna architektura i mocne algorytmy kryptograficzne mogą skutecznie przezwyciężyć problem braku jednolitości systemów przy zachowaniu autonomii poszczególnych instytucji.

W polskich realiach punktem odniesienia dla takiego kierunku zmian jest projekt SBŁP. Ma on stać się wielowarstwowym, zintegrowanym systemem, nadzorowanym przez ministra właściwego do spraw wewnętrznych. System ma połączyć różne kanały komunikacyjne – od sieci stacjonarnych i radiowych, przez komórkowe, aż po satelitarne – w jedno spójne środowisko łączności administracji państwowej. Najważniejszym zadaniem SBŁP ma być zapewnienie ciągłości łączności między organami państwa zarówno w czasie pokoju, jak i w sytuacjach zagrożenia czy wojny oraz umożliwienie interoperacyjności między odrębnymi systemami cywilnymi, służb bezpieczeństwa i struktur wojskowych. Projekt zakłada wyodrębnienie kilku komponentów funkcjonalnych: SBŁP-J, SBŁP-N, SBŁP-V, SBŁP-M, SBŁP-T i SBŁP-S. Wszystkie są oparte na certyfikowanych rozwiązaniach kryptograficznych.

Istotną zaletą koncepcji SBŁP jest możliwość wykorzystania istniejącej infrastruktury, takiej jak sieci OST112 czy GovNet, zarówno dla systemów jawnych, jak i niejawnych. Pozwoliłoby to ograniczyć koszty i przyspieszyć wdrożenie systemu. Integracja z funkcjonującymi już rozwiązaniami (np. wykorzystanie systemu

elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

[19] *Tchap, the French administration federation: past, present and future - Julie Ripa*, YouTube, 29 X 2024 r., https://www.youtube.com/watch?v=m1roliPrNqc [dostęp: 19 III 2026].

[20] GovLINK, Australian Government – Department of Finance, https://www.finance.gov.au/government/whole-government-information-and-communications-technology-services/govlink [dostęp: 19 III 2026].

CATEL w komponencie SBŁP-M) zwiększy redundancję kanałów i umożliwi stopniowe przechodzenie z rozwiązań rozproszonych do bardziej spójnej architektury. Na obecnym etapie nie zostało jednak ujawnione, czy SBŁP będzie całkowicie nowym systemem projektowanym od podstaw, zbiorem zmodyfikowanych istniejących rozwiązań czy połączeniem obu podejść. Wiele wskazuje na to, że ze względów ekonomicznych i organizacyjnych może dominować podejście ewolucyjne, polegające na stopniowej integracji i unifikacji.

Planowanie i realizacja takiej transformacji wymaga podejścia etapowego. W fazie pilotażowej można zbudować fundament nowego systemu, oparty na otwartych protokołach (jak Matrix) i zintegrować z nim ograniczoną liczbę resortów, testując w praktyce mechanizmy interoperacyjności i bezpieczeństwa. Następny etap to rozszerzanie zasięgu na kolejne instytucje oraz wdrażanie translatorów protokołów dla starszych systemów, tak aby umożliwić im wymianę informacji bez konieczności natychmiastowej wymiany całej infrastruktury (np. z metadanych TETRA na standard JSON-LD lub Matrix do formatu XMPP). Równolegle należałoby prowadzić certyfikację zgodności z przyjętymi standardami bezpieczeństwa (np. ISO 27001) oraz wypracowywać wspólne polityki bezpieczeństwa, które docelowo można częściowo zautomatyzować. W perspektywie długofalowej możliwa byłaby także integracja z systemami komunikacji na poziomie Unii Europejskiej, zgodnie z promowanymi koncepcjami typu GovStack, które zakładają budowę ustandaryzowanych, modułowych komponentów możliwych do łączenia według potrzeb[21].

Korzyści z wdrożenia zintegrowanego, interoperacyjnego systemu łączności są wielowymiarowe. Poza skróceniem czasu reakcji na sytuacje kryzysowe i podniesieniem poziomu bezpieczeństwa informacji można oczekiwać znacznego obniżenia kosztów utrzymania infrastruktury oraz większej odporności na awarie i ataki. Warunkiem osiągnięcia sukcesu pozostaje jednak zachowanie równowagi – system musi być na tyle jednolity, by wszystkie instytucje mogły bezproblemowo współpracować, a jednocześnie na tyle modułowy, by można go było dostosowywać do specyficznych zadań poszczególnych użytkowników i rozwijać wraz ze zmianami technologii oraz zagrożeń. Jeśli SBŁP zostanie zaprojektowany jako otwarta, interoperacyjna platforma, a nie kolejny zamknięty system resortowy o ograniczonym zasięgu, to może stać się fundamentem nowej jakości w łączności państwowej.

[21] GovStack, https://www.govstack.global/about/ [dostęp: 19 III 2026].

Podsumowanie

Podsystem łączności administracji państwowej jest jedną z kluczowych determinant odporności państwa na współczesne zagrożenia, a jego skuteczność wynika z równoczesnego oddziaływania czterech czynników: ram prawnych, jakości procesów planowania i projektowania, dojrzałości technologicznej oraz kompetencji użytkowników. Pomimo istnienia rozbudowanej infrastruktury telekomunikacyjnej obecny system łączności nie jest w pełni zintegrowany, co prowadzi do opóźnień, dysfunkcji i zwiększenia podatności na zakłócenia w sytuacjach kryzysowych. Tym samym potwierdzona została hipoteza o niedostosowaniu obecnego systemu łączności do aktualnych zagrożeń.

W wymiarze aplikacyjnym zaproponowano model optymalizacji podsystemu łączności, w którym zróżnicowane systemy i media transmisji są integrowane przez spójne warstwy planistyczno-organizacyjne i techniczne. Model ten zakłada wykorzystanie istniejących zasobów infrastrukturalnych, ich stopniową integrację oraz nowe funkcjonalności umożliwiające automatyczne kierowanie ruchem informacyjnym różnymi kanałami, w zależności od priorytetu, wrażliwości danych i dostępności łączy. Tak ujęta modernizacja redukuje ryzyko utraty łączności w skrajnych sytuacjach oraz ogranicza koszty przez odejście od dublowania rozwiązań na rzecz świadomej konsolidacji.

W artykule doprecyzowano kryteria oceny odporności systemów łączności w kategoriach czterech komplementarnych wymiarów:

1) prawnego (zgodność i kompletność regulacji),
2) planistycznego (jakość koncepcji funkcjonalnych),
3) redundancji (zapewnienie wielotorowości komunikacji),
4) integracji (rzeczywista zdolność do współdziałania między systemami).

Ujęcie to sprzyja odejściu od uproszczonego, infrastrukturalnego spojrzenia na łączność i pozwala włączyć ją w główny nurt badań nad systemem bezpieczeństwa narodowego.

Ograniczenia badania – w szczególności brak pełnego dostępu do danych operacyjnych oraz do szczegółowych założeń rozwijanego SBŁP – wskazują na potrzebę kontynuacji prac nad empiryczną weryfikacją różnych wariantów integracji istniejących systemów. Za zasadne należy uznać zwłaszcza dalsze badania nad architekturami federacyjnymi, mechanizmami tłumaczenia protokołów i standardami wymiany danych pomiędzy podmiotami bezpieczeństwa do implementacji w systemach łączności państwowej.

Wnioski płynące z przeprowadzonych badań prowadzą do jednoznacznej konkluzji: inwestycje w cyfrową transformację i integrację systemu łączności nie są jedynie kwestią modernizacji technicznej, lecz warunkiem utrzymania realnej

zdolności operacyjnej państwa w XXI w. Implementacja przedstawionych rekomendacji może przełożyć się na skrócenie czasu reakcji administracji, służb bezpieczeństwa i ratownictwa w sytuacjach kryzysowych, co będzie miało bezpośredni wpływ na ciągłość funkcjonowania instytucji publicznych, ochronę ludności oraz zachowanie stabilności państwa w warunkach narastającej niepewności strategicznej.

Bibliografia

Bieńkowski M., *Funkcjonowanie systemu ochrony ludności w Polsce*, „Kontrola Państwowa" 2019, nr 5, s. 52–70.

Contec CMS8000 Contains a Backdoor, CISA, 2025.

Gawroński M., *Systemy teleinformatyczne wspomagania kierowania systemem bezpieczeństwa narodowego*, „Wiedza Obronna" 2014, nr 2–3, s. 47–86.

Pilżys J., *Zarządzanie systemami łączności i transmisją danych w sytuacjach kryzysowych*, „Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" 2015, t. 8, nr 1, s. 33–49.

Źródła internetowe

Drugi dzień z awarią systemu ratownictwa medycznego. Ministerstwo uspokaja, TVN24, 15 V 2021 r., https://tvn24.pl/polska/awaria-systemu-ratownictwa-medycznego-st5095494 [dostęp: 18 III 2026].

Dussutour C., *French government launches in-house developed messaging service*, *Tchap*, European Commission, 10 XII 2021 r., https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/french-government-launches-house-developed-messaging-service-tchap [dostęp: 19 III 2026].

Europejskie Rady Interoperacyjności, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/ia/europejskie-ramy-interoperacyjnosci [dostęp: 30 III 2026].

Gąsior M., *W pożarze mostu spłonęły łącza MON. Kilka instytucji bez dostępu do internetu*, naTemat, 15 II 2015 r., https://natemat.pl/133507,w-pozarze-mostu-splonely-lacza-mon-kilka-instytucji-bez-dostepu-do-internetu [dostęp: 18 III 2026].

Goldberg J., *The Trump Administration Accidentally Texted Me Its War Plans*, The Atlantic, 24 III 2025 r., https://www.theatlantic.com/politics/archive/2025/03/trump-administration-accidentally-texted-me-its-war-plans/682151/ [dostęp: 18 III 2026].

GovLINK, Australian Government – Department of Finance, https://www.finance.gov.au/government/whole-government-information-and-communications-technology-services/govlink [dostęp: 19 III 2026].

GovStack, https://www.govstack.global/about/ [dostęp: 19 III 2026].

Ogólnopolska awaria Centrum Powiadamiania Ratunkowego 112, Onet, 16 XII 2024 r., https://wiadomosci.onet.pl/kraj/awaria-centrum-powiadamiania-ratunkowego-112/bltrlw7 [dostęp: 18 III 2026].

Tchap, the French administration federation: past, present and future – Julie Ripa, YouTube, 29 X 2024 r., https://www.youtube.com/watch?v=m1roliPrNqc [dostęp: 19 III 2026].

Wanat Z., *Leaked email scandal engulfs Poland's political elite*, Politico, 24 VI 2021 r., https://www.politico.eu/article/leaked-email-scandal-engulfs-poland-political-elite-mails-hacking/ [dostęp: 18 III 2026].

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28 VIII 2014 r.).

Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (DzU z 2024 r. poz. 1907, ze zm.).

Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (DzU z 2024 r. poz. 1221, ze zm.).

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (t.j. DzU z 2025 r. poz. 825, ze zm.).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. DzU z 2025 r. poz. 194).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. DzU z 2025 r. poz. 1209).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2023 r. poz. 122, ze zm.).

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. DzU z 2025 r. poz. 504).

Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (DzU z 2017 r. poz. 1928).

Rozporządzenie Ministra Obrony Narodowej z dnia 20 kwietnia 2022 r. w sprawie działania wojskowego systemu telekomunikacyjnego (DzU z 2022 r. poz. 870).

Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (t.j. DzU z 2022 r. poz. 2065).

Inne dokumenty

ISO/IEC/IEEE 24748-1 – Systems and software engineering – Life cycle management – Part 1: Guidelines for life cycle management.

Najwyższa Izba Kontroli, *Informacja o wynikach kontroli: Organizacja i przygotowanie do działań ratowniczych na autostradach i drogach ekspresowych*, 2017 r.

PN-EN ISO/IEC 27000 –Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia, Polski Komitet Normalizacyjny.

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa z dnia 30 maja 2022 r. (DC.WFKSC.7250.1.2022), Kancelaria Prezesa Rady Ministrów, 2022 r.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, Warszawa 2020.

David Cybulski

Specjalista w dziedzinie cyberbezpieczeństwa. Doświadczenie zawodowe zdobywał na rynku prywatnym oraz w administracji państwowej. Pasjonat zagadnień związanych z innowacyjnymi rozwiązaniami z zakresu cyberbezpieczeństwa oraz nowych technik cyberataków grup APT, ze szczególnym uwzględnieniem ataków socjotechnicznych. Jego zainteresowania naukowe obejmują ochronę infrastruktury krytycznej, aktywność wybranych grup APT, tematykę bezpieczeństwa zjawiska Shadow IT oraz działania Cyber Threat Intelligence / Threat Hunting wobec wybranych grup cyberprzestępczych.

Kontakt: dcybulski@proton.me