Agnieszka Brzostek*

Cyfrowa suwerenność państwa jako cel niemieckiej strategii cyberbezpieczeństwa z 2021 roku

Streszczenie

Nowa strategia cyberbezpieczeństwa Niemiec z 8 września 2021 roku stworzyła podstawy strategiczne działania rządu federalnego w dziedzinie bezpieczeństwa na najbliższe 5 lat. Strategia jest wbudowana w europejską strategię cyberbezpieczeństwa i pomaga kształtować cyfrową przyszłość Europy. Dlatego rząd federalny postrzega cyberbezpieczeństwo jako wspólne zadanie państwa, biznesu, nauki i społeczeństwa. Wymaga to zorganizowanego podejścia i opartej na zaufaniu współpracy, żeby móc znaleźć wspólne odpowiedzi na cyberzagrożenia i zbudować cyfrową suwerenność państwa.

Słowa kluczowe: cyfrowa suwerenność, strategia cyberbezpieczństwa, polityka cyberbezpieczeństwa Niemiec

* Dr Agnieszka Brzostek, Instytut Prawa, Akademia Sztuki Wojennej, e-mail: a.brzostek@akademia.mil.pl, ORCID: 0000-0002-7444-0186.

Wstęp

Nasze życie kształtują możliwości zdigitalizowanego świata. Technologie takie, jak: sztuczna inteligencja (AI), sieciowe urządzania elektroniczne i nowe, innowacyjne kanały komunikacyjne, dokonują rewolucyjnych zmian w naszej codzienności, w życiu zawodowym czy w kontaktach z administracją publiczną. Coraz więcej procesów zostało przeniesionych do cyberprzestrzeni, a pandemia COVID-19 jeszcze bardziej wzmocniła tę tendencję. Już przed wybuchem pandemii COVID-19 pojawiały się postulaty dotyczące suwerenności cyfrowej oznaczającej niezależność oraz samostanowienie w odniesieniu do technologii cyfrowych w Niemczech i w Europie. Podczas pandemii okazało się, że dostęp do niektórych technologii w czasach kryzysu jest ograniczony i może prowadzić do ubezwłasnowolnienia gospodarki, np. półprzewodniki doprowadziły do skrócenia czasu pracy i jednocześnie spowodowały trudności produkcyjne w niemieckim przemyśle. Szczególną uwagę trzeba zwrócić na wzmacnianie Chińskiej Republiki Ludowej jako światowego lidera technologii i innowacji, geopolityczne konflikty i globalną konkurencję. Te przypadki, i wiele innych, pokazują, że utrzymanie i wzmocnienie suwerenności cyfrowej w przyszłości będzie odgrywać podstawową rolę w zapewnieniu zdolności do działania, a także zdolności do innowacji i zapewnienia konkurencyjności gospodarki[1]. Wszystkie te elementy niosą za sobą zwiększenie zagrożeń w cyberprzestrzeni. Państwo ma obwiązek ocenić i aktywnie kształtować szybki rozwój cyfryzacji w taki sposób, żeby zapewnić niezbędne warunki do wysokiego poziomu bezpieczeństwa i ochrony cyberprzestrzeni. Należy przyjąć, że ten rodzaj bezpieczeństwa jest gwarancją powodzenia cyfryzacji w dłuższym czasie. Nowa strategia cyberbezpieczeństwa Niemiec z 8 września 2021 roku[2] stworzyła podstawy strategiczne działania rządu federalnego na rzecz bezpieczeństwa na najbliższe 5 lat. Jest ona kontynuacją przyjętych przez rząd

1 M. Seifried, I. Bertschek, *Schwerpunktstudie Digitale Souveränität, Bestandsaufnahme und Handlungsfelder 2021*, Berlin 2021.

2 Cybersicherheitsstrategie für Deutschland 2021, s. 8, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=54839E13D7EBF107CCFCCDFFE002AC92.1_cid373?__blob=publicationFile&v=1 [dostęp: 20.03.2022].

federalny strategii w 2011[3] i 2016 roku[4]. Wszystkie wyznaczały kierunek przyszłej polityki bezpieczeństwa cybernetycznego[5]. Strategia jest wbudowana w europejską strategię cyberbezpieczeństwa i pomaga kształtować cyfrową przyszłość Europy[6]. Dlatego rząd federalny postrzega cyberbezpieczeństwo jako wspólne zadanie państwa, biznesu, nauki i społeczeństwa. Wymaga to zorganizowanego podejścia i opartej na zaufaniu współpracy, żeby móc znaleźć wspólne odpowiedzi na cyberzagrożenia. Zagrożenia cybernetyczne nie kończą się na granicach państwowych. Podobnie jak w wielu innych dziedzinach, Niemcy są włączone w sieć europejskiej i międzynarodowej współpracy w dziedzinie cyberbezpieczeństwa, dlatego cyberbezpieczeństwo można zagwarantować tylko we współpracy z europejskimi i międzynarodowymi partnerami. W ramach tej współpracy Niemcy, jako jedno z państw, wnioskowały do Unii Europejskiej o przyspieszenie działań mających na celu osiągnięcie cyfrowej suwerenności i lepszego wykorzystania jednolitego rynku cyfrowego[7]. W strategii z 2021 roku jako jeden z podstawowych celów wskazano

3 Cybersicherheitsstrategie für Deutschland 2011, https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf?__blob=publicationFile [dostęp: 22.03.2022].

4 Cybersicherheitsstrategie für Deutschland 2016, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf [dostęp: 22.03.2022]

5 Także „Biała Księga" z 2016 r. Zob. M.M. Kosman, *Niemcy wobec problemów bezpieczeństwa narodowego. Refleksje wokół „Białej Księgi" z 2016 r.* [w:] *Konflikty zbrojne i obronność na przełomie XX i XXI w. Aspekty polityczne i prawne*, red. Ł. Jureńczyk, P. Radziszewski, S. Sadowski, Bydgoszcz 2018; E. Cziomer, *Znaczenie „Białej Księgi 2016" dla oceny nowych wyzwań w polityce bezpieczeństwa Niemiec*, „Bezpieczeństwo. Teoria i Praktyka" 2017, nr 1.

6 Strategia z 2021 r. wpisuje się w politykę cyberbezpieczeństwa UE. W swoich założeniach zawiera, zgodnie z dyrektywą NIS, ramy sterujące w strategii (zob. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. Urz. UE 2016, L 194/1, art. 7, ust. 1, lit. b.), cele i priorytety oraz organy, które będą odpowiadać za osiągnięcie tych celów. Ważna w procesie budowania cyfrowej suwerenności jest dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (ibidem 2019, L 130/92). Obecnie trwają prace nad stworzeniem bezpiecznej przestrzeni cyfrowej, która będzie chronić wartości UE oraz prawa podstawowe i bezpieczeństwo obywateli, a jednocześnie zwiększać suwerenność cyfrową Europy. Zasadnicze znaczenie w tym względzie ma „cyfrowy kompas", czyli zaproponowana przez Komisję Europejską strategia określająca konkretne cele cyfrowe i etapy pośrednie do 2030 r. Postęp prac zob. https://www.consilium.europa.eu/pl/policies/a-digital-future-for-europe/ [dostęp: 28.03.2022].

7 M. Fraser, *Czym jest cyfrowa suwerenność i dlaczego warto w nią inwestować*?, https://cyberdefence24.pl/social-media/cybermagazyn-czym-jest-cyfrowa-suwerennosc-i-dlaczego-warto-w-nia-inwestowac [dostęp: 27.03.2022].

stworzenie cyfrowej suwerenności państwa. Do efektywnego wdrożenia tej strategii jest wymagane przyjęcie rozwiązań prawnych i organizacyjnych, a co najważniejsze, nieustanne monitorowanie i kontrola wyników.

Celem prezentowanego artykułu jest analiza prawnych i administracyjnych form działania federalnych organów na rzecz wdrożenia polityki opartej na suwerenności cyfrowej państwa. Dlatego należy rozważyć nie tylko kwestie definicyjne, lecz także rolę organów państwowych w prognozowaniu dalszego rozwoju, dla którego najważniejszy będzie proces monitowania i kontroli systemu cyfryzacji .

Cyfrowa suwerenność jako cel strategii cyberbezpieczeństwa z 2021 roku

Suwerenność oznacza „powyżej" lub „wyższy" (fr. *souveraineté*; łac. *superanus*) i można go przypisać różnym poziomom działania. Związany z jednostką oznacza bycie suwerennym, bycie pewnym siebie i lepszym ze względu na wykorzystanie własnych umiejętności i możliwość działania. Państwo lub jego rząd są suwerenne, gdy korzystają z suwerennych praw państwa. Na poziomie państwowym dokonuje się dalszego rozróżnienia między suwerennością wewnętrzną a zewnętrzną. Podstawowa niezależność państwa od innych państw oznacza suwerenność zewnętrzną, a suwerenność wewnętrzna to samostanowienie w sprawach własnej organizacji państwowej takiej, jak: typ rządu, system prawny i porządek społeczny. W dyskursie politologicznym pojęcie „suwerenność" jest interpretowane w sposób bardziej zróżnicowany. Oprócz wcześniej wspomnianej suwerenności wewnętrznej i zewnętrznej istnieje suwerenność współzależności. Opisuje ona skuteczną kontrolę transgraniczną, procesy wymiany. Czwarta forma interpretacji dotyczy międzynarodowej suwerenność prawnej, wskazuje na uznanie jako suwerenne państwo przez inne państwa. Termin „suwerenność" obejmuje różne aspekty i różne punkty widzenia[8].

Suwerenność cyfrowa już od 2016 roku była jednym z głównych celów działania rządu federalnego w dziedzinie cyberbezpieczeństwa. W strategii wyjaśniono, że suwerenność cyfrową należy rozumieć jako „zdolność i możliwość jednostek i instytucji do samodzielnego, samodzielnego i bezpiecznego

8 M. Seifried, I. Bertschek, op. cit.

pełnienia swojej funkcji w cyfrowym świecie”[9]. Wymaga ona suwerenności technologicznej obejmującej oprogramowanie, sprzęt i architekturę[10].

W niemieckiej literaturze suwerenność cyfrowa jest rozumiana jako wiedza na temat zastosowania technologii i wynikających z tego konsekwencji. Jednocześnie jest ona niezbędnym warunkiem kształtowania procesu transformacji cyfrowej. Ponieważ rozwój technologiczny dokonuje się bardzo szybko, należy więc uwzględnić procesy poznawcze, które stają się działaniami projektowymi przyszłego społeczeństwa cyfrowego. Istotne jest także to, żeby podążać za nim. Zauważa się, że priorytetowym wyzwaniem jest osiągnięcie dojrzałości cyfrowej, gdyż pewna niedbałość w tej dziedzinie uniemożliwia cyfrową suwerenność. Cyfrowa suwerenność jest możliwa poprzez cyfrową dojrzałość zarówno jednostki, jak i prywatnych firm oraz państwa i jego instytucji[11]. Na poziomie europejskim suwerenność cyfrowa oznacza zwiększenie powiązania polityki gospodarczej i polityki bezpieczeństwa ze strategicznymi partnerami w celu zmniejszenia należności i zachowania zdolności do działania i kształtowania polityki[12].

Ponieważ suwerenność cyfrowa ma podstawowe znaczenie dla bezpieczeństwa cybernetycznego i informacyjnego, więc niezbędnymi, wstępnymi warunkami jej zaistnienia są bezpieczne technologie i rozwiązania, umiejętności rozpoznania i oceny możliwości potencjonalnych zagrożeń związanych z technologiami cyfrowymi. Wysoki poziom bezpieczeństwa cybernetycznego przyczynia się do wzmocnienia suwerenności cyfrowej w każdym aspekcie życia publicznego i społecznego, czyli, jak wskazuje to strategia: obywateli, biznesu, nauki i państwa. Dlatego właśnie suwerenność cyfrowa stała się główną wytyczną strategii bezpieczeństwa cybernetycznego z 2021 roku zobowiązującą do działania w następujących obszarach:

1) badania nad aplikacjami i upowszechnianiem badań;
2) cyberbezpieczeństwo jako cecha jakości – „Made in Germany”;
3) zdolność państwa do oceny nowych technologii, jako europejski dostawca, oraz budowa niemieckiej bezpiecznej administracji;

9 Cybersicherheitsstrategie für Deutschland 2021..., s. 23.

10 *Schlüsselaspekte digitaler Souveränität*, https://gi.de/fileadmin/GI/Allgemein/PDF/Arbeitspapier_Digitale_Souveraenitaet.pdf [dostęp: 28.03.2022]. Zob. też S. Werden, *Digitale Souveränität, ein Orientierungsversuch* [w:] *Digitale Souveränität. Vertrauen in der Netzwerkgesellschaft*, red. M. Friedrichsen, P.-J. Bisa, Wiesbaden 2016, s. 35.

11 V. Wittpahl, *Digitale Souveränität: Bürger, Unternehmen, Staat*, Berlin 2017.

12 Cybersicherheitsstrategie für Deutschland 2021..., s. 23.

4) suwerenność całkowita poprzez wspólną wizję i strategię cyberbezpieczeństwa UE[13].

Wskazane obszary świadczą o złożoność procesu suwerenności cyfrowej, zwłaszcza ze względu na jego różnych uczestników. Oznacza to, że suwerenność cyfrowa jest postrzegana w sposób zróżnicowany i różnorodny, w zależności od pola działania. Wobec tego nasuwa się pytanie: jak osiągnąć ten cel? Przede wszystkim istotna jest tutaj organizacja państwa w zakresie cyberbezpieczeństwa.

Jak osiągnąć suwerenność cyfrową? Organizacja państwa w zakresie cyberbezpieczeństwa

Dyrektywa NIS nałożyła na państwa członkowskie obowiązek utworzenia organów właściwych w zakresie bezpieczeństwa sieci i informacji. W Niemczech na poziomie federalnym zmiany legislacyjne zostały już wcześniej zawarte w ustawie o Federalnym Urzędzie Bezpieczeństwa Teleinformatycznym z 2009 roku[14] i w ustawie o zwiększeniu bezpieczeństwa systemów teleinformatycznych z 2015 roku[15], dlatego po implementacji dyrektywy NIS do prawa federalnego wprowadzono stosunkowo niewiele zmian[16]. Przepisy wdrażające dyrektywę przyjęto na podstawie ustawy w 27 kwietnia 2017 roku[17].

W strategii cyberbezpieczeństwa z 2021 roku podkreśla się, jak w poprzednich strategiach, że za podstawowe działania na rzecz cyberbezpieczeństwa odpowiadają: Krajowa Rada Cyberbezpieczeństwa (Cyber-Sicherheitsrat – NCSR), Narodowe Centrum Cyberobrony (Nationale Cyber-Abwehrzentrum

13 Ibidem.

14 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG), https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Gesetz/bsi-gesetz_node.html [dostęp: 20.03.2022].

15 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0), https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig_2-0.html [dostęp: 20.03.2022].

16 D. Adamiec i in., *Informacja na temat legislacji dotyczącej systemu cyberbezpieczeństwa w wybranych państwach Unii Europejskiej (Belgia, Czechy, Estonia, Francja, Holandia, Niemcy, Szwecja)*, „Zeszyty Prawnicze" 2021, nr 3, s. 300–301.

17 Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis-richtlinienumsetzungsgesetz.html [dostęp: 26.03.2022].

– NCAZ, Cyber A-Z) oraz Centralne Biura Informatyki w Sektorze Bezpieczeństwa (Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich – ZITiS). Obecna strategia podkreśla znaczenie NCSR i jej roli jako strategicznego doradcy rządu federalnego[18]. Realizacja specyfikacji i celów strategicznych odbywa się przede wszystkim przez organy wyodrębnione w kancelarii federalnej i ministerstwa. Działania federalne obejmują dwa poziomy, tj. strategiczny i operacyjny. Poziom strategiczny tworzą ministerstwa, które odpowiadają za projekty dotyczące cyberbezpieczeństwa oraz sprawują nadzór nad ich realizacją. Na poziomie federalnym za wewnętrzną politykę cyberbezpieczeństwa odpowiada Federalne Ministerstwo Spraw Wewnętrznych i Ojczyzny, (Bundesministeriums des Innern und für Heimat – BMI) oraz Ministerstwo Spraw Zagranicznych – za cyberbezpieczeństwo polityki zagranicznej. Za cyberobronę odpowiada Federalne Ministerstwo Obrony (Bundesministerium der Verteidigung – BMVg)[19].

Poziom operacyjny obejmuje przede wszystkim działania Federalnego Urzędu ds. Bezpieczeństwa Informacji (Bundesamt für Sicherheit in der Informationstechnik –BSI) jako centralnej agencji rządu federalnego ds. bezpieczeństwa informacji. W jej skład wchodzą: Centrum Operacji Bezpieczeństwa (Bundes Security Operations Center - BSOC), Federalny Zespół Reagowania na Awarie Komputerowe (Computer Emergency Response Team für Bundesbehörden – CERTBund) oraz Krajowe Centrum Sytuacji IT (Nationales IT-Lagezentrum). Odpowiada za bezpieczeństwo i ochronę technologii informatycznych i sieci federalnych oraz krajowych infrastruktur krytycznych, a także za kształtowanie bezpieczeństwa informacji poprzez testowanie, standaryzację, certyfikację, zatwierdzanie i usługi konsultingowe dla państwa, biznesu i społeczeństwa oraz ściśle współpracuje z podmiotami ze wszystkich dziedzin[20].

Federalny Urząd Ochrony Konstytucji (Bundesamt für Verfassungsschutz – BfV) służy ochronie bezpieczeństwa wewnętrznego i informuje rząd federalny oraz opinię publiczną o stanie bezpieczeństwa. Odpowiada za gromadzenie informacji i ich ocenę o ekstremistycznych lub motywowanych terrorystycznie atakach cybernetycznych. Służba Kontrwywiadu Wojskowego (Amt für den militärischen Abschirmdienst – AD) stanowi osłonę Bundeswehry w zakresie szpiegostwa i sabotażu oraz przeciw ekstremizmowi i terroryzmowi w cyberprzestrzeni. Federalna Służba Wywiadowcza (Bundesnachrichtendienst – BND)

18 Cybersicherheitsstrategie für Deutschland 2021..., s. 55–56.
19 Ibidem, s. 19.
20 Ibidem, s. 19–20.

odpowiada za pozyskiwanie informacji o innych krajach, które mają znaczenie dla Niemiec z punktu widzenia polityki zagranicznej i bezpieczeństwa, także w celu ich gromadzenia i oceny w cyberprzestrzeni. Usługa domeny cybernetycznej i informacyjnej (Kommando Cyber- und Informationsraum – KdoCIR) koordynuje cyberobronę w Bundeswehrze[21].

W Niemczech kraje związkowe są odpowiedzialne za bezpieczeństwo w cyberprzestrzeni. W strategii podkreślono, że rząd federalny ma szczególne zadania wynikające z przepisów dotyczących zapobiegania zagrożeniom (np. związanych z terroryzmem międzynarodowym, bezpieczeństwa obiektów kolejowych kolei federalnych, ochrony granic czy bezpieczeństwa), w tym w cyberprzestrzeni. Zadania te wykonują Federalny Urząd Policji Kryminalnej (Bundeskriminalamt – BKA), Policja Federalna (Bundespolizei – BPOL) i BSI. Za ściganie w cyberprzestrzeni odpowiada wymiar sprawiedliwości ze wsparciem państwowych urzędów dochodzeniowo-śledczych i organów policyjnych państw lub przez BKA i BPOL w zakresie ich kompetencji. Współpraca pomiędzy wymienionymi i innymi właściwymi organami na poziomie operacyjnym odbywa się m.in. w Nationale Cyber-Abwehrzentrum (NCAZ lub Cyber-AZ) znajdującym się w strukturze BSI, który pełni funkcję centralnej informacji i platformy koordynacyjnej. Zadaniem Centralnego Urzędu Informatyki w Sektorze Bezpieczeństwa (Zentrale Stelle fur Informationstechnik im Sicherheitsbereich – ZITiS), jako dostawcy usług na rzecz organów bezpieczeństwa w Federalnym Ministerstwie Spraw Wewnętrznych, jest wzmocnienie umiejętności cybernetycznych i suwerenności cyfrowej. Ponadto w działania na rzecz cyberbezpieczeństwa są zaangażowane agencje wchodzące w skład rządu federalnego, którym powierzono zabezpieczenie federalnej infrastruktury IT. Należą do nich: Federalna Agencja Radia Cyfrowego dla Władz i Organizacji z Zadaniami Bezpieczeństwa (Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben – BDBOS) – federalny operator sieci, Federalne Centrum Technologii Informacyjnych (Informationstechnikzentrum Bund – ITZBund), a także Ministerstwo Spraw Zagranicznych – operator swojego międzynarodowego IT[22]. Konferencja Ministrów Spraw Wewnętrznych i jej krajowa grupa robocza ds. cyberbezpieczeństwa, Rada Planowania IT i jej grupa robocza ds. bezpieczeństwa informacji koordynują współpracę federalno-krajową na poziomie strategicznym. Te ostatnie są

21 Ibidem, s. 20.
22 Ibidem.

również odpowiedzialne za zarządzanie bezpieczeństwem informacji między władzami szczebla federalnego i krajów związkowych[23]. Istnieje wiele form współpracy między rządem federalnym a krajami związkowymi. Jest to przede wszystkim współpraca w ramach CERT (VCV) czy ścisła koordynacja urzędów policji kryminalnej krajów związkowych z BKA jako centralnym urzędem policji. W tę współpracę operacyjną są zaangażowane także centralne biura koordynacyjne ds. cyberbezpieczeństwa, tworzone coraz częściej przez kraje związkowe. Należy jeszcze wspomnieć, że krajowy system łącznikowy BSI kształtuje relacje BSI z partnerami z krajów związkowych i jest dostępny dla nich jako punkt kontaktowy na poziomie regionalnym[24].

Przyszłość suwerenności cyfrowej – inicjatywy i obawy rządu federalnego

Rząd federalny podjął różne inicjatywy i środki, żeby kształtować cyfrową zmianę w Niemczech. Obecna strategia wdrożeniowa „Kształtowanie cyfryzacji"[25] dotyczy różnych priorytetowych projektów wdrażania środków polityki cyfrowej, w tym w obszarach umiejętności cyfrowych, infrastruktury, cyfrowej transformacji państwa i społeczeństwa oraz etyki na rzecz społeczeństwa cyfrowego. Wraz z utworzeniem agencji cybernetycznej możliwe są międzywydziałowe projekty badawcze o wysokim potencjale innowacyjnym w dziedzinie cyberbezpieczeństwa i powiązanych kluczowych technologii w celu zaspokojenia potrzeb związanych z bezpieczeństwem wewnętrznym i zewnętrznym w Niemczech. Strategia sieciowa rządu federalnego z 2013 roku została zrewidowana i zaktualizowana o „Strategię sieci 2030 dla administracji publicznej"[26]. W ten sposób uwzględniono zwiększone wymagania wobec zdolności komunikacyjnych całej administracji publicznej w Niemczech, nowe

23 Ibidem, s. 21.

24 Ibidem. Zob. K. Chałubińska-Jentkiewicz, A. Brzostek, *Strategie cyberbezpieczeństwa współczesnego świata*, Warszawa 2021, s. 139–142.

25 Digitalisierung gestalten Umsetzungsstrategie der Bundesregierung, https://www.bundesregierung.de/breg-de/service/publikationen/digitalisierung-gestalten-1605002 [dostęp: 29.03.2022].

26 Netzstrategie 2030 für die öffentliche Verwaltung Bedarfsgerechte, leistungsfähige und sichere Netzinfrastrukturen für die öffentliche Verwaltung, https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/Moderne-Verwaltungskommunikation/netzstrategie_2030_fuer_die_oeffentliche_verwaltung.pdf?__blob=publicationFile [dostęp: 28.03.2022].

osiągnięcia techniczne oraz zwiększone wymagania wobec bezpieczeństwa. Celem jest utworzenie dla niemieckiej administracji publicznej (IVÖV) sieci informacyjnej, za którą będzie odpowiadał Federalny Operator Sieci (Bundesanstalt für den Digitalfunk der Behörden und Organisationem mit Sicherheitsaufgaben – BDBOS). W tym celu określono następujące cele strategiczne:

- narodowa suwerenność cyfrowa;
- wydajność infrastruktury sieciowej;
- bezpieczeństwo informacji oraz ochrona i poufność danych;
- zrównoważony rozwój i elastyczność;
- współpraca cyfrowa i międzypoziomowa.

„Strategia sieci 2030 dla administracji publicznej" jest zatem ważnym elementem zapewniającym bezpieczeństwo cybernetyczne w Niemczech[27].

Przyjęcie 12 lutego 2020 roku przez rząd federalny dokumentu na rzecz wzmocnienia przemysłu, bezpieczeństwa i obrony[28] ma na celu utrzymanie i wzmocnienie zdolności rozwojowych w Niemczech i w UE. Strategia ta określa podstawowe kierunki polityki rządu federalnego wobec sektora bezpieczeństwa i obrony, a zatem jest fundamentem ochrony suwerenności cyfrowej. Rząd federalny określił priorytetowe zadania w pięciu obszarach:

- wzmocnienie badań, rozwoju i innowacji;
- ustalenie warunków ramowych dla wydajnej produkcji;
- optymalizacja zakupów;
- wspieranie politycznie eksportu i jego odpowiedzialna kontrola;
- ochrona interesów bezpieczeństwa[29].

Z myślą o administracji publicznej rada planowania IT w marcu 2021 roku podjęła decyzję w sprawie „Strategii wzmocnienia suwerenności cyfrowej dla IT w administracji publicznej". Oprócz celów strategicznych: „opcji zmiany", „zdolności strukturyzacji" i „wpływu na dostawców", wdraża różne podejścia do rozwiązań i środki wzmacniające cyfrową suwerenność administracji. Prawnym regulacjom towarzyszy proces kształtowania umiejętności i wiedzy eksperckiej dotyczącej cyberbezpieczeństwa, a także zróżnicowania rozwiązań IT opartych na otwartym kodzie źródłowym[30].

27 Cybersicherheitsstrategie für Deutschland 2021..., s. 26.
28 Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie, https://www.bmwi.de/Redaktion/DE/Downloads/S-T/strategiepapier-staerkung-sicherits-und-verteidigungsindustrie.pdf?__blob=publicationFile&v=4 [dostęp: 27.03.2022].
29 Cybersicherheitsstrategie für Deutschland 2021..., s. 23.
30 Ibidem.

W strategii podkreślono: żeby osiągnąć suwerenność cyfrową i odporność na zagrożenia hybrydowe, należy przede wszystkim uniezależnić się od zagranicznych technologii informacyjnych. Oprócz mechanizmów testowych wynikających z ustawy o handlu zagranicznym i płatnościach oraz rozporządzenia w sprawie handlu zagranicznego[31] rząd federalny pracuje nad elastycznymi instrumentami, które będzie można wykorzystać w odpowiedzi na groźbę wyprzedaży przyszłych kluczowych i podstawowych technologii w dziedzinie bezpieczeństwa i przemysłu obronnego[32].

W strategii podkreślono, że rząd federalny zainicjował wiele przedsięwzięć w celu promowania bezpieczeństwa IT i aktywnego przeciwdziałania niepożądanym przejęciom. Można je podzielić na zadania w sferze funkcjonowania gospodarki, edukacji i innowacyjności.

Jeżeli chodzi o „wzmacnianie badań, rozwoju i innowacji", to latem 2020 roku została utworzona Agencja ds. Innowacji Cyberbezpieczeństwa GmbH (Agentur für Innovation in der Cybersicherheit GmbH). W celu zaspokojenia potrzeb Niemiec dotyczących bezpieczeństwa wewnętrznego i zewnętrznego agencja będzie inicjowała oraz finansowała projekty badawcze o wysokim potencjale innowacyjnym w dziedzinie bezpieczeństwa cybernetycznego i powiązanych kluczowych technologii[33]. Pod nazwą „Digitalisierung gestalten" rząd federalny ustanowił nowy program ramowy badań nad bezpieczeństwem IT. W dziedzinie edukacji oprócz badań i rozwoju w instytucie badawczym CODE Federalne Siły Zbrojne w Monachium prowadzą zajęcia i szkolenia głównie dla funkcjonariuszy federalnych i pracowników, z naciskiem na bezpieczeństwo cybernetyczne. W dziedzinie badań nad 6G rząd federalny ogłosił, że celem Niemiec jest przejęcie kierowniczej roli jako dostawcy godnej zaufania technologii komunikacyjnej w gospodarce światowej i pomoc w kształtowaniu zmian technologicznych na wczesnym etapie. W pierwszej kolejności jest planowana budowa czterech hubów badawczych 6G oraz platformy dla przyszłych technologii komunikacyjnych i 6G.

Rząd federalny, tworząc strategie cyberbezpieczeństwa, założył, że transparentność działań państwa jest ważna dla budowania zaufania obywateli do państwa, a to oznacza, że korzyści z inicjatyw rządowych muszą być dla

31 Außenwirtschaftsgesetz (AWG) sowie der Außenwirtschaftsverordnung (AWV) ergeben, https://www.bmwi.de/Redaktion/DE/Gesetze/Aussenwirtschaft/AWG.html [dostęp: 27.03.2022].

32 Cybersicherheitsstrategie für Deutschland 2021..., s. 23.

33 Ibidem.

społeczeństwa zrozumiałe. Dlatego mierzalność i przejrzystość zostały po raz pierwszy uwzględnione w strategii. Wdrożenie i przyszłe aktualizacje mogą być dzięki temu systematycznie przygotowywane. Wdrożenie założeń strategii powinno podlegać systematycznej ocenie na koniec okresu i regularnie sprawdzane w trakcie jej obowiązywania. W tym celu pożądane cele są formułowane w sposób mierzalny we wszystkich sferach działania. Wskaźniki są opracowywane dla każdego celu strategicznego, żeby móc sprawdzić stopień ich osiągnięcia. Dlatego rząd postawił pierwsze pytanie: co chcemy osiągnąć? Otóż, zbada, co trzeba zrobić, żeby rozwiązania dotyczące bezpieczeństwa stosowane w administracji federalnej mogły być promowane w sposób bardziej zrozumiały dla użytkowników lub rozwiązania przyjazne dla użytkownika mogły być zaprojektowane tak, żeby były bardziej bezpieczne[34]. Następne pytanie rządu dotyczyło oczekiwanego efektu. Rozwiązania przyjazne dla użytkownika, ergonomia, a także wydajność rozwiązań bezpieczeństwa odpowiadają wymaganym, pożądanym i równie oczekiwanym właściwościom dostępnych na rynku urządzeń i rozwiązań. Rozwiązania rynkowe są osiągane poprzez integrację właściwości bezpieczeństwa. Po zrewidowaniu kwestii rozwoju i bezpieczeństwa chęć inwestycyjna do wdrażania i stosowania rozwiązań związanych z bezpieczeństwem wzrośnie. Następne pytanie dotyczy tego, jak należy to zmierzyć? Rząd federalny sprawdzi, czy cel został osiągnięty poprzez:

– uwzględnienie w swoich przetargach wymagań dotyczących łatwości rozwiązywania problemów związanych z bezpieczeństwem;

– zintensyfikowanie badania i rozwój w obszarze przyjaznych dla użytkownika rozwiązań bezpieczeństwa. Tematy użytecznego bezpieczeństwa na etapie projektowania coraz częściej trafiają do programów i wytycznych finansowania badań;

– wzrost liczby dostępnych na rynku, przyjaznych dla użytkownika produktów, które mają zintegrowane funkcje bezpieczeństwa informatycznego, takie jak szyfrowanie typu end-to-end;

– wzrost wykorzystania produktów z funkcjami bezpieczeństwa IT[35].

Rząd federalny określił rolę BSI, która będzie prowadziła obserwację dostępności produktów i usług IT dla rynku konsumenckiego oraz własne testy tych produktów. BSI utworzyło centrum usług do udzielania podstawowych

34 Ibidem, s. 30.
35 Ibidem.

porad, rejestrowania, koordynacji, odpowiadania i dokumentowania zapytań kierowanych przez rządowe, biznesowe i społeczne grupy docelowe (wielokanałowe wsparcie pierwszego poziomu). Ponadto w BSI na stałe utworzono Radę Doradczą ds. Ochrony Konsumentów Cyfrowych (Beirat Digitaler Verbraucherschutz)[36].

Zakończenie

Niemiecka strategia cyberbezpieczeństwa z 2021 roku wpisuje się w europejską koncepcję cyberbezpieczeństwa, ze szczególnym naciskiem na budowę cyfrowej suwerenności państwa, uwzględniając przede wszystkim zdolność oraz możliwość jednostki i instytucji do samodzielnego i bezpiecznego pełnienia swojej funkcji w cyfrowym świecie. Sytuacja gospodarcza, a przede wszystkim geopolityczna i chęć niezależności technologicznej od Stanów Zjednoczonych Ameryki i Chin, a także skutki gospodarcze pandemii COVID-19 znacznie przyspieszyły proces dążenia do suwerenności cyfrowej. Założenia strategiczne, ich rozwinięcie w legislacji i wewnętrznych dokumentach rządowych będą skuteczne tylko w przypadku ciągłego monitoringu i analizy ryzyka. Dotyczy to zarówno poziomu państwowego, jak i makroekonomicznego[37]. Nie mniej istotny jest proces budowania umiejętności cyfrowych w społeczeństwie. Są to elementy niezbędne do utrzymania i wzmocnienia suwerenności cyfrowej. Suwerenność cyfrowa nie jest stanem statycznym, który można osiągnąć, ale jest dynamiczna i podlega ciągłym zmianom. Niemiecki rząd dostrzegł, że niezbędne dla niemieckiej gospodarki stało się inwestowanie w technologie cyfrowe, a także w umiejętności zachowania się w cyberprzestrzeni. Dla gospodarki suwerenność cyfrowa stanie się decydującym czynnikiem rozwoju w przyszłości.

36 Ibidem.
37 M. Seifried, I. Bertschek, op. cit.

Bibliografia

Adamiec D. i in., *Informacja na temat legislacji dotyczącej systemu cyberbezpieczeństwa w wybranych państwach Unii Europejskiej (Belgia, Czechy, Estonia, Francja, Holandia, Niemcy, Szwecja)*, „Zeszyty Prawnicze" 2021, nr 3.

Chałubińska-Jentkiewicz K., Brzostek A., *Strategie cyberbezpieczeństwa współczesnego świata*, Warszawa 2021.

Cziomer E., *Znaczenie „Białej Księgi 2016" dla oceny nowych wyzwań w polityce bezpieczeństwa Niemiec*, „Bezpieczeństwo. Teoria i Praktyka" 2017, nr 1.

Fraser M., *Czym jest cyfrowa suwerenność i dlaczego warto w nią inwestować?*, https://cyberdefence24.pl/social-media/cybermagazyn-czym-jest-cyfrowa-suwerennosc-i-dlaczego-warto-w-nia-inwestowac [dostęp: 27.03.2022].

Kosman M.M., *Niemcy wobec problemów bezpieczeństwa narodowego. Refleksje wokół „Białej Księgi" z 2016 r.* [w:] *Konflikty zbrojne i obronność na przełomie XX i XXI w. Aspekty polityczne i prawne*, red. Ł. Jureńczyk, P. Radziszewski, S. Sadowski, Bydgoszcz 2018.

Schlüsselaspekte digitaler Souveränität, https://gi.de/fileadmin/GI/Allgemein/PDF/Arbeitspapier_Digitale_Souveraenitaet.pdf [dostęp: 28.03.2022].

Seifried M., Bertschek I., *Schwerpunktstudie Digitale Souveränität, Bestandsaufnahme und Handlungsfelder 2021*, Berlin 2021.

Werden S., *Digitale Souveränität, ein Orientierungsversuch* [w:] *Digitale Souveränität. Vertrauen in der Netzwerkgesellschaft*, red. M. Friedrichsen, P.-J. Bisa, Wiesbaden 2016.

Wittpahl V., *Digitale Souveränität: Bürger, Unternehmen, Staat*, Berlin 2017.

Digital state sovereignty as the goal of the German cybersecurity strategy of 2021

Abstract

Germany's new cybersecurity strategy of September 8, 2021 has created a strategic framework for the federal government to act in the field of security for the next five years. The strategy is embedded in the European cybersecurity strategy and also helps shape Europe's digital future. Therefore, the federal government sees cybersecurity as a joint task of the state, business, science and society. This requires a structured approach and trust-based cooperation to be able to find common answers to cyber threats and build digital state sovereignty.

Key words: digital sovereignty, cybersecurity strategy, Germany's cybersecurity policy