PIOTR MICKIEWICZ[1]
Uniwersytet Gdański
ORCID: 0000-0002-3533-337X

DOI : 10.14746/rie.2024.18.12

Ewolucja niemieckiej polityki bezpieczeństwa cybernetycznego w latach 2011–2024

Wprowadzenie

W świecie ponowoczesnym obszarem kreującym szereg procesów jest cyberprzestrzeń, zaś jedną z najważniejszych potrzeb ludzkich stało się zapewnienie bezpieczeństwa informacyjnego. Rolą państwa jest zapewnienie bezpiecznego funkcjonowania jego organów i instytucji oraz obywateli w przestrzeni informacyjnej, określane jako zapewnienie bezpieczeństwa informacyjnego. Jest ono osiągane między innymi poprzez dążenie do pełnej kontroli własnej infosfery w postaci ochrony zasobów informacyjnych państwa i jego elementów składowych. Pojęcie „bezpieczeństwo informacyjne" jest definiowane w różny sposób i postrzegane w różnych kontekstach. Autor opowiada się za podejściem zaprezentowanym przez amerykański ośrodek badawczy National Initiative for Cybersecurity Careers and Studies, który definiuje to pojęcie jako „zbiór dyrektyw, przepisów, zasad i praktyk, które określają sposób zarządzania, ochrony i dystrybucji informacji przez organizację" (*A Glosary*, hasło „*Information Security Policy*")[2]. Elementem tak definiowanego bezpieczeństwa informacyjnego, które niekiedy jest postrzegane jako osobny obszar przedmiotowy, jest bezpieczeństwo cybernetyczne/cyberbezpieczeństwo. Przyjmując, że jeżeli bezpieczeństwo informacyjne w polityce państwa sprowadza się do zapewnienia komponentów technologicznych niezbędnych do ochrony danych, to w ramach działań na rzecz swojego bezpieczeństwa cybernetycznego państwo tworzy procedury i komponenty techniczne wykorzystywane do ochrony swoich zasobów informatycznych. Rozwiązanie to powoduje, że do definiowania pojęcia „cyberbezpieczeństwo" wykorzystuje się tzw. wąskie i szerokie podejście uznając, iż jest to ochrona systemów, sieci przesyłowych oraz zawartych informacji (definicja wąska) lub całościowa strategia zawierająca koncepcje ochrony uwzględniające prewencję, profilaktykę oraz edukację społeczną (*A Glosary*, hasło „*Cybersecurity*").

Przyjęty do rozwiązania problem badawczy to proces modyfikacji niemieckiej polityki bezpieczeństwa cybernetycznego w świetle zmiany specyfiki zagrożeń tego typu oraz przebiegu procesu zmierzającego do ujednolicenia procedur ochronnych w państwach członkowskich UE. Celem jest zaś ocena adekwatności wdrażanych zmian w kontekście przeobrażeń tego typu zagrożeń oraz proponowanych przez instytucje

[2] Podobny pogląd w Polsce reprezentują między innymi Piotr Potejko i Marek Madej. Zob. Potejko, 2009, s. 194; Madej, 2009, s. 18.

UE form kooperacji państw członkowskich. Przyjęta hipoteza to stwierdzenie że niemieckie władze federalne prowadzą szeroko zakrojone działania na rzecz ochrony cybernetycznej, wykorzystując do tego rozbudowany system bezpieczeństwa cybernetycznego państwa i równocześnie prowadząc politykę wspierającą działania Komisji Europejskiej mające na celu ujednolicenie procedur ochronnych w UE. Zasadnicze mikro-problemy badawcze, jakie pozwoliły zweryfikowanie tak sformułowane hipotezy to: prezentacja zakresu aktywności Komisji Europejskiej zmierzającej do stworzenia jednolitych procedur ochrony cybernetycznej w państwach członkowskich, analiza sposobu funkcjonowania niemieckiego systemu ochrony cybernetycznej oraz sposobu implementacji zaleceń Komisji Europejskiej zmierzających do stworzenia jednolitych procedur ochronnych. Bazą materiałową wykorzystaną do przygotowania opracowania stanowią dokumenty strategiczne oraz określające zadania poszczególnych ogniw niemieckiego systemu bezpieczeństwa cybernetycznego, a także dokumenty wytworzone przez instytucje UE. Z tego względu zastosowane metody badawcze to przede wszystkim analiza dokumentów częściowo uzupełniana przez elementy analizy systemowej i porównawczej. Punktem wyjścia do rozważań jest ewolucja unijnej polityki w latach 2011–2024 postrzegana jako działania na rzecz stworzenia jednolitych mechanizmów ochrony cybernetycznej państw członkowskich i ograniczony do wdrażania rozwiązań prawnych, które powinny zostać implementowane do rozwiązań krajowych. Ocena procesu ewolucji niemieckiego systemu ochrony cybernetycznej to analiza zakresu kompetencji federalnych urzędów współtworzących ten system oraz zakresu zmian w sposobie ich funkcjonowania i modyfikacji zadań, jakie nakładano na te instytucje w latach 2005–2024. Rozważania te uzupełniają oceny odnoszące się do zakresu modyfikacji niemieckiej koncepcji zapewniania bezpieczeństwa cybernetycznego, jakie wprowadza pierwsza w historii tego państwa strategia bezpieczeństwa z 2023 roku.

Polityka ochrony cybernetycznej Unii Europejskiej

Zaangażowanie instytucji Unii Europejskiej w kreowanie jednolitej polityki cybernetycznej wynika głównie z uznania, iż rozwijający się rynek usług cyfrowych staje się jedną z najważniejszych determinantów rozwoju społeczno-gospodarczego (*Rozporządzenie Parlamentu Europejskiego i Rady 2021/694*)[3]. Równocześnie dostrzeżono skalę zagrożeń wynikających z korzystania z cyberprzestrzeni dla indywidualnego użytkownika oraz jej wykorzystania do destabilizacji gospodarczej i politycznej państw członkowskich. Przeświadczenie to powoduje, że w polityce Unii Europejskiej wyróżnić można dwa obszary działań na rzecz zapewniania bezpieczeństwa cybernetycznego. Pierwszy odnosi się do kwestii dostępu i sposobu zarządzania cyberprzestrzenią, postrzeganą jako Internet. Druga koncentruje się na – postrzeganej kompleksowo – problematyce ataków cybernetycznych i ochrony systemów, sieci przesyłowych oraz baz danych. W pierwszym z wymienionych obszarów za cel uznano stworzenie multilateralnego systemu zarządzania Internetem obejmującego zarówno treści, jakie

[3] Kwestię tę podniesiono także w programie „Cyfrowa Europa” na lata 2021–2027, przeznaczając na ten cel 7,588 mld EUR.

zawierają zasoby internetowe, jak i kwestie techniczne odnoszące się między innymi do protokołów internetowych (*Komunikat Komisji*..., COM 2014/72, s. 7–10). W dużej mierze obszar zainteresowań instytucji europejskich został skoncentrowany na kwestii dostępności do wiedzy i stosowania praw autorskich oraz ochrony użytkownika przed niechcianymi informacjami (spaming, phishing, malvertisin itp.), a także złośliwymi lub szpiegowskimi programami (*Komunikat Komisji...*, COM 2006/688; *Decyzja ramowa Rady 2005/222/WSiSW*, *Rozporządzenie Parlamentu Europejskiego i Rady 2016/679*). Natomiast drugi obszar to przede wszystkim budowa odporności informatycznej i klasycznej infrastruktury krytycznej państw członkowskich. Zakładający także zdolność do ochrony, jak i nakładania sankcji prawnych wobec podmiotów kreujących takowe zagrożenia (*Dyrektywa Rady 2008/114/WE*)[4]. Przyjęty w 2009 roku program działania obejmuje pięć obszarów aktywności, które określono jako budowa odporności („gotowość” i „zapobieganie”), wykrywanie ataków cybernetycznych, reagowanie na ich wystąpienie, niwelowanie skutków oraz przywracaniu sprawności operacyjnej systemów i sieci (*Komunikat*..., KOM 2009/149, s. 9–13). Oceniając proces ewolucji tej koncepcji przeciwdziałania zagrożeniom w cyberprzestrzeni wskazać należy, iż ważną jej częścią od roku 2016 jest proces dostosowywania rozwiązań prawnych i instytucjonalnych w państwach członkowskich, której najważniejszym dokumentem stała się (do czasu jej nowelizacji) dyrektywa o bezpieczeństwie sieci i informacji (*Networkand Information Security Directive* – NIS Directive).

Postrzegając politykę cybernetyczną Unii Europejskiej w latach 2011–2024 jako kompleksowe działania na rzecz zapewnienia bezpieczeństwa cybernetycznego obywatelom UE oraz budowę systemu ochrony cybernetycznej informatycznej i klasycznej infrastruktury krytycznej, podkreślić należy iż znaczna cześć tej aktywności UE odnosiła się do kwestii kreowania prawa wtórnego i tworzenia ram pozwalających na implementację tego prawa w system prawny państw członkowskich (Małecka, 2021, s. 69–91). Dopiero w drugim etapie, tj. po roku 2016 zdecydowanym priorytetem stała się odporność cybernetyczna państw członkowskich. Za najważniejsze rozwiązania, które wdrożono w tym okresie uznać należy powszechne stosowanie w polityce cybernetycznej państw członkowskich szerokiej definicji cyberbezpieczeństwa obejmującej:

– zwiększenie zdolności operacyjnej do zwalczania wszelkich form cyberprzestępczości;
– wdrożenie (uzgodnionych w ramach UE) uniwersalnych przepisów regulujących zwalczanie cyberprzestępczości,
– zacieśnienie współpracy z sektorem prywatnym (*Komunikat Komisji...*, COM 2011/287 final).

Celem tych działań niezmiennie pozostaje zabezpieczenie funkcjonalności systemów i sieci teleinformatycznych oraz ich baz danych (*Wspólny Komunikat*..., Jont 2013/1 final), a realizatorem prowadzonych działań są państwa członkowskie. Zostały one zobligowane do zapewnienia bezpieczeństwa cybernetycznego na swoim teryto-

[4] Zakres tych działań określono w cytowanej dyrektywie, a część działań zrealizowano w latach 2001–2005, opierając się na zapisach tzw. Polityki bezpieczeństwa sieci i informacji (Network and Information Security, NIS) z 2001 roku oraz Zielonej księdze w sprawie europejskiego programu ochrony infrastruktury krytycznej z 2005 roku.

rium przy współpracy władz administracyjnych z operatorami teleinformatycznymi oraz instytucjami europejskimi. Zasadą wiodącą jest realizacja przedsięwzięć ochronnych w pięciu obszarach priorytetowych za które uznano:
– osiągnięcie odporności na zagrożenia cybernetyczne;
– radykalne ograniczenie cyberprzestępczości;
– opracowanie polityki obronnej i rozbudowa zdolności w dziedzinie bezpieczeństwa cybernetycznego w powiązaniu z WPBiO;
– rozbudowa zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cybernetycznego;
– ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla UE i promowanie podstawowych unijnych wartości (*Komunikat Komisji*..., COM 2011/ 287 final, s. 5–24).

Szczególne znaczenie w gronie powyższych celów strategicznych przyznano kwestii promowania wartości oraz poszanowania praw i wolności osobistych. Zwłaszcza uzyskania powszechnej dostępności do przestrzeni cyfrowej oraz zachowania prawa do swobody wypowiedzi oraz zapewnienia ochrony danych wrażliwych (*Komunikat Komisji*..., COM (2011) 287 final, s. 4–5). Natomiast skala zagrożenia cyberatakami w okresie pandemii COVID-19, jak i wynikająca z rosyjskiego oddziaływania cybernetycznego doprowadziła do podjęcia przez organy europejskie prac nad kompleksowymi założeniami ochrony cyberprzestrzeni. Zasadnicza decyzja to wdrożenie dyrektywy NIS 2 (*Dyrektywa Parlamentu Europejskiego i Rady 2022/2555*) określającej prawne i organizacyjne wymogi dla narodowych systemów ochrony cybernetycznej i obowiązek objęcia ochroną określonych sektorów gospodarczych, społecznych i administracyjnych państw członkowskich[5]. W konsekwencji tych uzgodnień system ochrony cybernetycznej państw członkowskich tworzą organy państwa i powiązane z nim, osoby prawne i fizyczne oraz podmioty nieposiadające osobowości prawnej. Zakres ich obowiązków i zadań jest natomiast określany w narodowych dokumentach strategicznych, które są implementacją zaleceń Komisji Europejskiej sformułowanych zwłaszcza określonych w dwóch dokumentach tj. Komunikacie Komisji do Parlamentu Europejskiego i Rady pt. *Zarządzanie Internetem. Kolejne działania* (*Komunikat Komisji*..., COM 2009/0277) oraz unijnej strategii cybernetycznej (*Wspólny Komunikat*..., Jont 2013/1 final). Częściowo odnaleźć je można także w Strategii bezpieczeństwa UE na lata 2020–2025 z lipca 2020 r. (*Komunikat Komisji*..., COM 2020/605 final). W dokumentach tych uznano, że władze państwowe powinny opracować i wdrożyć systemowe rozwiązania określające zasady bezpiecznego udostępniania cyberprzestrzeni i ochrony danych w niej przechowywanych przy uznaniu prawa podmiotów niepaństwowych w zarządzaniu cyberprzestrzenią. Jako zadanie własne

[5] Dyrektywa NIS 2 ma zastosowanie do podmiotów publicznych oraz prywatnych świadczących usługi lub prowadzących działalność w UE i jednocześnie kwalifikują się jako średnie przedsiębiorstwa lub przekraczają pułapy dla średnich przedsiębiorstw. Za sektory, w których obowiązują jej zapisy uznano: energetykę, transport, bankowość, infrastrukturę rynków finansowych, opiekę zdrowotną, zaopatrzenia w wodę pitną, ścieki, infrastrukturę cyfrową, zarządzanie usługami ICT, administrację publiczną, przestrzeń kosmiczną, usługi pocztowe i kurierskie, gospodarowanie odpadami, produkcja, przetwarzanie i dystrybucja chemikaliów, produkcja, przetwarzanie i dystrybucja żywności, wytwórczość, usługi cyfrowe oraz badania naukowe.

Komisji Europejskiej uznano natomiast stworzenie rozwiązań systemowych (prawno-organizacyjnych) oraz zapewnienie środków finansowych umożliwiających wykrywanie oraz niwelowanie skutków ataków cybernetycznych oraz wsparcie, zwłaszcza małych i średnich przedsiębiorstw, w procesie podnoszenia kompetencji cyfrowych pracowników.

Ewolucja niemieckiej koncepcji bezpieczeństwa cybernetycznego 2011–2024

Kreatorem niemieckiej polityki ochrony cyberprzestrzeni, a właściwie ochrony systemów teleinformatycznych od lat 90. XX wieku jest Federalne Biuro ds. Bezpieczeństwa Informacji (Bundesamt für Sicherheitin der Informationstechnik – BSI). Do końca XX wieku zadaniem BSI była koordynacja działań władz federalnych ukierunkowanych na niwelowanie możliwości wykorzystania systemów teleinformatycznych do działań określanych jako przestępstwa gospodarcze. Dopiero w roku 2005, zgodnie z zaleceniami Komisji Europejskiej opracowano tzw. Federalny Plan ochrony infrastruktury teleinformatycznej (Nationalen zum Schutz der Informationsinfrastrukturen – NPSI) zawierający zakres działań ochronnych realizowanych w administracji publicznej oraz w sektorze infrastruktury krytycznej (Oleksiewicz, s. 121). Był on modyfikowany zgodnie z zaleceniami Komisji Europejskiej w latach 2006–2009, ale nie zmieniono zakresu prowadzonych działań. Kompleksowa koncepcja przeciwdziałania zagrożeniom cybernetycznym w Republice Federalnej Niemiec powstała w roku 2011 w – przyjętej 23 lutego 2011 r. – strategii cyberbezpieczeństwa. Bezpieczeństwo cybernetyczne RFN zostało zdefiniowane, w jako konglomerat działań prowadzonych w celu zapewnienia możliwości bezpiecznego funkcjonowania sieciowych systemów informacyjnych, które wpływają na obszary życia społecznego i gospodarczego oraz umożliwiają rozwój społeczno-gospodarczy (*Cyber-Sicherheitsstrategie...*, s. 16–17). W praktyce zakres tych działań obejmuje trzy sfery funkcjonowania państwa:

– gospodarczą, gdzie celem jest zapewnienie możliwości bezpiecznego funkcjonowania sieciowych systemów informacyjnych, wpływających na poszczególne obszary życia gospodarczego oraz umożliwiających rozwój społeczno-gospodarczy;
– publiczną, w której zamierzeniem jest zapewnienie bezpieczeństwa sieciom i bazom danych instytucji publicznych;
– administracyjno-polityczną, dla której celem jest budowa federalnej sieci informatycznej dla urzędów federalnych i państw związkowych (*Cyber-Sicherheitsstrategie...*, cele strategiczne nr 4 i 5).

Bezpieczeństwo w cyberprzestrzeni ma zapewnić – w myśl założeń Strategii – osiągnięcie, jednoznacznie sprecyzowanych celów w dziesięciu obszarach strategicznych. W sferze organizacyjnej zakładały one powołanie *Narodowego Centrum Przeciwdziałania Zagrożeniom dla Cyberprzestrzeni* (*Nationales Cyber-Abwehrzentrum* – NCAZ) oraz określenie form zaangażowania się w jego działanie federalnych instytucji odpowiadających za bezpieczeństwo teleinformatyczne. Zakres, określonych w celach strategicznych, przedsięwzięć ukierunkowanych na przeciwdziałanie i zwalczanie zagrożenia można sprowadzić do następujących:

– zapewnienie ochrony teleinformatycznej infrastruktury krytycznej w oparciu o federalny plan ochrony infrastruktury krytycznej (*Nationaler Plan zum Schutz der Informationsinfrastrukturen* – NPSI);
– zapewnienie ochrony teleinformatycznej małych i średnich przedsiębiorstw i zasobów będących własnością obywateli;
– zapewnienie bezpieczeństwa sieciom i bazom danych instytucji publicznych poprzez docelową budowę tzw. federalnej sieci informatycznej dla urzędów federalnych i państw związkowych;
– zwiększenie efektywności Zespołów Reagowania na Incydenty Komputerowe (CERT) państw związkowych i poprawa ich współpracy, miedzy innymi poprzez nadanie kompetencji w tym obszarze – powołanej specjalnie – Rady Planowania teleinformatyki;
– skuteczne zwalczanie ataków na systemy informatyczne poprzez podjęcie ścisłej współpracy BKA i przedstawicieli sektorów gospodarczych, także w zakresie wymiany informacji o zdarzeniach oraz tworzenia technicznych rozwiązań w dotyczących ochrony systemów teleinformatycznych;
– stworzenie i wdrożenie do powszechnego stosowania katalogu instrumentów ograniczających poziom zagrożenia (*Cyber-Sicherheitsstrategie*..., s. 9–14).

Przyjęta w tym czasie koncepcja ograniczała więc zakres przedmiotowy cyberbezpieczeństwa do sfery zarządzania kryzysowego, co wpłynęło na zakres prowadzonych działań ochronnych. Uznano, że ochroną powinny być objęte systemy teleinformatyczne decydujące o funkcjonowaniu państwa, zwłaszcza informatyczna infrastruktura krytyczna, elementy technologii informatycznych oraz komunikacyjnych, wpływające na sposób funkcjonowania społeczeństwa i administracji oraz Internet. Zasadniczymi formami wrogiego oddziaływania w cyberprzestrzeni wg tych założeń były cyberataki, cyberszpiegostwo oraz sabotaż cybernetyczny (*Cyber-Sicherheitsstrategie*..., s. 17). Przyjęta koncepcja przeciwdziałania oparta została na wynikach corocznych analiz stanu bezpieczeństwa teleinformatycznego przedstawianych w formule raportu *Die Lage der IT-Sicherheit in Deutschland*. Zawiera on szczegółowy opis zagrożeń, form stosowanych działań, obszarów objętych ich oddziaływaniem oraz rozwiązania mające ograniczyć skalę zagrożenia. Natomiast określony w *Planie Ochrony Infrastruktury Teleinformatycznej* (NPSI) zakres ochrony cyberprzestrzeni stanowił podstawę do konstrukcji planów działań ochronnych wdrażanych przez kierownictwa firm i organów zarządzających elementami infrastruktury krytycznej. Jego integralnym elementem jest także poprawa poziomu zabezpieczenia systemów teleinformatycznych, wykorzystywanych przez małe i średnie firmy oraz ośrodki edukacyjne[6]. Działania te są uzupełniane przedsięwzięciami realizowanymi przez administrację publiczną w ramach strategii *Federalne Zarządzanie Teleinformatyczne*. Celem tych przedsięwzięć jest zapewnienie niezakłóconego działania systemów mających usprawnić sposób funkcjonowania administracji publicznej. Przedsięwzięcia te zostały poszerzone w wyniku oceny skali zagrożenia cybernetycznego w okresie wprowadzenia stanu zagrożenia pandemicznego związanego z wirusem COVID-19. W okresie tym Federalny Urząd Policji Kryminalnej (BKA) zarejestrował 108 tysięcy incydentów

[6] Przedsięwzięcia te są nadzorowane przez, powołaną w 2011 roku przez Ministerstwo Gospodarki Technologii oraz stowarzyszenia przemysłowe, specjalną grupę zadaniową.

cybernetycznych rocznie (Fürstenau). Kierując się wynikami przywołanego raportu przyjęto, że realnym zagrożeniem państwa federalnego i jego obywateli staje się sukcesywne stosowanie złośliwego oprogramowania i cyberataków skoncentrowane na próbach wyłudzenia lub przejęcia funduszy. Za szczególnie groźne zjawiska uznano proceder ransomware, czyli wrogiego szyfrowania zasobów w celu uzyskania okupu, kradzież danych osobowych i kont oraz ataki na platformy pracy zdalnej. W tej sytuacji uznano, że obowiązkiem władz federalnych powinno być także wdrażanie rozwiązań zapewniających wysoki poziom bezpieczeństwa i ochrony w cyberprzestrzeni w całokształcie koncepcji cyfryzacji państwa. W konsekwencji równie istotnym co informatyczna infrastruktura krytyczna priorytetowym obszarem niemieckiej polityki bezpieczeństwa cybernetycznego stały się sieci i systemy teleinformatyczne wykorzystywane przez obywateli oraz zawierające dane wrażliwe obywateli. Zmiana pierwotnego podejścia do przedmiotowego zakresu cyberbezpieczeństwa została usankcjonowania w ustawie o bezpieczeństwie sieci teleinformatycznych (I IT-Sicherheits gesetz 2.0) z 7 maja 2021 r. Jej zapisy zakładały szybkie wdrożenie rozwiązań technicznych umożliwiających zapobieganie atakom cybernetycznym oraz samoobronę użytkownika systemów i sieci teleinformatycznych. Jednakże za najistotniejsze rozwiązania uznać należy poszerzenie kompetencji nadzorczych federalnego urzędu do spraw bezpieczeństwa technik informacyjnych (Bundesamt für Sicherheit in der Informationstechnik – BSI) oraz określenie czterech grup ryzyka, które powinny zostać poddane ochronie cybernetycznej. Za takowe uznano struktury administracyjne, sfery nauki i gospodarki oraz samo społeczeństwo.

Równie istotną co poszerzenie zakresu odpowiedzialności systemu bezpieczeństwa cybernetycznego było poszerzenie uprawnień jego elementów składowych. Wiodącymi instytucjami w zakresie przygotowania i wdrażania rozwiązań kreujących politykę ochrony w przestrzeni cybernetycznej pozostają *Narodowa Rada Cyberbezpieczeństwa* (*Nationaler Cyber-Sicherheitsrat – NCS*) oraz *Rada Planowania Teleinformatycznego*, w której gestii pozostaje ochrona sieci informatycznych. Federalnym organem koordynującym współpracę pomiędzy organami administracji oraz strukturami gospodarczymi, które mogą być celem ataku cybernetycznego pozostaje *Narodowe Centrum Przeciwdziałania Zagrożeniom dla Cyberprzestrzeni* (NCAZ)[7]. Pełni przede wszystkim rolę federalnego ośrodka gromadzenia, analizy i wymiany informacji[8] oraz platformy współpracy instytucji zajmujących się monitorowaniem zagrożenia, koordynacją form reagowania na zaistniałe zdarzenie oraz opracowania koncepcji zwalczania. Zadaniem Centrum jest wykrycie zagrożenia, jego analiza pod kątem potencjalnych szkód dla systemów IT i infrastruktury krytycznej oraz opracowanie wytycznych i zalecanych form reakcji. Natomiast reakcję na stwierdzone incydenty prowadzić mają operatorzy i administratorzy sieci, przy wsparciu, funkcjonujących w krajach

[7] Jej działaniami kieruje Pełnomocnik Rządu Federalnego ds. Teleinformatycznych, a w jej skład wchodzą przedstawiciele federalnych ministerstw spraw zagranicznych, wewnętrznych, obrony narodowej, gospodarki, finansów, sprawiedliwości oraz oświaty, a także delegaci władz krajów związkowych.

[8] Stosowne okresowe raporty, zawierające ocenę stanu zagrożenia i wytyczne dla działań prowadzonych na szczeblu federalnym, przekazywane są do *Narodowej Rady Cyberbezpieczeństwa*. Są one także wykorzystywane do opracowania kolejnych *Die Lage der IT-Sicherheit in Deutschland*.

związkowych, Zespołów Reagowania na Incydenty Komputerowe (CERT – Computer Emergency Response Team).

Stworzony w pierwszej dekadzie XXI wieku niemiecki system cyberbezpieczeństwa podtrzymał wiodącą rolę Bundesamt für Sicherheit in der Informationstechnik. Niezmiennie odpowiada on za ocenę podatności systemów IT na ataki cybernetyczne, analizę techniczną i informatyczną ataku cybernetycznego i jego skutków. W pierwotnych rozwiązaniach część zadań związanych ze zwalczaniem zagrożeń wykonywały także inne ograny federalne. Wskazać należy rolę Federalnego Urzędu ds. Ochrony Konstytucji (Bundesamt für Verfassungsschutz – BfV), którego zadaniem było wykrycie mocodawców ataku, Federalnego Urzędu ds. Ochrony Ludności i Reagowania Kryzysowego (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe*) odpowiadającego za ocenę skutków ataku dla funkcjonowania infrastruktury krytycznej oraz – współpracujących ściśle w zakresie wykrycia sprawców ataku cybernetycznego – Federalnego Urzędu Kryminalnego (*Bundeskriminalamt – BKA*) oraz Federalnego Urzędu Celnego (*Zollkriminalamt*). W systemie tym funkcjonują także policja federalna, odpowiadająca za ocenę zagrożenia, wykrycie sprawców na terenie RFN, Bundeswehra, a właściwie – odpowiadający za ochronę wojskowych systemów informatycznych oraz udzielenie ewentualnej pomocy urzędom federalnym – kontrwywiad wojskowy oraz Federalna Służba Wywiadu, monitorująca zagrożenie poza granicami kraju. Formalnie jednak Bundeswehra, Federalna Służba Wywiadowcza, Federalny Urząd Kryminalny, Kryminalny Urząd Celny oraz Policja Federalna posiadają status „członków stowarzyszonych” w NCAZ (Brzostek, 2021, s. 306). Rola Federalnego Urzędu ds. Bezpieczeństwa Informacji została znacznie rozszerzona w regulacjach prawnych z 2015 i 2021 roku. Poza zadaniem w postaci wykrywania i zwalczania zagrożeń w przestrzeni cybernetycznej, na mocy zapisów znowelizowanej 25 lipca 2015 roku ustawy o BSI (*Gesetz über das Bundesamt für Sicherheit*) oraz ustawy o bezpieczeństwie systemów teleinformatycznych z 17 lipca 2015 r. (*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*)[9]. Organ ten odpowiada także za opracowanie zasad klasyfikacji informatycznej infrastruktury krytycznej oraz określenie wymogów związanych z ochroną informatyczną całej federalnej infrastruktury krytycznej. Zawierają one szczegółowe rozwiązania dla konkretnych systemów IT, dotyczące inwestycji w celu zabezpieczenia ich funkcjonalności (*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme* Anhang 4 zu § 1 Nummer 4 und 5, § 5, Absatz 4 Nummer 1 und 2, Anlagenkategorien und Schwellenwerte im Sektor Informationstechnik und Telekommunikation). Urząd uzyskał także uprawnienia do korzystania z podległego Federalnemu Urzędowi ds. Ochrony Ludności i Reagowania Kryzysowego systemu informatycznego (*BSI-KritisV*) oraz prawo do otrzymywania raportów o zdarzeniach w poszczególnych segmentach infrastruktury krytycznej (wcześniej raporty takie przesyłał do Urzędu jedynie sektor energetyki jądrowej). Posiada także uprawnienia do nakładania na operatorów systemów i sieci teleinformatycznych oraz instytucji ich wykorzystujących obowiązków (stosowania określonych procedur) w zakresie ochrony danych, form zabezpieczenia w przypadku ich digitalizacji i procedur informowania o próbach zakłócania pracy systemów

[9] Od 2021 roku obowiązuje jej drugi wariant określany jako 2.0.

teleinformatycznych oraz prób włamania do osobistych kont w systemach[10]. Uczestniczy w procesie weryfikacji operatorów systemów IT, przeprowadzając, co 2 lata stosowne egzaminy i – w porozumieniu z radą nadzorczą instytucji – może wystąpić z wnioskiem o odsunięcie operatora systemu od wykonywania obowiązków. Może zażądać informacji o rozwiązaniach w zakresie bezpieczeństwa wdrażanych produktów teleinformatycznych i zbierać informacje o podmiotach gospodarczych, wykorzystujących sieci teleinformatyczne (*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*, art. 7). Szczególnym nadzorem BSI objęto sposób stosowania procedur w działach infrastruktury krytycznej decydującej o sposobie funkcjonowania społeczeństwa, czyli systemach: energetycznym, dostaw wody pitnej, wyżywienia, telekomunikacyjnych oraz technologii informatycznych (*Verordnung zur Bestimmung*) i systemu bankowego. BSI nałożyło także szereg obowiązków na operatorów sieci teleinformatycznych i instytucji ich wykorzystujących w zakresie ochrony danych, form zabezpieczenia w przypadku ich digitalizacji oraz prób włamania do osobistych kont w systemie. BSI posiada także mobilne zespoły reagowania na incydenty tzw. MIRT-y. Ich zadaniem jest reagowanie na incydenty cybernetyczne w instytucjach federalnych i państw związkowych oraz operatorów infrastruktury krytycznej. Kolejne poszerzenia kompetencji BSI wynikają ze zmian wdrażanych od 2020 roku przez Unię Europejską. We wprowadzonych na przestrzeni 2021–2023 roku rozwiązaniach Bundesamt für Sicherheit in der Informationstechnik jest centralnym federalnym organem odpowiadającym za prowadzenie polityki cybernetycznej państwa i system ochrony cyberprzestrzeni. W jego gestii znajduje się prawo do opracowania strategii cybernetycznej i bezpieczeństwa cybernetycznego oraz standardy postępowania obowiązujące zarówno władze krajów związkowych, jak i podmioty prywatne. Jest uprawniony do monitorowania procesu ich stosowania oraz certyfikacji rozwiązań w zakresie cyberbezpieczeństwa. Istotnym novum we wdrożonych rozwiązaniach jest zobligowanie BSI do zapewnienia ochrony cybernetycznej sieciom komórkowym między innymi poprzez certyfikację kluczowych jej komponentów. W ten sam sposób ocenić należy, nałożony na BSI, obowiązek ochrony samych indywidualnych użytkowników systemów teleinformatycznych. W praktyce urząd pełni rolę swoistego centrum porad teleinformatycznych oraz instytucji certyfikującej wdrażane przez operatorów rozwiązania i produkty.

Kierunki rozwoju polityki bezpieczeństwa cybernetycznego RFN po 2023 roku

W procesie realizacji polityki bezpieczeństwa cybernetycznego Republiki Federalnej Niemiec po 2023 roku szczególną rolę odegrać powinny zapisy pierwszej w historii państwa niemieckiego strategii bezpieczeństwa oraz proces poszerzania unijnej polityki o kwestie obronne[11]. Przyjęty w 2023 roku dokument jest pierw-

[10] Wynika to z zapisów par. 3 punkt 3 i 8b, ustawy o BSI z 2015 roku.

[11] W Republice Federalnej Niemiec do roku 2023 zasadniczymi dokumentami tego typu były tzw. Białe Księgi publikowane w latach 1994, 2006, 2016, a obecnie Narodowa Strategia Bezpieczeństwa (*Sicherheit für Deutschland*).

szą strategią sektorową odnoszącą się w sposób kompleksowy do problematyki bezpieczeństwa państwa, co powoduje, że zasadnym jest określenie zmian w poszczególnych obszarach funkcjonalnych polityki bezpieczeństwa RFN. W dokumencie tym wprowadzono pojęcie „zintegrowane bezpieczeństwo”, które określono jako kooperację niemieckich ośrodków społeczno-polityczno-gospodarczych pod egidą rządu federalnego zakładającą wykorzystywanie wszelkich dostępnych instrumentów i środków zapewniających określony poziom bezpieczeństwa państwa, a także – w domyśle – społeczeństwa i obywatela (*Integrierte Sicherheit für Deutschland*, s. 30). Problematyka bezpieczeństwa cybernetycznego została w tym dokumencie usytuowana w obszarze „odporność” i częściowo „zrównoważenie”. Wynika to wprost z uznania, iż prawo do dostępu do systemów i sieci oraz ochrona tych zasobów jest elementem gwarantowania praw i wolności, a także uznania, iż bezpieczeństwo państwa to także problematyka bezpieczeństwa ludzkiego, chociaż w dokumencie posłużono się pojęciem *human security* wg definicji OZN z 1994 roku (*Human Development Report 1994*, s. 22–24). Zastosowanie tej definicji doprowadziło do znacznego poszerzenia zakresu prowadzonych działań w odniesieniu do indywidualnych użytkowników oraz firm oferujących usługi za pośrednictwem systemów i sieci teleinformatycznych. Rozwiązania te należy uznać za adekwatną odpowiedź na zagrożenia, które pojawiły się w okresie pandemii COVID-19. Za rozwiązanie leżące w interesie RFN uznać także należy propozycje Komisji Europejskiej wzmacniające kooperację państw członkowskich w zakresie polityki wczesnego ostrzegania oraz wspólną budowę zespołów szybkiego reagowania na incydenty cybernetyczne. Budowany od 2021 roku system Joint Cyber Unit wpisuje się w pełni w niemiecką koncepcję międzynarodowego systemu reagowania na ataki cybernetyczne, który powinien zastąpić koncepcje reagowania wyłącznie na tzw. *skoordynowanej reakcji na incydenty cybernetyczne na dużą skalę*. Natomiast za potencjalny problem natury politycznej uznać należy koncepcję cyberobrony kreowanej przez Europejską Agencję Obrony i Centrum Analiz Wywiadowczych.

Podsumowanie

Niemiecka polityka bezpieczeństwa cybernetycznego jest w znacznej mierze tworzona w oparciu o plan budowy wspólnotowej przestrzeni cybernetycznej UE oraz wynikające z tej koncepcji zalecenia i inne formy unijnego prawa wtórnego. Rozwiązanie to stało się wiodącą zasadą po roku 2022 i określiło sposób angażowania się Republiki Federalnej w budowę unijnego systemu odporności cybernetycznej. Niemiecka polityka cybernetyczna w wymiarze zewnętrznym została skoncentrowana na wsparciu propozycji instytucji unijnych zmierzających do powszechnego stosowania przez państwa członkowskie „szerokiej definicji” bezpieczeństwa cybernetycznego oraz tworzenia unijnych standardów ochrony cybernetycznej. Angażując się w ten proces państwo niemieckie dąży zarówno do zajęcia pozycji lidera procesu ewolucji unijnych działań ochronnych, jak i sukcesywnego podnoszenia zakresu własnego bezpieczeństwa poprzez dobrze przeprowadzaną implementację

prawa wtórnego UE. Oceniając niemieckie rozwiązania formalno-prawne podkreślić należy, że ta implementacja współkreuje federalną politykę bezpieczeństwa cybernetycznego. Równocześnie jednak wdrażane rozwiązania pozwoliły na uzyskanie dużego zakresu kompatybilności niemieckiego systemu z instytucjami UE zajmującymi się oceną zagrożeń w cyberprzestrzeni. W konsekwencji zbudowano „pionowy” (nie hierarchiczny) układ kooperacji pomiędzy instytucjami UE, federalnymi organami zajmującymi się ochroną cybernetyczną oraz operatorami systemów, a także opracowano kompleksowy model działań ochronnych w odniesieniu do istniejącego katalogu zagrożeń.

Wskazując na znaczenie planu budowy przez kraje UE komplementarnego systemu bezpieczeństwa cybernetycznego w niemieckiej polityce podkreślić należy także umiejętne określenie roli instytucji państwa, jak i interesariuszy gospodarczych i społecznych w procesie jego zapewniania. Przede wszystkim niemieckie plany zapewniania odporności cybernetycznej zakładają iż ich celem jest wzmocnienie nie tyle poziomu bezpieczeństwa co suwerenności cybernetycznej państwa. Obejmującej działania mające zapewnić poczucie bezpieczeństwa w sferze politycznej, gospodarczej i społecznej. Rolę kreatora działań wypełniają instytucje federalne, a celem prowadzonych działań niezmiennie jest maksymalne umożliwienie bezpiecznego wykorzystania przestrzeni cyfrowej przez jej użytkowników na obszarze państwa. Modyfikacji podlegają natomiast cele operacyjne, które są dobrze dostosowywane do specyfiki i ewolucji zagrożeń. Nie wpływają one natomiast na sposób organizacji systemu bezpieczeństwa cybernetycznego, koncentrując się na wskazaniu zadań dla poszczególnych jego elementów składowych. Oceniając sposób funkcjonowania niemieckiego systemu bezpieczeństwa cybernetycznego wskazać należy na duży poziom korelacji zadań pomiędzy sferą zarządzania kryzysowego i ochrony ludności. Formalnie gros zadań jest skoncentrowanych na ochronie informatycznej infrastruktury krytycznej, ale część z nich wprost odnosi się do kwestii zapewnienia możliwości bezpiecznego wykorzystania cyberprzestrzeni w procesach społeczno-gospodarczych, zwłaszcza odnoszących się do nowych technologii czy procesów zrównoważonego rozwoju. Równie istotną rolę w tym systemie przyznano procesowi edukacji mającym przygotować niemieckie społeczeństwo do dostrzeżenia symptomów zagrożenia i reakcji na ich wystąpienie. Zadanie to zostało włączone w działania prowadzone w ramach systemu ochrony ludności, jednakże jest to także element zwiększenia odporności cybernetycznej społeczeństwa. Wskazując na powyższe podkreślić należy, że z zakresu ścisłej kooperacji wyłączona zostanie najprawdopodobniej sfera militarna. Założenia strategii bezpieczeństwa, jak i postawa pacyfistyczna społeczeństwa i części establishmentu politycznego pozwalają na sformułowanie wniosku, że budowa regionalnej odporności cybernetycznej w wymiarze polityczno-militarnym będzie przez władze polityczne RFN blokowana. Dotyczy to zwłaszcza kwestii prowadzenia działań wyprzedzających, co pozwala na przyjęcie konkluzji, iż niemiecka aktywność zostanie skoncentrowana na kwestii wdrażania zapisów dyrektywy NIS 2 przez kraje członkowskie.

Author Contributions

Conceptualization (Konceptualizacja): Piotr Mickiewicz

Data curation (Zestawienie danych): Piotr Mickiewicz

Formal analysis (Analiza formalna): Piotr Mickiewicz

Writing – original draft (Piśmiennictwo – oryginalny projekt): Piotr Mickiewicz

Writing – review & editing (Piśmiennictwo – sprawdzenie i edytowanie): Piotr Mickiewicz

Competing interests: The author have declared that no competing interests exist

(Sprzeczne interesy: Autor oświadczył, że nie istnieją żadne sprzeczne interesy)

Bibliografia

A Glossary of Common Cybersecurity Words and Phrases, *National Initiative for Cybersecurity Careers and Studies*, https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#letter-c, 12.02.2024.

Brzostek A. (2021), *Organy władzy publicznej w zakresie ochrony cyberbezpieczeństwa w wybranych strategiach cyberbezpieczeństwa*, „Przegląd Prawa Konstytucyjnego”, nr 1(59), DOI 10.15804/ppk.2021.01.18.

Cyber-Sicherheitsstrategie für Deutschland, Budnesministerium des Inner, https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile, 12.02.2024.

Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r.: W sprawie ataków na systemy informatyczne, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32005F0222, 12.02.2024.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r.: W sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32022L2555, 12.02.2024.

Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r.: W sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=celex%3A32008L0114, 12.02.2024.

Fürstenau M. (2021), *Cyberprzestępczość kwitnie. Dzięki pandemii koronawirusa*, „Deutsche Welle” z dnia 11.05.2021, https://www.dw.com/pl/cyberprzest%C4%99pczo%C5%9B%C4%87-kwitnie-dzi%C4%99ki-pandemiikoronawirusa/a-57497463, 12.02.2024.

Gesetz über das Bundesamt für Sicherheit in derInformationstechnik (BSI-Gesetz – BSIG), https://www.gesetze-im-internet.de/bundesrecht/bsig_2009/gesamt.pdf, 12.02.2024.

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz).

Human Development Report 1994, United Nations Development Programme (UNDP), Oxford University Press, New York–Oxford 1994.

Integrierte Sicherheit für Deutschland (2023), Deutscher Bundestag Drucksache 20/7220, 14.06.2023, https://dserver.bundestag.de/btd/20/072/2007220.pdf, 12.02.2024.

Komunikat Komisji do Parlamentu Europejskiego i Rady: Zarządzanie Internetem. Kolejne działania, COM/2009/0277 końcowy, Bruksela 52009DC0277, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0277:FIN:PL:HTML, 12.02.2024.

Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: W sprawie strategii UE w zakresie unii bezpieczeństwa, COM (2020) 605 final, https://eur-lex.europa.eu/legal-content/PL/ TXT/?uri=CELEX:52020DC0605, 12.02.2024.

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: W sprawie walki ze spamem, oprogramowaniem szpiegującym i złośliwym, Bruksela, 15.11.2006, COM(2006)688 wersja ostateczna. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:PL:PDF, 12.02.2024.

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów: W sprawie ochrony krytycznej infrastruktury informatycznej. Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności 30.03.2009 (KOM (2009) 149 wersja ostateczna, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52009DC0149&from=IT, 12.02.2024.

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Jednolity rynek w obszarze praw własności intelektualnej – Wspieranie kreatywności i innowacji celem zapewnienia wzrostu gospodarczego, atrakcyjnych miejsc pracy oraz wysokiej jakości produktów i usług w Europie (COM (2011) 287 final from 24.5.2011), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52011DC0287, 12.02.2024.

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Polityka wobec Internetu i zarządzanie Internetem: Rola Europy w kształtowaniu przyszłości zarządzania Internetem, 12.2.2014, COM (2014) 72 final, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52009DC0149, 12.02.2024.

Madej M. (2009), *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, w: *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa.

Małecka A. (2021), *Polityka cyberbezpieczeństwa Unii Europejskiej na początku trzeciej dekady XXI wieku*, „Rocznik Bezpieczeństwa Międzynarodowego”, vol. 15, nr 2, DOI: https://doi.org/10.34862/rbm.2021.2.5.

Mickiewicz P. (2017), *System bezpieczeństwa cybernetycznego wybranych państw. Analiza porównawcza*, „Rocznik Bezpieczeństwa Międzynarodowego”, t. 17, nr 1, DOI: https://doi.org/10.34862/rbm.2017.1.5.

Oleksiewicz I. (2019), *Zarys polityki cyberbezpieczeństwa Unii Europejskiej. Casus Polski i RFN*, Elipsa, Warszawa.

Potejko P. (2009), *Bezpieczeństwo informacyjne*, w: *Bezpieczeństwo państwa*, red. K. A. Wojtaszczyk, A. Materska-Sosnowska, Warszawa.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.: *W sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych), https://uodo.gov.pl/pl/404/224, 12.02.2024.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program „Cyfrowa Europa” oraz uchylające decyzję (UE) 2015/2240, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32021R0694, 12.02.2024.

Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz BSIKritisverordnung– BSI-KritisV, https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/kritis-vokabinett.pdf?__blob=publicationFile, 12.02.2024.

Wspólny Komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, Jont (2013) 1 final, Bruksela

7.02.2013, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52013JC0001, 12.02.2024.

Streszczenie

Celem artykułu jest ukazanie zakresu i procesu ewolucji niemieckiej polityki bezpieczeństwa cybernetycznego w kontekście zaleceń opracowywanych przez instytucje UE. Wykazano w nim, że odporność cyfrowa RFN jest osiągana poprzez skorelowane działania organów federalnych państwa i aktorów korzystających z systemów i sieci teleinformatycznych, zwłaszcza ze sfery biznesu, nauki i edukacji. W jej kreowaniu uwzględniane są zalecenia instytucji UE, które stanowią jeden z elementów prawnych i organizacyjnych pozwalających na stworzenie systemu zapewniającego określony poziom bezpieczeństwa cybernetycznego. Przyjmowane rozwiązania w pełni wpisują się w unijną strategię cyberbezpieczeństwa, co pozwala państwu niemieckiemu współkreować unijną politykę w tym zakresie. Dotyczy to zwłaszcza działań na rzecz wdrożenia dyrektywy NIS 2. Natomiast państwo niemieckie nie zamierza się angażować, a wręcz dąży do ograniczenia zakresu potencjalnych wspólnotowych przedsięwzięć ofensywnych o charakterze polityczno-militarnym, nawet jeżeli przyjąć one by miały charakter działań wyprzedzających.

Słowa kluczowe: infosfera, bezpieczeństwo cybernetyczne, Unia Europejska, Republika Federalna Niemiec

Evolution of Germany’s cyber security policy from 2011 to 2024

Summary

The purpose of the article is to show the scope and process of evolution of Germany’s cybersecurity policy in the context of recommendations being developed by EU institutions. It shows that Germany’s digital resilience is achieved through the correlated actions of the state’s federal bodies and actors using ICT systems and networks, especially from the spheres of business, science and education. In its creation, the recommendations of EU institutions are taken into account, which are one of the legal and organizational elements that allow the creation of a system to ensure a certain level of cyber security. The solutions adopted are fully in line with the EU cyber security strategy, which allows the German state to co-create the EU policy in this area. This is especially true of the efforts to implement the NIS 2 Directive. In contrast, the German state does not intend to get involved, and in fact seeks to limit the scope of potential Community offensive ventures of a political-military nature, even if they were to be adopted as pre-emptive measures.

Key words: infosphere, cybersecurity, European Union, Federal Republic of Germany

Data przekazania tekstu: 21.10.2024; data zaakceptowania tekstu: 15.11.2024.
Article submitted: 21.10.2024; article accepted: 15.11.2024.