dr inż. Marta Chodyka
Akademia Bialska im. Jana Pawła II
ORCID: 0000-0002-8819-2451
https://doi.org/10.29316/9788368103199_7

BEZPIECZEŃSTWO BAZ DANYCH JAKO ELEMENT ODPORNOŚCI CYBERNETYCZNEJ SIŁ ZBROJNYCH

DATABASE SECURITY AS AN ELEMENT OF THE CYBER RESILIENCE OF ARMED FORCES

Streszczenie

Celem rozdziału jest zbadanie roli ochrony baz danych w zapewnieniu cyberodporności sił zbrojnych. Główny problem badawczy sformułowano następująco: jak zabezpieczenie wojskowych baz danych wpływa na tę odporność? Postawiono hipotezę, że wdrożenie skutecznych mechanizmów ochrony (technicznych i organizacyjnych) istotnie wzmacnia cyberodporność sił zbrojnych. Zastosowaną metodą badawczą była jakościowa analiza literatury naukowej oraz dokumentów strategicznych dotyczących bezpieczeństwa narodowego i cyberobrony, ze szczególnym uwzględnieniem środowiska wojskowego. Analiza objęła rolę baz danych, główne cyberzagrożenia oraz kluczowe środki ochrony. Wyniki potwierdzają hipotezę – bezpieczeństwo baz danych stanowi kluczowy filar cyberodporności. Wnioski wskazują na potrzebę integracji ochrony baz danych z wojskową strategią cyberbezpieczeństwa poprzez

Summary

The aim of this chapter is to examine the role of database protection in ensuring the cyber resilience of armed forces. The main research question is: how does securing military databases influence cyber resilience? The hypothesis assumes that implementing effective technical and organizational protection mechanisms significantly strengthens the cyber resilience of armed forces. The adopted research method was a qualitative analysis of scholarly literature and strategic documents concerning national security and cyber defense, with particular emphasis on the military environment. The analysis covered the role of databases, major cyber threats, and key protection measures. The findings confirm the hypothesis – database security constitutes a fundamental pillar of cyber resilience. The conclusions emphasize the need to integrate database protection into the broader military cybersecurity strategy through the

ustanowienie wysokich standardów zabezpieczeń, ciągłe monitorowanie, szkolenie personelu i współpracę z partnerami.

Słowa kluczowe: bezpieczeństwo baz danych, cyberodporność, infrastruktura krytyczna, siły zbrojne, wielowarstwowa obrona, zagrożenia cybernetyczne

establishment of high protection standards, continuous monitoring, personnel training, and cooperation with allied partners.

Keywords: database security, cyber resilience, critical infrastructure, armed forces, defense-in-depth, cyber threats

Wstęp

Współczesne siły zbrojne funkcjonują w silnie zinformatyzowanym środowisku, w którym dane stanowią krytyczny zasób warunkujący powodzenie działań militarnych. Zapewnienie odporności cybernetycznej (cyberodporności) – rozumianej jako zdolność do przygotowania się na zakłócenia, przetrwania ataku oraz szybkiego przywrócenia sprawności systemów po incydencie – stało się jednym z kluczowych wymogów bezpieczeństwa narodowego[1]. W domenie militarnej cyberodporność przekłada się na zdolność sił zbrojnych do utrzymania ciągłości dowodzenia, łączności i realizacji zadań operacyjnych nawet w obliczu agresji w cyberprzestrzeni[2]. Organizacja Traktatu Północnoatlantyckiego NATO (ang. *North Atlantic Treaty Organization*) od kilku lat podkreśla, że odporność – zarówno na poziomie poszczególnych państw, jak i całego Sojuszu – jest warunkiem wiarygodnego odstraszania i efektywnej obrony kolektywnej[3]. Już w 2016 roku NATO wskazała odporność jako fundamentalny element strategii obronnej, określając ją mianem „*pierwszej linii obrony i odstraszania*". W tym kontekście wydano zalecenia dla państw członkowskich, nakładające obowiązek wzmacniania zdolności w zakresie zapewnienia ciągłości działania infrastruktury krytycznej oraz systemów dowodzenia. Zgodnie z art. 3 Traktatu Północnoatlantyckiego[4], każdy członek Sojuszu jest zobowiązany do rozwijania indywidualnych zdolności obronnych, co w praktyce przekłada się na konieczność podejmowania działań

[1] *Resilience as the first line of defence and deterrence*, NATO official publications, 2021.

[2] M. M. Marczyk, M. Stolarz, B. Terebiński (red.), *Cyberbezpieczeństwo: zagrożenia i wyzwania,* Mobilne sieci i systemy teleinformatyczne w cyberbezpieczeństwie Sił Zbrojnych RP, Wydawnictwo Akademii Sztuki Wojennej, Warszawa, 2023, s. 116-157.

[3] *Resilience as the first …*, op. cit.

[4] Umowa między Stronami Traktatu Północnoatlantyckiego o współpracy w dziedzinie informacji atomowych z 18.06.1964, (Dz. U. 2001.143.1594).

ukierunkowanych na ochronę kluczowych zasobów przed nowymi, często asymetrycznymi, zagrożeniami w cyberprzestrzeni[5].

Siły Zbrojne Rzeczypospolitej Polskiej, podobnie jak armie innych państw NATO, intensywnie rozwijają zdolności cyberobrony. Utworzenie wyspecjalizowanych Wojsk Obrony Cyberprzestrzeni oraz przypisanie wojsku ustawowego zadania „*ochrony i obrony cyberprzestrzeni*" państwa[6] świadczy o rosnącym znaczeniu domeny cyfrowej w systemie obronnym. Doświadczenia ostatnich dwóch dekad unaoczniły, że wojsko musi być przygotowane na zakłócenia w cyberprzestrzeni o charakterze zarówno technicznym, jak i informacyjnym[7]. Utrata dostępu do kluczowych systemów informatycznych lub kompromitacja poufnych danych może sparaliżować dowodzenie i logistykę, zagrażając bezpieczeństwu państwa. Dane od zawsze były decydującym czynnikiem na polu walki, a wyciek informacji może stanowić dla wroga ogromny sukces wywiadowczy. Właśnie dlatego bezpieczeństwo informacji – w szczególności bezpieczeństwo baz danych, które gromadzą i udostępniają te informacje – stało się integralną częścią strategii cyberbezpieczeństwa sił zbrojnych[8].

Celem niniejszego rozdziału jest określenie roli bezpieczeństwa baz danych jako kluczowego elementu budującego odporność cybernetyczną sił zbrojnych. Przedmiotem analizy jest ustalenie, w jakim zakresie oraz w jaki sposób skuteczne zabezpieczenie wojskowych baz danych wpływa na zdolność sił zbrojnych do kontynuowania operacji w warunkach zakłóceń cybernetycznych. W związku z powyższym sformułowano problem badawczy w postaci pytania: w jaki sposób skuteczne zabezpieczenie baz danych w systemach wojskowych wpływa na odporność cybernetyczną sił zbrojnych? Przyjęta hipoteza badawcza zakłada, że odpowiednie zabezpieczenie baz danych – poprzez wdrożenie adekwatnych mechanizmów technicznych oraz procedur organizacyjnych – znacząco wzmacnia odporność cybernetyczną sił zbrojnych, chroniąc kluczowe informacje przed utratą lub ingerencją oraz zapewniając ciągłość operacyjną nawet w sytuacji wystąpienia cyberataku. Innymi

[5] J. Keplin, *Budowanie odporności państwa na działania hybrydowe*, Przegląd Bezpieczeństwa Wewnętrznego, Numer 29(15), 2023, s. 13-38.

[6] B. Kuś, *Siły Zbrojne Rzeczypospolitej Polskiej a cyberbezpieczeństwo. Zagadnienia organizacyjno-prawne*, Cybersecurity & Law, nr 2, 2023, s. 32-50.

[7] M. Pollard, *A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States*, Pepperdine Policy Review: Vol. 16, Article 1, 2024.

[8] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, Warszawa 2019.

słowy, im wyższy poziom bezpieczeństwa baz danych, tym wyższa ogólna cyberodporność struktur wojskowych. W celu weryfikacji powyższej hipotezy w rozdziale przeanalizowano istniejące koncepcje odporności w cyberprzestrzeni w kontekście bezpieczeństwa narodowego, określono znaczenie baz danych dla funkcjonowania systemów wojskowych, zidentyfikowano główne zagrożenia skierowane przeciwko wojskowym bazom danych oraz dokonano oceny skuteczności wybranych środków ochrony w kontekście utrzymania ciągłości działania systemów militarnych. Dla pogłębienia analizy sformułowano także pytania pomocnicze, w tym: jakie wyzwania w zakresie bezpieczeństwa informacji wynikają ze współczesnych strategii i doktryn obronnych, jakie rodzaje ataków stanowią największe zagrożenie dla baz danych sił zbrojnych oraz które metody zabezpieczeń mają największe znaczenie z perspektywy odporności systemów wojskowych. Niniejsze opracowanie ma charakter jakościowy i koncepcyjny. Zastosowano metodę analizy treści dostępnej literatury naukowej oraz dokumentów strategicznych dotyczących bezpieczeństwa informacji i obronności. Szczególną uwagę poświęcono krajowym dokumentom takim jak, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 oraz Resortowa strategia sztucznej inteligencji do roku 2039, a także doktrynom NATO i wytycznym instytucji międzynarodowych zajmujących się cyberbezpieczeństwem, m.in. ENISA (ang. *European Union Agency for Cybersecurity*) oraz NATO CCDCOE (ang. *Cooperative Cyber Defence Centre of Excellence*). Celem przyjętej metodologii było wyodrębnienie kluczowych ram pojęciowych i teoretycznych oraz identyfikacja powtarzających się zagrożeń i postulatów dotyczących ochrony baz danych w środowisku wojskowym. Analizie poddano także wybrane przypadki incydentów cybernetycznych opisywane w dostępnej literaturze przedmiotu, które posłużyły jako ilustracja praktycznych konsekwencji niewystarczającego zabezpieczenia danych operacyjnych. Ze względu na analityczno-koncepcyjny charakter pracy wnioski sformułowano na podstawie syntezy danych wtórnych – konfrontacji ustaleń literaturowych z aktualnym kontekstem strategicznym i organizacyjnym sił zbrojnych. Takie podejście umożliwiło sformułowanie wniosków o charakterze ogólnym, odnoszących się do systemowego znaczenia bezpieczeństwa baz danych w zapewnieniu cyberodporności struktur wojskowych. Analizę prowadzono z uwzględnieniem trzech poziomów: strategicznego (strategie i doktryny bezpieczeństwa), organizacyjnego (struktury i procedury instytucji wojskowych) oraz technicznego (mechanizmy zabezpieczające i architektura systemów informacyjnych).

Odporność systemów informacyjnych

Pojęcie odporności (ang. *resilience*) w kontekście bezpieczeństwa narodowego i wojskowego zyskało na znaczeniu w ostatnich latach, znajdując odzwierciedlenie w strategiach państwowych oraz analizach akademickich. Odporność cybernetyczna najczęściej definiowana jest jako zdolność systemu lub organizacji do przygotowania się na incydenty, przetrwania ataku oraz odzyskania zdolności działania w możliwie najkrótszym czasie[9]. NATO w oficjalnych dokumentach opisuje odporność jako umiejętność „*przygotowania się, wytrwania, reagowania oraz szybkiego odzyskania sprawności po strategicznych wstrząsach i zakłóceniach*" [10]. Ujęcie to podkreśla, że odporność jest procesem wieloetapowym, obejmującym zarówno fazę prewencji (przygotowania i wzmocnienia systemów), fazę reakcji w trakcie zagrożenia, jak i fazę odbudowy po incydencie.

W literaturze przedmiotu wskazuje się, że odporność stanowi kluczowy element nowoczesnej koncepcji odstraszania i obrony[11]. Rozumiana jako gotowość państwa, sprawność organizacyjna oraz przygotowanie infrastruktury krytycznej, stanowi fundament skutecznej reakcji na działania poniżej progu wojny – w tym zagrożenia cybernetyczne i dezinformację. Analizy NATO oraz niezależnych ośrodków badawczych potwierdzają, że odporność cybernetyczna systemów dowodzenia i łączności wymaga wdrażania strategii wielowarstwowej obrony oraz redundancji, które pozwolą na utrzymanie funkcji operacyjnych mimo zakłóceń[12]. Odporność nie polega na całkowitej niewrażliwości systemu, lecz na zdolności ograniczania skutków ataku i szybkiego odzyskania sprawności działania[13].

W kontekście sił zbrojnych szczególne znaczenie przypisuje się ciągłości działania systemów dowodzenia, łączności oraz ochronie danych operacyjnych. Koncepcja *mission assurance* zakłada konieczność zabezpieczenia

[9] M. P. Sallos, A. Garcia Perez, A. Bocanet, *Organisational cyber resilience: a heuristic for bridging foundations and applications*, Journal of Enterprise Information Management, 37(6), 2024, s. 1926-1952.

[10] *Resilience as the first …*, op. cit.

[11] J. P. Yaacoub, H. Noura, O. Salman, A, Chehab, *Security analysis of drones systems: Attacks, limitations, and recommendations*, Internet of Things, 11, 100218, 2020.

[12] A. Afina, R. Inverarity, B. Unal, *Cyber Resilience in NATO Command and Control Systems*. London: Chatham House, 2020.

[13] *Allied Command Transformation (ACT)*, Cyber Resilience Strategic Concept. Norfolk, VA, 2023.

wszystkich krytycznych komponentów infrastruktury wojskowej – w tym baz danych – przed różnymi typami zagrożeń. W literaturze krajowej zwraca się uwagę, że cyberbezpieczeństwo państwa obejmuje nie tylko ochronę systemów teleinformatycznych, ale także danych w nich przetwarzanych – co jednoznacznie wiąże ochronę baz danych z cyberodpornością narodową[14]. Równocześnie postuluje się dostosowanie systemu prawnego oraz struktur organizacyjnych sił zbrojnych do nowych wyzwań w domenie cyber[15].

Od strony technicznej, bezpieczeństwo baz danych było analizowane od dawna w kontekście informatyki i kryptografii, jednak dopiero niedawno pojawiły się badania poświęcone ich roli w środowisku militarnym[16]. Kluczowe cele bezpieczeństwa danych określane są w literaturze jako triada CIA – *Confidentiality*, *Integrity*, *Availability* – a w kontekście wojskowym poszerza się je o autentyczność i niezaprzeczalność informacji[17]. Przegląd aktualnych raportów pokazuje, że ataki ukierunkowane na wojskowe systemy informacyjne, w tym bazy danych, mogą skutkować naruszeniem każdego z tych atrybutów, zagrażając poufności danych operacyjnych, integralności komunikacji oraz dostępności zasobów w czasie rzeczywistym. W odpowiedzi na te wyzwania, zarówno w Stanach Zjednoczonych, jak i w Polsce, rozpoczęto działania mające na celu określenie strategii rozwoju sztucznej inteligencji w środowisku militarnym, w tym w kontekście ochrony danych. Raport GAO[18] szczegółowo analizuje stan rozwoju zdolności związanych z AI w systemach uzbrojenia, zwracając uwagę na potrzebę zapewnienia niezawodności i bezpieczeństwa komponentów informacyjnych, takich jak bazy danych. Z kolei polska „*Resortowa strategia sztucznej inteligencji do roku 2039"* opracowana przez MON[19] wskazuje kierunki rozwoju sztucznej inteligencji w Siłach Zbrojnych RP,

[14] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, Warszawa 2019.

[15] W. Kitler, K. Chałubińska-Jentkiewicz, K. Badźmirowska-Masłowska, *System bezpieczeństwa w cyberprzestrzeni RP*, Towarzystwo Wiedzy Obronnej, Warszawa 2018.

[16] H. Ahmad, I. Dharmadasa, F. Ullah, M. A. Babar, *A Review on C3I Systems' Security: Vulnerabilities, Attacks, and Countermeasures*, arXiv preprint arXiv:2104.11906, 2021 oraz A. Singh, *Military Computing Security: Insights and Implications*, Journal of Institution of Engineers (India): Series B, 104(3), 2023, s. 359-366.

[17] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2024.

[18] *Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon System*s, GAO-24-106221, Washington, DC: U.S. Government Accountability Office, 2024.

[19] *Resortowa strategia sztucznej inteligencji do roku 2039*, Ministerstwo Obrony Narodowej, Warszawa, 2020.

uwzględniając ochronę infrastruktury informacyjnej jako elementu cyberodporności systemów obronnych.

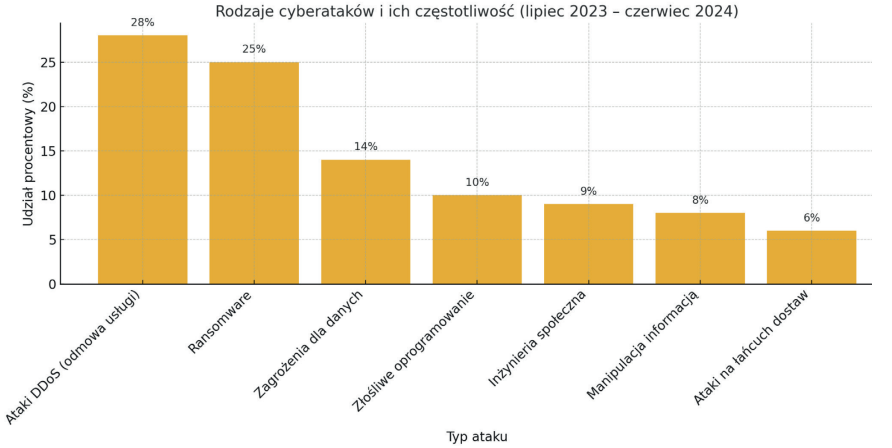
Podsumowując, dotychczasowe badania oraz dokumenty strategiczne jednoznacznie wskazują, że cyberodporność jest warunkiem sprawnego działania struktur państwowych i wojskowych w środowisku pełnym dynamicznych zagrożeń, a ochrona baz danych jako elementu krytycznej infrastruktury informacyjnej powinna stanowić jeden z priorytetów systemów bezpieczeństwa narodowego. Ujęcie to znajduje odzwierciedlenie zarówno w analizach międzynarodowych, takich jak raport GAO, jak i w krajowych dokumentach strategicznych, które wskazują na konieczność kompleksowego podejścia do bezpieczeństwa danych w środowisku operacyjnym oraz uwzględnienia specyfiki wojskowych systemów informacyjnych przy projektowaniu mechanizmów ochronnych.

Znaczenie baz danych w systemach wojskowych

Bazy danych stanowią strategiczny komponent systemów informacyjnych współczesnych sił zbrojnych, odgrywając zasadniczą rolę w planowaniu, prowadzeniu oraz zabezpieczaniu operacji militarnych. Ich znaczenie wynika nie tylko z funkcji przechowywania i przetwarzania informacji, lecz także z roli, jaką odgrywają w zapewnianiu ciągłości dowodzenia i wsparcia decyzyjnego w warunkach konfliktu zbrojnego. Bazy te obejmują zbiory danych personalnych, operacyjnych, logistycznych, technicznych, a także dane związane z rozpoznaniem i analizą zagrożeń.

W dobie rosnącej cyfryzacji sfery militarnej systemy bazodanowe stają się celem ataków ze strony zorganizowanych podmiotów – w tym grup przestępczych, cyberaktywistów oraz tzw. trwałych zagrożeń zaawansowanych (ang. *Advanced Persistent Threats*, APT)[20], często powiązanych z interesami państwowymi. Dane przedstawione w *ENISA Threat Landscape 2024* wskazują, że w okresie od lipca 2023 do czerwca 2024 zagrożenia dla dostępności systemów, *ransomware* oraz ataki na dane stanowiły trzy najczęściej odnotowywane formy ataków cybernetycznych. Łącznie odpowiadały one za ponad połowę wszystkich incydentów. Zestawienie tych danych prezentuje rysunek 1, który ilustruje udział procentowy poszczególnych typów ataków w globalnym krajobrazie zagrożeń.

[20] T. Wrightson, *Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization,* McGraw Hill, 2024.



Rysunek 1. Rodzaje cyberataków i ich częstotliwość (lipiec 2023 – czerwiec 2024)
Źródło: opracowanie własne na podstawie: European Union Agency for Cybersecurity (ENISA)[21].

Co istotne, ataki typu DDoS (ang. *Distributed Denial of Service*) po raz pierwszy wyprzedziły *ransomware* pod względem liczby przypadków, wskazując na zmianę dominujących strategii przeciwników. Znaczący udział ataków ukierunkowanych na systemy bazodanowe potwierdza konieczność traktowania ochrony danych jako jednego z priorytetów strategicznych w ramach bezpieczeństwa informacyjnego sił zbrojnych. Bazy danych stały się nie tylko celem ataków szyfrujących (np. *ransomware*), ale również areną operacji dezinformacyjnych, kradzieży informacji (*infostealerów*), sabotażu integralności danych oraz działań wykorzystujących techniki ukrywania się w infrastrukturze chmurowej i kanałach komunikacyjnych (np. *Slack, Telegram*). Warto także odnotować rosnącą rolę manipulacji informacjami z użyciem sztucznej inteligencji oraz wykorzystywanie inżynierii społecznej do kompromitacji zaufanych projektów *open source*. Oznacza to, że zagrożenia wobec baz danych nie ograniczają się jedynie do aspektów technicznych, ale obejmują również wymiar socjotechniczny i geopolityczny. Zróżnicowanie metod ataku wymusza stosowanie kompleksowych i wielowarstwowych mechanizmów zabezpieczeń, obejmujących zarówno szyfrowanie i segmentację dostępu, jak i monitoring aktywności, testowanie podatności, audyty oraz szkolenia personelu. Tylko zintegrowane podejście może zapewnić odpowiedni poziom cyberodporności struktur wojskowych wobec zmieniającego się krajobrazu zagrożeń.

[21] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2024*, 2024.

Współczesne zagrożenia wobec wojskowych baz danych przybierają charakter wielowymiarowy i coraz częściej wpisują się w szerszy kontekst kampanii hybrydowych prowadzonych przez aktorów państwowych oraz zorganizowane grupy cyberprzestępcze. Analiza danych zawartych w raporcie *ENISA Threat Landscape* 2024[22] pozwala na identyfikację dominujących trendów w zakresie ataków wymierzonych w strategiczne zasoby informacyjne, w tym w szczególności w systemy bazodanowe, pełniące kluczową rolę w infrastrukturze dowodzenia, rozpoznania, logistyki i analizy operacyjnej sił zbrojnych.

Jednym z fundamentalnych typów zagrożeń pozostają ataki aplikacyjne, w tym przede wszystkim wstrzykiwanie zapytań w języku strukturalnym (*SQL Injection*), które umożliwiają nieautoryzowany dostęp do danych, ich modyfikację lub trwałe usunięcie. Mechanizm tego rodzaju ataku polega na wprowadzeniu do aplikacji danych wejściowych w taki sposób, aby zostały one przetworzone jako część instrukcji SQL, co prowadzi do wykonania niezamierzonych operacji w bazie danych. W kontekście wojskowym, skuteczny atak typu *SQL Injection* może doprowadzić do kompromitacji informacji niejawnych, ujawnienia parametrów uzbrojenia lub lokalizacji jednostek operacyjnych, co stanowi poważne zagrożenie dla bezpieczeństwa narodowego[23]. Równolegle obserwuje się wzrost liczby incydentów wykorzystujących podatności typu zero-day oraz techniki ataków na komponenty pośredniczące, takie jak biblioteki mapowania obiektowo-relacyjnego czy *frameworki* interfejsów API. Tego rodzaju luki, zanim zostaną zidentyfikowane i załatane przez producentów, stają się wektorem wejściowym dla ataków ukierunkowanych, często inicjowanych przez wyspecjalizowane grupy APT (ang. *Advanced Persistent Threats*). Szczególnie niebezpieczne są ataki wykorzystujące połączenie podatności i socjotechniki, które umożliwiają trwałą infiltrację systemów oraz eskalację uprawnień w infrastrukturze wojskowe[24]. Kolejną kategorią zagrożeń są incydenty z wykorzystaniem złośliwego oprogramowania, zwłaszcza typu *ransomware* i tzw. *wipery* (ang. *data-wiping malware*). *Ransomware* prowadzi do zaszyfrowania zasobów informacyjnych i wymuszenia okupu za ich odszyfrowanie, co może sparaliżować operacje wojskowe poprzez utratę dostępu do danych rozpoznawczych, planistycznych czy logistycznych. *Wipery* natomiast – podszywające się pod *ransomware* – realizują trwałe uszkodzenie danych,

[22] European Union Agency for Cybersecurity (ENISA)*, ENISA Threat Landscape 2024*, 2024.

[23] J. Clarke, *SQL Injection Attacks and Defense*, Syngress, 2012.

[24] R. Rais, C. Morillo, E. Gilman, D. Barth, *Zero Trust Networks: Building Secure Systems in Untrusted Network*, 2nd Edition, Helion, Gliwice 2024.

często w sposób nieodwracalny, służąc jako narzędzie sabotażu informacyjnego w ramach działań kinetycznych i niekinetycznych. Oprogramowanie tego typu coraz częściej wykorzystuje techniki *Living Off the Land* (LOTL) i *Living Off Trusted Sites* (LOTS), operując w ramach zaufanych usług chmurowych lub kanałów komunikacyjnych (np. *Slack, Telegram*), co znacząco utrudnia jego detekcję i eliminację[25]. Niemniej istotnym zagrożeniem są ataki na integralność danych, prowadzone w sposób ukryty i trudny do wykrycia. Przeciwnik, który uzyska dostęp do systemu, może dokonać subtelnej modyfikacji danych operacyjnych, technicznych lub rozpoznawczych – np. zmieniając współrzędne celów, charakterystyki uzbrojenia lub parametry logistyczne. Efektem takich działań może być błędne decyzje dowódcze podejmowane na podstawie zmanipulowanej informacji. Skuteczna ochrona integralności wymaga wdrożenia polityki audytów, systemów wykrywania anomalii oraz stosowania mechanizmów spójności danych i zasady ograniczonego dostępu (ang. *least privilege*). Zagrożenia wewnętrzne (ang. *insider threats*), czyli działania podejmowane przez osoby posiadające autoryzowany dostęp do infrastruktury, stanowią kolejny istotny wektor ataku. Tego rodzaju incydenty są trudne do wykrycia ze względu na legalność dostępu oraz często brak jednoznacznych wskaźników naruszenia. Pomimo ich niskiej reprezentacji w statystykach, potencjalne skutki takich działań są katastrofalne, szczególnie gdy dotyczą systemów dowodzenia i kontroli. W ujęciu strategicznym, wojskowe bazy danych stają się celem kampanii prowadzonych przez grupy powiązane z wywiadem obcych państw, realizujących długotrwałą infiltrację środowisk informacyjnych. Działania te charakteryzują się wysokim stopniem ukrycia, wykorzystaniem szyfrowanej komunikacji, tunelowaniem danych oraz przechwytywaniem informacji poprzez kanały nieobjęte monitoringiem. Tego typu operacje są często trudne do wykrycia bez zastosowania zaawansowanych narzędzi klasy SIEM, DAM czy UEBA. W odpowiedzi na ewoluujące zagrożenia, raport ENISA rekomenduje wdrażanie modelu obrony warstwowej (ang. *defense-in-depth*), który uwzględnia nie tylko zabezpieczenia techniczne i kryptograficzne, ale również aspekty organizacyjne, szkoleniowe oraz proceduralne. Szczególny nacisk położony jest na rozwój odporności poprzez segmentację sieci, monitorowanie aktywności użytkowników, regularne audyty, szyfrowanie danych, a także testowanie odporności systemów na złożone scenariusze ataków – zarówno symulowane, jak i rzeczywiste.

[25] M. Sikorski, A. Honig, *Praktyczna Analiza Malware*. Przewodnik po usuwaniu złośliwego oprogramowania, Wydawnictwo Naukowe PWN, Warszawa 2021.

Współczesne ataki na wojskowe systemy informacyjne często przybierają postać złożonych kampanii, realizowanych zgodnie z koncepcją łańcucha ataku (ang. *kill chain*)[26]. Tego rodzaju działania są szczególnie charakterystyczne dla trwałych zagrożeń zaawansowanych (APT), które w sposób systematyczny prowadzą kampanie cyberszpiegowskie przeciwko instytucjom wojskowym. Podział ataku na poszczególne fazy pozwala na lepsze zrozumienie jego struktury i identyfikację potencjalnych punktów przeciwdziałania. Etapy złożonego ataku na bazę danych przedstawiona została w tabeli 1.

Tabela 1. Etapy złożonego ataku na bazę danych (model łańcucha ataku)

Faza	Opis działań
1. Rekonesans	Identyfikacja celu ataku (np. administratora systemu) oraz zebranie informacji przy użyciu metod z ogólnodostępnych źródeł (ang. *Open Source Intelligence*, OSINT).
2. Przekazanie	Dostarczenie złośliwego kodu, zwykle za pomocą ataku ukierunkowanego typu *spear phishing*.
3. Wykorzystanie	Uruchomienie podatności w oprogramowaniu (np. *exploit* przeglądarki lub klienta bazy danych).
4. Instalacja	Implementacja złośliwego oprogramowania (np. trojan zdalnego dostępu ang. Remote Access Trojan, RAT) na stacji roboczej ofiary.
5. Komunikacja (C2)	Nawiązanie kanału dowodzenia (ang. *Command and Control*, C2) i sterowanie zainfekowanym systemem.
6. Eskalacja	Uzyskanie wyższych uprawnień, ruch lateralny w sieci, przejęcie dodatkowych urządzeń i serwerów.
7. Działania końcowe	Eksfiltracja danych lub ich sabotaż (np. modyfikacja, usunięcie, zaszyfrowanie).

Źródło: opracowanie własne.

Każdy z wymienionych etapów może wykorzystywać odmienne techniki ataku i wymaga odmiennych mechanizmów detekcji oraz reakcji. Dla przykładu, faza rekonesansu może być ograniczona przez zastosowanie polityki ograniczonego ujawniania struktur organizacyjnych, faza dostarczenia – przez filtrowanie wiadomości i edukację personelu, faza wykorzystania – przez aktualizację i *hardening* systemów, a działania końcowe – przez zastosowanie mechanizmów audytu i monitoringu aktywności w bazie danych. Złożoność tych ataków polega na ich zdolności do ukrywania obecności intruza w systemie przez długi czas. Często wykorzystują one złośliwe oprogramowanie typu bezplikowego (ang. *fileless malware*), techniki tunelowania danych, ukrywanie zapytań w legalnym

[26] J. Dimaggio, *Art Of Cyberwarfare, An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime*, No Starch Press,US, 2022.

ruchu sieciowym, a także eksfiltrację poprzez kanały trudne do wykrycia[27]. Konsekwencją tego jest znaczne wydłużenie tzw. czasu wykrycia (ang. *dwell time*), który w środowisku militarnym może oznaczać realne zagrożenie dla bezpieczeństwa państwa. Wnioski płynące z analizy modelu łańcucha ataku pokazują, że skuteczne przeciwdziałanie wymaga nie tylko technologii, lecz także procedur organizacyjnych i odpowiednio przeszkolonego personelu. Tylko podejście wielowarstwowe – obejmujące edukację użytkowników, detekcję zagrożeń, mechanizmy prewencji i strategię reakcji – może zapewnić odporność systemów wojskowych baz danych na współczesne zagrożenia cybernetyczne.

Kluczowe środki ochrony baz danych w kontekście cyberodporności

Zabezpieczenie wojskowych systemów bazodanowych stanowi jeden z kluczowych elementów budowania odporności cybernetycznej sił zbrojnych. Wymaga to wdrożenia kompleksowej architektury ochronnej, która obejmuje mechanizmy techniczne, proceduralne oraz organizacyjne[28]. Poniższe środki zabezpieczające uznaje się za fundamentalne z punktu widzenia odporności informacyjnej systemów militarnych:

1) Kontrola dostępu i zarządzanie tożsamością. Efektywne zarządzanie dostępem do baz danych wymaga bezwzględnego przestrzegania zasady ograniczonego dostępu do informacji (ang. *need-to-know*). Oznacza to konieczność wdrożenia mechanizmów uwierzytelniania wieloskładnikowego (ang. *Multi-Factor Authentication*, MFA) oraz scentralizowanych systemów zarządzania tożsamościami i uprawnieniami (ang. *Identity and Access Management*, IAM). Ponadto, serwery baz danych powinny być umieszczone w wyodrębnionych segmentach sieci (np. strefie buforowej, ang. *Demilitarized Zone*, DMZ), z dostępem jedynie z poziomu zaufanych węzłów administracyjnych (tzw. serwerów pośredniczących, ang. *jump servers*). Obowiązkiem administratorów jest również cykliczna weryfikacja i audyt uprawnień użytkowników, zgodnie z zasadą minimalnego zakresu uprawnień (ang. *least privilege*).
2) Szyfrowanie danych w spoczynku i transmisji. Zastosowanie algorytmów kryptograficznych jest nieodzownym elementem ochrony poufności

[27] M. Serafin, *Bezpieczeństwo sieci firmowej. Kontrola ruchu wychodzącego*, Helion, Gliwice 2022.

[28] M. Kowalewski, Ochrona informacji i systemów teleinformatycznych w cyberprzestrzeni, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2017.

danych zarówno w stanie spoczynku (ang. *data at rest*), jak i w trakcie transmisji (ang. *data in transit*). Zalecane jest stosowanie szyfrowania na poziomie plików oraz transmisji sieciowej z użyciem protokołów bezpiecznych, takich jak *Transport Layer Security* (TLS). Dla zwiększenia bezpieczeństwa operacyjnego, mechanizmy szyfrowania powinny być zgodne ze standardami zatwierdzonymi dla środowisk o znaczeniu strategicznym (np. FIPS 140-2) i wspierane przez sprzętowe moduły zarządzania kluczami (ang. *Hardware Security Modules*, HSM). Ochronie szyfrowaniem powinny podlegać również kopie zapasowe, przechowywane poza główną infrastrukturą operacyjną.

3) Monitorowanie i detekcja anomalii. Rozbudowane mechanizmy monitorowania są konieczne do identyfikacji prób naruszeń bezpieczeństwa. Systemy klasy *Database Activity Monitoring* (DAM) umożliwiają bieżące śledzenie i analizę operacji wykonywanych na bazach danych, wykrywając m.in. nietypowe zapytania, próby eskalacji uprawnień, czy masowe eksporty danych[29]. Komplementarnie, narzędzia *Security Information and Event Management* (SIEM) oraz struktury *Security Operations Center* (SOC) pozwalają na korelację zdarzeń w skali całej organizacji i skracają czas identyfikacji obecności nieautoryzowanego podmiotu w infrastrukturze (tzw. *dwell time*). W jednostkach wojskowych zaleca się funkcjonowanie zespołów szybkiego reagowania na incydenty (ang. *Computer Security Incident Response Team*, CSIRT), pełniących funkcję ciągłego nadzoru.
4) Redundancja i kopie zapasowe. Zdolność do przywrócenia ciągłości funkcji operacyjnych wymaga prowadzenia regularnej polityki tworzenia kopii zapasowych danych, realizowanej według modelu 3-2-1 (trzy kopie, na dwóch różnych nośnikach, jedna poza główną lokalizacją – *off-site*). Kopie te powinny być izolowane od sieci operacyjnej, co zabezpiecza je przed atakami typu *ransomware*. Ponadto rekomendowane jest wdrożenie architektury wysokiej dostępności, z replikacją danych do centrów zapasowych, przy użyciu mechanizmów automatycznego przełączenia węzła (ang. *failover*). Tego typu redundancja pełni funkcję zarówno technicznej ochrony zasobów, jak i psychologicznego odstraszania przeciwnika, redukując spodziewaną skuteczność ataku.

[29] J. Bandler, A Merzon, *Cybercrime Investigations A Comprehensive Resource for Everyone*, Taylor & Francis Ltd, 2022.

5) Zarządzanie podatnościami i twarda konfiguracja. Zapewnienie zgodności systemu bazodanowego z wymaganiami bezpieczeństwa obejmuje stosowanie procedur aktualizacji (ang. *patch management*) oraz tzw. twardej konfiguracji (ang. *hardening*). Zaleca się okresowe stosowanie list kontrolnych opartych o wytyczne organizacji takich jak Departament Obrony Stanów Zjednoczonych (np. *Security Technical Implementation Guides* – STIG) czy Sojusz Północnoatlantycki (*Baseline Security Requirements*). Praktyki te obejmują m.in. dezaktywację nieużywanych funkcjonalności, filtrowanie portów, rotację kluczy kryptograficznych oraz wdrożenie polityk silnych haseł.
6) Szkolenie i standaryzacja działań personelu. Czynniki ludzkie pozostają jednym z najistotniejszych obszarów ryzyka dla systemów informacyjnych. Stąd kluczowe znaczenie ma systematyczne prowadzenie szkoleń i ćwiczeń z zakresu ochrony danych, w tym symulacji zagrożeń typu *phishing* oraz reagowania na incydenty. Siły zbrojne winny wdrażać instytucjonalne programy podnoszenia świadomości zagrożeń cybernetycznych oraz rozwijać kompetencje administratorów i operatorów systemów. Polityki bezpieczeństwa muszą jasno określać reguły postępowania, obowiązki personelu oraz procedury eskalacji incydentu. Przykładem dobrych praktyk w tym zakresie są ćwiczenia NATO *Locked Shields*, które umożliwiają praktyczne sprawdzenie gotowości struktur obronnych wobec realnych scenariuszy zagrożeń[30]. *Locked Shields* to największe na świecie ćwiczenia typu „live-fire" w zakresie cyberobrony, organizowane przez Centrum Doskonałości NATO ds. Współpracy w Zakresie Cyberobrony, (ang. *Cooperative Cyber Defence Centre of Excellence*, NATO CCDCOE). Uczestnicy – zespoły z różnych państw – muszą chronić systemy teleinformatyczne oraz krytyczną infrastrukturę fikcyjnego państwa przed złożonymi i zsynchronizowanymi atakami przeprowadzanymi przez zespół agresora, co pozwala im doskonalić zarówno umiejętności techniczne, jak i koordynację operacyjną w warunkach zbliżonych do rzeczywistych[31].

Skuteczna ochrona zasobów informacyjnych wymaga jednak nie tylko wdrażania pojedynczych środków zabezpieczających, lecz również ich uporządkowania w ramach kompleksowego, wielowarstwowego modelu obrony. Takie podejście umożliwia zintegrowane zarządzanie ryzykiem oraz zwiększa

[30] NATO CCDCOE, *Locked Shields – The World's Largest and Most Complex International Live-Fire Cyber Defence Exercise,* 2025.

[31] Locked Shields, https://ccdcoe.org/locked-shields/, [dostęp: 02.03.2025].

odporność infrastruktury na złożone, wieloetapowe ataki. Warstwowy model ochrony baz danych w systemie cyberodporności sił zbrojnych przedstawiony został na rysunku 2.



Rysunek 2. Warstwowy model ochrony baz danych w systemie cyberodporności sił zbrojnych
Źródło: opracowanie własne.

Każdy z przedstawionych środków ochronnych pełni określoną funkcję w warstwowym modelu bezpieczeństwa. Ich synergiczne wdrożenie prowadzi do znaczącego zwiększenia odporności organizacyjnej sił zbrojnych na zakłócenia w domenie informacyjnej. Ochrona baz danych jako zasobu o charakterze krytycznym, musi zostać osadzona w szerszym systemie zarządzania bezpieczeństwem informacyjnym, odpowiadającym aktualnym zagrożeniom oraz specyfice środowiska wojskowego.

Podsumowanie

W świetle przeprowadzonych analiz można stwierdzić, że bezpieczeństwo baz danych stanowi fundamentalny element budowania cyberodporności sił zbrojnych. Chroniąc krytyczne informacje i zapewniając ciągłość działania w warunkach cyberzagrożeń, efektywne zabezpieczenie wojskowych baz danych bezpośrednio przekłada się na zdolność armii do przetrwania ataków oraz szybkiego odtworzenia gotowości operacyjnej po incydencie. Wyniki

pracy potwierdziły postawioną hipotezę – wdrożenie skutecznych mechanizmów ochrony baz danych znacząco wzmacnia odporność cybernetyczną organizacji wojskowych. Jednocześnie wykazano, że zagrożenia skierowane przeciwko bazom danych mają charakter wielowymiarowy (od klasycznych ataków aplikacyjnych, poprzez ataki socjotechniczne, aż po zaawansowane, wieloetapowe operacje APT finansowane przez państwa), co oznacza, że nie istnieje jedno rozwiązanie gwarantujące pełne bezpieczeństwo. Wymagana jest kompleksowa, wielowarstwowa strategia obrony, łącząca aspekty techniczne, proceduralne i organizacyjne, aby zminimalizować ryzyko naruszeń na każdym etapie ataku i zapewnić odporność systemów informacyjnych. W trakcie badań zidentyfikowano kluczowe obszary zabezpieczenia wojskowych baz danych, które powinny funkcjonować w sposób komplementarny. Do fundamentalnych środków ochrony należą przede wszystkim: ścisła kontrola dostępu i zarządzanie tożsamością użytkowników (m.in. zasada najmniejszych uprawnień, uwierzytelnianie wieloskładnikowe, segmentacja sieci i odseparowanie serwerów baz danych), szyfrowanie danych w spoczynku i podczas transmisji zgodnie z najwyższymi standardami kryptograficznymi, rozbudowane mechanizmy monitorowania aktywności i detekcji anomalii (np. systemy klasy SIEM/DAM oraz zespoły szybkiego reagowania CSIRT), a także zapewnienie redundancji i regularne tworzenie izolowanych kopii zapasowych. Istotnym elementem jest również ciągłe zarządzanie podatnościami i twarda konfiguracja systemów (regularne aktualizacje, audyty bezpieczeństwa, zgodność ze standardami typu STIG), uzupełniane przez systematyczne szkolenie personelu oraz standaryzację procedur. Synergiczne wdrożenie tych zróżnicowanych środków tworzy warstwowy system ochrony, który skutecznie podnosi odporność całej infrastruktury informacyjnej – nawet jeśli pojedynczy mechanizm zawiedzie, pozostałe elementy mogą zapobiec eskalacji incydentu i utrzymać kluczowe funkcje operacyjne. Uzyskane wyniki mają istotne znaczenie praktyczne dla kształtowania polityki cyberbezpieczeństwa w sektorze obronnym. Przede wszystkim wskazują na potrzebę trwałej integracji ochrony baz danych z szerszą strategią cyberobrony sił zbrojnych. Rekomenduje się, aby bezpieczeństwo danych zostało uwzględnione w doktrynach i planach operacyjnych jako jeden z priorytetów obrony infrastruktury krytycznej. Planowanie i rozwój systemów wojskowych powinny obejmować ustanowienie wysokich standardów zabezpieczeń (zarówno technologicznych, jak i proceduralnych), wdrożenie stałego monitoringu zagrożeń i mechanizmów wczesnego ostrzegania, regularne szkolenia specjalistyczne oraz ćwiczenia symulacyjne,

a także ścisłą współpracę z partnerami (np. w ramach sojuszniczych platform wymiany informacji o incydentach czy ćwiczeń, takich jak Locked Shields). Takie holistyczne podejście zapewni, że ochrona baz danych nie będzie odizolowanym wysiłkiem, lecz częścią zintegrowanego systemu odporności cybernetycznej armii. Ze względu na analityczno-koncepcyjny charakter badań, wnioski mają charakter uogólniony i wskazują kierunki działań, wymagając dalszego pogłębienia w przyszłych pracach. Warto podkreślić, że brak empirycznej weryfikacji stanowi naturalne ograniczenie niniejszego studium – stąd pożądane są dalsze badania ukierunkowane na praktyczne sprawdzenie sformułowanych postulatów. Zasadne byłoby przeprowadzenie pogłębionych analiz przypadków rzeczywistych incydentów skierowanych przeciw bazom danych sił zbrojnych oraz symulacji ataków w kontrolowanych warunkach, aby ilościowo ocenić skuteczność poszczególnych mechanizmów obronnych. Kolejnym kierunkiem badań powinno być dostosowanie proponowanych środków ochrony do rozwijających się technologii – takich jak, sztuczna inteligencja czy komputery kwantowe – oraz do ewoluujących wektorów ataku. Kontynuacja badań nad odpornością cybernetyczną wojskowych baz danych, połączona z wymianą doświadczeń między jednostkami naukowymi a instytucjami obronnymi, przyczyni się do dalszego doskonalenia zdolności ochrony informacji w siłach zbrojnych.

Podsumowując, bezpieczeństwo baz danych to nie tylko kwestia techniczna, ale strategiczny czynnik determinujący zdolność armii do działania w obliczu współczesnych zagrożeń – jego wzmacnianie powinno być stałym elementem rozwoju systemu obronnego państwa.

Literatura

1. Afina, A.,Inverarity, R.,Unal, B., *Cyber Resilience in NATO Command and Control Systems*. London: Chatham House, 2020.
2. Ahmad, H., Dharmadasa, I., Ullah, F., Babar, M. A., *A Review on C3I Systems' Security: Vulnerabilities, Attacks, and Countermeasures*, ACM Computing Surveys, 55(9), 2021, s. 1-38. https://doi.org/10.1145/3558001
3. Bandler, J., Merzon, A., *Cybercrime Investigations A Comprehensive Resource for Everyone*, Taylor & Francis Ltd, 2022.
4. Clarke, J., *SQL Injection Attacks and Defense*, Syngress, 2012.
5. Dimaggio, J., *Art of Cyberwarfare, An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime*, No Starch Press,US, 2022.
6. Keplin, J., *Budowanie odporności państwa na działania hybrydowe*, Przegląd Bezpieczeństwa Wewnętrznego, nr 29(15), 2023, s. 13-38. https://doi.org/10.4467/20801335PBW.23.018.18760

7. Kitler, W., Chałubińska-Jentkiewicz, K., Badźmirowska-Masłowska, K., *System bezpieczeństwa w cyberprzestrzeni RP*, Towarzystwo Wiedzy Obronnej, 2018.
8. Kowalewski, M., Ochrona informacji i systemów teleinformatycznych w cyberprzeni, Oficyna Wydawnicza Politechniki Warszawskiej, 2017.
9. Kuś, B., *Siły Zbrojne Rzeczypospolitej Polskiej a cyberbezpieczeństwo. Zagadnienia organizacyjno-prawne*, Cybersecurity & Law, nr 2, 2023, s. 32-50.
10. Marczyk, M.M., Stolarz, M., Terebiński, B. (red.), *Cyberbezpieczeństwo: zagrożenia i wyzwania,* Mobilne sieci i systemy teleinformatyczne w cyberbezpieczeństwie Sił Zbrojnych RP, Wydawnictwo Akademii Sztuki Wojennej, Warszawa, 2023, s. 116-157.
11. Pollard, M., *A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States*, Pepperdine Policy Review: Vol. 16, Article 1, 2024.
12. Rais, R., Morillo, C., Gilman, E., Barth, D., *Zero Trust Networks: Building Secure Systems in Untrusted Network, 2nd Edition*, Helion, 2024.
13. Sallos, M.P., Garcia Perez, A., Bocanet, A., *Organisational cyber resilience: a heuristic for bridging foundations and applications*, Journal of Enterprise Information Management, 37(6), 2024, s. 1926-1952. https://doi.org/10.1108/JEIM-06-2023-0317
14. Serafin, M., *Bezpieczeństwo sieci firmowej. Kontrola ruchu wychodzącego*, Helion, 2022.
15. Sikorski, M., Honig, A., *Praktyczna Analiza Malware. Przewodnik po usuwaniu złośliwego oprogramowania*, Wydawnictwo Naukowe PWN, 2021.
16. Singh, A., *Military Computing Security: Insights and Implications*, Journal of Institution of Engineers (India): Series B, 104(3), 2023, s. 359-366.
17. Wrightson, T., *Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization,* McGraw Hill, 2024.
18. Yaacoub, J.P., Noura, H.,Salman, O., Chehab, A., *Security analysis of drones systems: Attacks, limitations, and recommendations*, Internet of Things,11, 2020, 100218. https://doi.org/10.1016/j.iot.2020.100218
19. European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2024, 2024.
20. GAO, *Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon System*s, GAO-24-106221, Washington, DC: U.S. Government Accountability Office, 2024.
21. Ministerstwo Obrony Narodowej, *Resortowa strategia sztucznej inteligencji do roku 2039*, Warszawa, 2020.
22. NATO, *Allied Command Transformation (ACT)*, Cyber Resilience Strategic Concept. Norfolk, VA, 2023.
23. NATO, *Resilience as the first line of defence and deterrence*, NATO official publications, 2021.
24. NATO CCDCOE, *Locked Shields – The World's Largest and Most Complex International Live-Fire Cyber Defence Exercise*, 2025.
25. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, dokument rządowy, 2019.
26. Umowa między Stronami Traktatu Północnoatlantyckiego o współpracy w dziedzinie informacji atomowych z 18.06.1964, (Dz. U. 2001.143.1594).