Studia Bobolanum 28
nr 3 (2017): 41-56

Polityka bezpieczeństwa cybernetycznego RFN

Izabela Oleksiewicz

Politechnika Rzeszowska
Rzeszów

1. Podstawowe dokumenty RFN w polityce antycyberterrorystycznej

W 2009 r. opublikowano – w ramach Ministerstwa Spraw Wewnętrznych – *Narodową Strategię Ochrony Infrastruktury Krytycznej* (*Nationale Strategie zum Schutz Kritischer Infrastrukturen*)[1]. Dokument jest ogólny i w opinii autora raczej nie spełnia wymogów prawdziwej strategii. Brak przede wszystkim mierzalnych i wyraźnie określonych celów. Dokument wylicza inicjatywy i pakiety środków, w odniesieniu do bezpieczeństwa infrastruktury krytycznej, przyjęte przez Niemcy w poprzednich latach. Są to m.in. istniejące wewnętrzne akty prawne, podpisane umowy międzynarodowe, ćwiczenia z zarządzania kryzysowego LÜKEX (*Länderübergreifende Krisenmanagement Exercise* – które nie dotyczą jednak *stricte* bezpieczeństwa IT) oraz elementy programu *Badania dla bezpieczeństwa cywilnego* (*Forschung für die zivile Sicherheit*)[2]. *Strategia* zawiera również przykłady zagrożeń dla infrastruktury krytycznej – wśród nich nie znalazł się jednak cyberatak.

Strategię cyberbezpieczeństwa dla Niemiec przyjęto 23 lutego 2011 r.[3]. Jest to krótki i dosyć ogólny dokument, naświetlający jedynie podstawowe założenia polityki państwa oraz priorytetowe kierunki działań w omawianym obszarze. Mimo swojej zwięzłości zawiera jednak kilka konkretnych rozwiązań (już wdrożonych). Podobnie jak w przypadku generalnych założeń polityki bezpieczeństwa RFN, w wymiarze operacyjnym strategia

---

1 *Nationale Strategie zum Schutz Kritischer Infrastrukturen* (Berlin: Bundesministerium des Innern, 2009), 5-6.

2 Ta*mże*, 10-13.

3 *Cyber Security Strategy for Germany* (Berlin: Bundesministerium des Innern, 2011), 4-6.

stawia na wszechstronne podejście (*comprehensive approach*), którego głównymi elementami są wymiana informacji i koordynacja – zarówno w wymiarze krajowym, jak i międzynarodowym.

Strategia określa główne obszary, na których powinien skupić się rząd federalny. Przede wszystkim są to:

- ochrona krytycznych informacji i infrastruktury;
- zapewnienie bezpieczeństwa systemom IT w Niemczech;
- wzmocnienie bezpieczeństwa IT w administracji publicznej;
- efektywne zwalczanie przestępczości w cyberprzestrzeni;
- efektywna koordynacja działań na rzecz zapewnienia cyberbezpieczeństwa w Europie i na świecie;
- używanie godnych zaufania technologii informacyjnych;
- rozwijanie kadr w organach federalnych (weryfikacja już zatrudnionych zasobów oraz racjonalne planowanie);
- rozwój narzędzi odpowiedzi na cyberataki;
- utworzenie Narodowego Centrum Przeciwdziałania Cyberzagrożeniom (Nationales Cyber-Abwehrzentrum) i Narodowej Rady Cyberbezpieczeństwa (Nationaler Cyber–Sicherheitsrat).

Część powyższych zadań zakreślona jest dosyć ogólnie, natomiast *Strategia* zawiera również bardziej szczegółowe zalecenia. Przykładowo, w odniesieniu do punktu dotyczącego wzmocnienia bezpieczeństwa IT w administracji publicznej, autorzy dokumentu zakładają utworzenie wspólnej, uniwersalnej infrastruktury sieciowej dla administracji federalnej[4]. W zakresie prawa międzynarodowego przewiduje się podjęcie wysiłku legislacyjnego, aby zharmonizować niemieckie prawo karne z zaleceniami określonymi w Konwencji Rady Europy na temat cyberprzestępczości nr 185105. Niemcy rozważą również zasadność wypracowania analogicznych rozwiązań w ramach Narodów Zjednoczonych[5].

Na poziomie europejskim *Strategia* zakłada wsparcie dla „umiarkowanego zwiększenia" mandatu Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA – *European Network and Information Security Agency*)[6]. Dokument postuluje prace nad zwiększeniem stopnia współpracy międzynarodowej w omawianej dziedzinie na forum takich instytucji jak ONZ, OBWE, Rada Europy, OECD, G7/8 i NATO. Jednym z pomysłów jest stworzenie kodeksu postępowania państw w cyberprzestrzeni (nazwa-

[4] www.coe.int/cybercrime, dostęp 11 lipca, 2017.

[5] *Konwencja Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r.*, Dz.U. 2015, poz. 728.

[6] Izabela Oleksiewicz Krzysztof Michalski, Ewelina Sienkiewicz, *Bezpieczeństwo w społeczeństwie informacyjnym. Zagadnienia w wymiarze online i offline* (Warszawa: Oficyna Wydawnicza PRz, 2017), 45.

nego cyberkodem), który mógłby zawierać również środki budowy zaufania – rozwiązanie znane z bardziej tradycyjnych traktatów o współpracy wojskowej i wymianie informacji. Wychodząc z założenia, że NATO jest podstawą bezpieczeństwa transatlantyckiego, *Strategia* opowiada się za budowaniem cyberkompetencji Sojuszu – m.in. ustanowieniem jednakowych standardów bezpieczeństwa dla cywilnej infrastruktury krytycznej. Warto w tym miejscu zaznaczyć, że Niemcy regularnie biorą udział w cyberćwiczeniach NATO *Locked Shields.*

Strategia cyberbezpieczeństwa zawiera również słownik definicji. Jako cyberatak zdefiniowano atak IT w cyberprzestrzeni skierowany przeciw jednemu lub wielu systemom IT, mający na celu zmniejszenie bezpieczeństwa IT przez naruszenie prywatności, integralności lub dostępności danych. Jeśli cyberatak jest przeprowadzany lub zarządzany przez zagraniczne służby wywiadowcze, jest aktem cyberszpiegostwa. Cyberatak, który ma na celu osłabienie integralności lub dostępności systemów IT, jest aktem cybersabotażu. W opinii autora te definicje są dosyć wąsko lub nieprecyzyjnie nakreślone. Zawierają one również listę obszarów infrastruktury krytycznej na poziomie federalnym. Są to takie organizacje lub instytucje, które mają podstawowe znaczenie dla społeczeństwa, a ich brak lub uszkodzenie mogłoby doprowadzić do powstania wąskich gardeł zaopatrzeniowych, istotnych zakłóceń bezpieczeństwa publicznego lub innych dramatycznych konsekwencji[7].

W listopadzie 2016 r. opublikowano kolejną *Strategię cyberbezpieczeństwa dla Niemiec* (*Cyber-Sicherheitsstrategie für Deutschland 2016*)[8], która ma być kontynuacją poprzedniej. Nowa *Strategia 2016* określa ramy strategiczne dla działalności rządu federalnego z odniesieniami do cyberbezpieczeństwa. Wynika to z faktu, że wiele środków przewidzianych w poprzednim planie zostało już wdrożonych – np. powołanie Narodowego Centrum Przeciwdziałania Cyberzagrożeniom i stworzenie platformy dla strategicznej i operacyjnej wymiany między organami z cyberbezpieczeństwa jako punktu wymiany polityki i biznesu Narodowego Centrum Przeciwdziałania Cyberzagrożeniom – i stało się ważnym składnikiem w różnych koncepcjach strategicznych i rządowych. Zgodnie z wytycznymi nowej *Strategii* w konsekwencji rząd federalny RFN będzie musiał położyć nacisk na cyberpolitykę w nadchodzących latach w następujących czterech obszarach:

---

[7] Należą do nich następujące sektory: energia; technologia informacyjna i telekomunikacja; transport; zdrowie; woda; żywność; sektor finansowy i ubezpieczeń; państwo i administracja; media i kultura.

[8] *Cyber-Sicherheitsstrategie für Deutschland 2016* (Berlin: Bundesministerium des Innern, 2016), 4-9.

1. stworzenie bezpiecznych i autonomicznych podstaw prawnych do działania w środowisku cyfrowym;
2. tworzenie wspólnych programów w zakresie cyberbezpieczeństwa państwa i gospodarki;
3. wydajne i trwałe zapewnienie bezpieczeństwa systemom IT w Niemczech;
4. aktywna i efektywna koordynacja działań na rzecz zapewnienia cyberbezpieczeństwa Niemiec w Europie i na świecie.

Kolejnym istotnym elementem legislacji w dziedzinie cyberbezpieczeństwa jest ustawa z 17 lipca 2015 r. o zwiększeniu bezpieczeństwa systemów technologii informacyjnych (ustawa o bezpieczeństwie IT)[9]. Zawiera ona innowacyjne rozwiązania w zakresie bezpieczeństwa IT zarówno na poziomie państwowym, jak i dla podmiotów prywatnych (zwanych w ustawie „operatorami").

Zgodnie z § 3 ustawy dotyczy ona działalności podmiotów z obszaru infrastruktury krytycznej i wprowadza dla nich liczne obowiązki, które obejmują:

1. wdrożenie środków ochrony systemów IT pod rygorem otrzymania grzywny w wysokości do 100 tys. euro w ciągu dwóch lat od wejścia w życie aktów wykonawczych do ustawy, które będą zawierały szczegóły dotyczące tych środków w zakresie każdego sektora infrastruktury krytycznej[10];
2. regularną (nie rzadziej niż raz na dwa lata) kontrolę spełnienia standardów ochrony cybernetycznej. Działania dopuszczalne w tym zakresie to m.in. audyty bezpieczeństwa lub odnawianie certyfikatów. Operatorzy będą musieli przekładać sprawozdania z kontroli do BSI, który będzie mógł wnioskować o dalsze informacje lub podjęcie konkretnych środków;
3. wyznaczenie osoby do kontaktu z BSI;
4. obowiązek natychmiastowego poinformowania BSI o podejrzeniu cyberataku – zdefiniowanego jako istotne zakłócenie dostępności, integralności, autentyczności i poufności systemów IT, ich komponentów i procesów, które może doprowadzić lub doprowadziło do awarii lub upośledzenia funkcjonowania infrastruktury krytycznej.

[9] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBI. I S. 1324).

[10] Ustawodawca przewidział możliwość samoregulacji: operatorzy lub związki gospodarcze danego sektora będą mogły wypracować własne standardy w zakresie minimum wymagań bezpieczeństwa IT i wnioskować do Federalnego Urzędu Bezpieczeństwa Teleinformatycznego (BSI – Bundesamt für Sicherheit in der Informationstechnik) o ich uznanie.

Zgodnie z § 8a ust. 2 omawianej ustawy operatorzy infrastruktury krytycznej muszą przynajmniej raz na dwa lata dowieść implementacji i stosowania środków ochrony systemów IT. Taki dowód może polegać na przeprowadzeniu audytu IT lub uzyskaniu/odnowieniu odpowiedniego certyfikatu. Wymagania dotyczące poszczególnych sektorów zostaną określone w aktach wykonawczych do ustawy.

Specjalne obowiązki nałożono w myśl § 8c ustawy na operatorów telekomunikacyjnych. Muszą oni informować klientów o przypadkach ataków na ich łącza, np. o atakach typu „botnet"[11], oraz przechowywać dane o ruchu w sieci przez 6 miesięcy do celów dochodzeniowych. Istnieją zwolnienia z wyżej opisanych obowiązków, m.in. małe przedsiębiorstwa nie będą musiały wdrażać środków ochrony systemów IT, podobnie jak te podmioty, które zostały zobowiązane do implementacji takich lub podobnych środków na mocy oddzielnych ustaw (np. elektrownie). Według przewidywań rządu federalnego omawiany reżim powinien objąć nie więcej niż 2 tys. operatorów infrastruktury krytycznej. Krytycy ustawy wskazują na wysokie koszty dostosowania gospodarki do nowych standardów – prywatne szacunki oscylują wokół poziomu 1,1 mld euro rocznie. Nie podoba się im również prawo operatorów telekomunikacyjnych do przechowywania informacji o działaniach ich klientów w sieci[12]. Wreszcie, w ustawie nie określono jasno, jakiego typu zdarzenia podlegają obowiązkowi zgłoszenia do BSI – cyberataki przyjmują różne formy i nie wszystkie stanowią istotne zagrożenie. Sektor prywatny wskazywał również na obawy o utratę zaufania klientów, w razie gdyby informacje o ataku przedostały się do wiadomości publicznej.

Zgodnie z art. 6 ustawy o Telekomunikacji (TKG)[13] „dostawca usługi" inaczej „usługodawca" (*Diensteanbieter*) oznacza osobę, która w pełni lub częściowo komercyjnie świadczy usługi telekomunikacyjne lub uczestniczy w świadczeniu takich usług.

1.1. „Baza danych telekomunikacyjnych"

Warto dodać, że ustawa przewiduje uchwalenie licznych aktów wykonawczych, które zostaną pogrupowane zgodnie z poszczególnymi sektora-

---

[11] Skutecznie zainfekowany komputer łączy się z serwerem i czeka na polecenia od cyberprzestępcy. Wiele zainfekowanych w ten sposób komputerów, kontrolowanych przez jednego przestępcę lub grupę, nazywamy botnetami, http://di.com.pl, dostęp 7 lipca, 2017.

[12] Odbywa się to w myśl pkt 30 art. 3 ustawy telekomunikacyjnej (TKG). Mogą być one gromadzone, przetwarzane lub wykorzystywane do świadczenia usługi telekomunikacyjnej.

[13] Telekommunikationsgesetz vom 22.06.2004 (BGBI, I S. 1963).

mi infrastruktury krytycznej. W połowie 2015 r. niemiecka prasa doniosła o istnieniu tajnej strategii Bundeswehry na wypadek wojny w cyberprzestrzeni. Dokument nie jest publicznie dostępny (choć jego prawdopodobna treść została zamieszczona w Internecie), jednak wydaje się zasadne przytoczenie choćby pobieżnie spekulacji prasowych. Według tygodnika „Der Spiegel", Ministerstwo Obrony Narodowej ma planować znaczny rozwój kompetencji Niemiec w zakresie prowadzenia cyberkonfliktu. Istniejące zasoby miałyby zostać jeszcze bardziej zcentralizowane oraz dodatkowo rozwijane[14].

Według dokumentu, rząd federalny liczy się w przyszłości z atakami na niemieckie systemy IT, w tym na kluczową infrastrukturę, które mogą nosić znamiona ataku zbrojnego. Takie ataki będą stanowić coraz większe zagrożenie dla Niemiec z uwagi na ich postępującą digitalizację, usieciowienie oraz poleganie na technologiach typu „chmura obliczeniowa". Rozwijanie kompetencji armii w zakresie cyberbezpieczeństwa pozostaje w zgodzie z koncepcją „powiązanego bezpieczeństwa" (*vernetzte Sicherheit*), które jest rozwijane w Niemczech od wielu lat. W związku z tym, Internet i inne platformy komunikacji miałyby być postrzegane przez armię jako taki sam teatr wojny, jak ląd, morze i powietrze. Dokument wskazuje, że zasoby armii – w tym jej rozmaite platformy intranetowe i systemy obronne – muszą być chronione przed cyberatakami. Wspomina się również, że w przyszłości powinien zostać w Niemczech przeprowadzony audyt w zakresie zidentyfikowania i rozwijania kluczowych technologii IT[15].

Według doniesień, dozwolone miałyby być również operacje ofensywne, prowadzone zgodnie z ogólnymi regułami przeprowadzania operacji wojskowych. Przykładowo, podczas zagranicznych misji specjalne jednostki Bundeswehry mogłyby wspierać walczących na miejscu przez ograniczanie zdolności wroga do wykorzystywania Internetu i łączności mobilnej. Cyberataki na systemy przeciwnika miałyby się cechować wysoką skutecznością i precyzją, a tym samym w znaczący sposób uzupełniać tradycyjne zdolności Bundeswehry. W omawianym zakresie dokument planuje np. rozwijanie zdolności punktowego wydobywania informacji z systemów komunikacyjnych wroga. Wszelkie kompetencje powinny być

[14] *Germany passes strict cyber-security law to protect „critical infrastructure", 11.07.2015,* dostęp 7 lipca, 2017, https://www.rt.com/news/273058-german-cyber-security-law/.

[15] *Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg, 2015,* dostęp 7 lipca, 2017, https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/#Strategische-Leitlinie-Cyber-Verteidigung.

zarządzane centralnie oraz uprzednio rozwijane tak, aby możliwe było włączenie ich już na etapie planowania misji i operacji.

Armia powinna być również w stanie efektywnie odpowiedzieć (tj. przerwać wrogą operację, zminimalizować jej skutki, jak najszybciej przywrócić stan wyjściowy oraz móc zidentyfikować agresora) na atak na niemieckie systemy IT, który nosiłby znamiona ataku zbrojnego. Za tego typu zdarzenia w tajnym dokumencie konkretnie uznano ataki na sieci komunikacyjne i transportowe.

2. Realizacja polityki antycybertyterrorystycznej w RFN

Głównym organem federalnym w zakresie cyberbezpieczeństwa jest Federalny Urząd Bezpieczeństwa Teleinformatycznego (BSI – Bundesamt für Sicherheit in der Informationstechnik)[16], który podlega Ministerstwu Spraw Wewnętrznych. Urząd, który ma siedzibę w Bonn, powstał w 1991 r. Pełni on nadrzędną rolę koordynacyjną i wyznaczającą główne kierunki działań w obszarze cyberbezpieczeństwa, w tym ochrony infrastruktury krytycznej, bezpieczeństwa internetowego, kryptografii oraz certyfikacji i akredytacji produktów i audytorów bezpieczeństwa IT.

Ustawa o bezpieczeństwie IT zawiera wiele postanowień wzmacniających rolę BSI jako centralnego punktu gromadzącego i analizującego informacje w zakresie cyberbezpieczeństwa. Głównym zadaniem urzędu jest ocena raportów dotyczących potencjalnych cyberataków na infrastrukturę krytyczną. Urząd współpracuje m.in. z Federalną Służbą Wywiadu i Federalnym Urzędem Ochrony Konstytucji (jest to służba kontrwywiadowcza), a także z innymi organami w ramach Narodowego Centrum Przeciwdziałania Cyberzagrożeniom[17].

BSI pełni także istotną rolę informacyjną. W 2016 r. wydało raport o stanie bezpieczeństwa IT w Niemczech (*Die Lage der IT-Sicherheit in Deutschland 2016*)[18]. Zawiera on kompleksowy przegląd techniczny sła-

[16] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009 (BGBI. I S. 2821).

[17] Ustawa zgodnie z § 3 ustawy wyposażyła BSI w następujące kompetencje: wydawanie ostrzeżeń; wydawanie zaleceń odnośnie do środków bezpieczeństwa lub wykorzystania określonych produktów bezpieczeństwa; prawo do kontroli produktów i systemów IT; opracowanie minimalnych standardów cyberbezpieczeństwa dla infrastruktury federalnej, które zostaną przyjęte w formie aktów wykonawczych do ustawy o bezpieczeństwie IT.

[18] „Die Lage der IT-Sicherheit in Deutschland 2016", dostęp 11 lipca, 2016, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5.

bych punktów systemu i aktualnych zagrożeń. Utworzenie wielu organów państwowych, mających kompetencje w obszarze cyberbezpieczeństwa, przewidziała *Strategia* z 2011 r. Postulowano w niej powołanie Narodowego Centrum Przeciwdziałania Cyberzagrożeniom (*Nationales Cyber-Abwehrzentrum,* NCAZ) oraz Narodowej Rady Cyberbezpieczeństwa (*Nationaler Cyber-Sicherheitsrat*). Raport o stanie bezpieczeństwa IT w Niemczech opisuje i analizuje aktualną sytuację w zakresie bezpieczeństwa IT, przyczyny ataków cybernetycznych oraz środki i metody wykorzystywane podczas ataku[19].

Narodowe Centrum Przeciwdziałania Cyberzagrożeniom z siedzibą w Bonn jest platformą umożliwiającą współpracę organów niemieckiej administracji właściwych w sprawach ochrony cyberprzestrzeni. Organ rozpoczął działalność w kwietniu 2011 r. i według założeń ma być pierwszym ogniwem walki z zagrożeniami cybernetycznymi. Pracami zarządza przede wszystkim Federalny Urząd Bezpieczeństwa Teleinformatycznego (BSI) i to w jego strukturach działa Centrum. Do najważniejszych zadań Centrum należą przeciwdziałanie zagrożeniom dla cyberprzestrzeni oraz ich zwalczanie, w tym wymiana informacji, analiza incydentów teleinformatycznych i ich ewaluacja, wypracowywanie mechanizmów skutecznej ochrony i prewencji oraz neutralizacja rezultatów ataków, a także ocena skuteczności realizacji postanowień strategii ochrony cyberprzestrzeni. Zrzeszone w Centrum organy dostarczają informacje zgodnie z właściwością rzeczową – BSI ocenia incydent pod względem technicznym. W działalność NCAZ zaangażowanych jest wiele dalszych jednostek policyjnych i służb specjalnych: Federalny Urząd Ochrony Konstytucji (*Bundesamt für Verfassungsschutz* – BfVSchG)[20], Federalny Urząd Ochrony Ludności i Reagowania Kryzysowego (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe* – BBK)[21], Federalny Urząd Kryminalny (Bundeskriminalamt – BKA)[22], Federalna Służba Wywiadu (*Bundesnachrichtendienst* – BND)[23],

[19] Bundesamt für Sicherheit in der Informationstechnik, dostęp 11 lipca, 2014, https://www.bsi.bund.de.

[20] Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG) vom 20 Dezember 1990 (BGBI. I S. 2576).

[21] Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (Zivilschutz- und Katastrophenhilfegesetz – ZSKG) vom 25.03.1997 (BGBI. I S. 726).

[22] Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt z 25.12.2008 r. BGBI. I. S. 3083).

[23] Gesetz über den Bundesnachrichtendienst (BND – Gesetz – BNDG) vom 20 Dezember 1990 (BGBI. I S. 2576).

Celny Urząd Kryminalny (*Zollkriminalamt* – ZKA)[24] oraz policja federalna (*Bundespolizei* – BPol)[25]. Do prac NCAZ oddelegowana została także Bundeswehra.

BfVSchG bada, czy za atak odpowiada zagraniczna służba specjalna, a BBK ocenia skutki zamachów dla infrastruktury krytycznej. Pozostałe organy rozpoznają nowe metody i narzędzia ataku. W konsekwencji NCAZ potrafi w krótkim czasie przedstawić aktualną i kompleksową informację na temat zagrożeń dla cyberprzestrzeni. W ramach działań prewencyjnych NCAZ okresowo, a dodatkowo w razie potrzeby, przedstawia Narodowej Radzie Cyberbezpieczeństwa stosowne wytyczne, a w sytuacjach nadzwyczajnych składa raport bezpośrednio sztabowi kryzysowemu w MSW[26].

Przedmiotem zmian legislacyjnych w wymienionych aktach prawnych jest to, że agencjom ochrony, takim jak Federalny Urząd Ochrony Konstytucji, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Federalnego czy Celny Urząd Kryminalny i Federalny Urząd Policji Kryminalnej zapewniono niezbędne kompetencje dochodzeniowo-śledcze w tym zakresie, włącznie z cyberprzestępczością. Mogą one także pozyskiwać stosowne informacje od władz migracyjnych. Dopiero gdy wszystkie niemieckie władze zostały w pełni zaangażowane w działania antyterrorystyczne, można uznać, że wejście w życie tej ustawy jest w stanie zapobiec terroryzmowi i zarazem daje możliwość stosowania zaostrzonej polityki migracyjnej podyktowanej względami bezpieczeństwa państwa[27].

Federalny Urząd Ochrony Konstytucji może stosować w warunkach określonych w § 8 ust. 2 zdanie 1 środki techniczne w celu określania położenia terminali mobilnych lub aktywnie podłączone do określonego urządzenia lub w celu ustalenia numeru karty. Środek jest dozwolony tylko w przypadku braku możliwości zastosowania innych środków technicznych wymienionych w zdaniu 1 w celu identyfikacji terminali na miejscu albo w celu ustalenia liczby urządzeń lub gdy ustalenie numeru karty jest o wiele trudniejsze. Dane osobowe osób trzecich mogą być pobierane przy okazji takiego działania, jeśli jest to nieuniknione ze względów technicz-

[24] Gesetz über das Zollkriminalamt und die Zollfahndungsämter (Zollfahndungsdienstgesetz – ZFdG) vom 16. August 2002 (BGBl. I S. 3202).

[25] Gesetz über die Bundespolizei (Bundespolizeigesetz – BPolG) vom 19. Oktober 1994 (BGBl. I S. 2978, 2979).

[26] Kamila Sacewicz, „Niemiecka strategia ochrony cyberprzestrzeni", *Przegląd Bezpieczeństwa Wewnętrznego,* nr 7 (2012): 132.

[27] Szerzej: Izabela Oleksiewicz, *Polityka antyterrorystyczna Unii Europejskiej* (Lublin: UMCS, 2013), 423.

nych, w celu osiągnięcia celu określonego w zdaniu 1. Takie osoby można tylko skazać na podstawie § 8a ust. 3 nr 1 i 2 pkt b.[28].

Natomiast zmiany w ustawie o Federalnym Urzędzie Policji Kryminalnej rozszerzyły zakres jej kompetencji śledczych w celu uwzględnienia niektórych poważnych typów przestępstw, a także wzmocniły uprawnienia Federalnego Urzędu Policji Kryminalnej zarówno jako centrali administracji, jak i federalnego kraju związkowego przez rozszerzenie jego uprawnienia na pozyskiwanie danych. Regulacje odnoszące się do prawa o cudzoziemcach miały zaś na celu:

- przyznanie organom bezpieczeństwa koniecznych prawnych kompetencji;
- wzmocnienie koniecznej wymiany danych pomiędzy władzami;
- zapobieganie przestępcom terrorystycznym przyjeżdżającym do Niemiec;
- poprawienie środków bezpieczeństwa w celu zapewnienia ustalenia tożsamości podczas procedury wizowej;
- umożliwienie tzw. powietrznym szeryfom (zbrojnym członkom Federalnej Straży Granicznej) wykorzystywania niemieckich statków powietrznych do zapewnienia i przywracania bezpieczeństwa oraz ochrony na pokładzie samolotu;
- zwiększenie środków do przeprowadzenia lepszej kontroli granicy;
- zidentyfikowanie ekstremistów, którzy już są obecni na terytorium Niemiec[29].

Według założeń ustawy z 20 grudnia 1990 r. Federalna Służba Wywiadowcza jest organem federalnym pod jurysdykcją Urzędu Kanclerskiego. Dlatego też Departament Policji nie może być związany z Federalną Służbą Wywiadowczą, której zadaniem jest:

- gromadzenie i zbieranie informacji o obcych służbach wywiadowczych;
- wykorzystywanie informacji na temat zagranicznych państw, których polityka bezpieczeństwa może powodować implikacje polityczne dla Republiki Federalnej Niemiec;
- przetwarzanie niezbędnych informacji w celu zwiększenia bezpieczeństwa RFN.
- Dlatego też BNDG ma w myśl § 2 ustawy następujące kompetencje:

1. ma prawo chronić swoich ludzi, miejsca, przedmioty i środki, aby wpłynąć w ten sposób na bezpieczeństwo państwa;
2. może podejmować działania niezbędne do kontroli bezpieczeństwa osób, które pracują dla BNDG;

[28] Szerzej: Raport RFN dla ONZ dok. nr S/AC.37/2003/(1455)/10.

[29] Oleksiewicz, *Polityka antyterrorystyczna,* 436.

3. ma prawo weryfikacji wykonywanych zadań oraz dostępu do niezbędnych informacji;
4. jest odpowiedzialna za dostęp innych organów władzy do wydarzeń za granicą, które mają wpływ na polityczne bezpieczeństwo RFN.

Narodowa Rada Cyberbezpieczeństwa została powołana 23 lutego 2011 r. Jest organem koordynującym współpracę między organami administracji, a także z prywatnymi podmiotami, w tym głównie przedsiębiorcami. Na jej czele stoi pełnomocnik Rządu ds. Teleinformatycznych. W skład Rady wchodzą przedstawiciele: Urzędu Kanclerskiego, Ministerstwa Obrony, Ministerstwa Spraw Zagranicznych, Ministerstwa Spraw Wewnętrznych, Ministerstwa Gospodarki i Energii, Ministerstwa Sprawiedliwości i Ochrony Konsumenta oraz Ministerstwa Finansów, a także krajów związkowych (landów) oraz tzw. stowarzyszonych członków – prywatnych partnerów będących przedstawicielami niemieckiej gospodarki. Celem Rady jest przede wszystkim analiza dostępnych instrumentów prewencji oraz zadań politycznych przez przedstawicieli państwa i gospodarki. Organ spotyka się trzy razy do roku[30]. W razie potrzeby skład ten poszerzany jest o dalsze resorty, przedstawicieli biznesu i świata nauki. Przedmiotowemu organowi powierzono koordynację współpracy w obrębie niemieckiego rządu, a także na styku państwa i gospodarki.

Mimo że w Niemczech kompetencje z zakresu cyberbezpieczeństwa należą przede wszystkim do cywilnych jednostek, również i Bundeswehra ma pewne kompetencje w tym zakresie. Od 1 stycznia 2013 r. działa Centrum Operacyjne Systemów IT Bunderswehry (BITS – *Betriebszentrum IT-System der Bundeswehr*) z siedzibą w Rheinbach[31]. Jest to autonomiczna jednostka w ramach armii. W Centrum zatrudnionych jest ok. 600 żołnierzy i 80 pracowników cywilnych. Są oni podzieleni na cztery wydziały: zarządzania ryzykiem i bezpieczeństwem IT; zarządzania IT; planowania, zarządzania i realizacji oraz operacyjny.

Główne zadanie Centrum Operacyjnego sprowadza się przede wszystkim do ochrony systemów IT należących do Bundeswehry – nie tylko lokalnie, ale również np. na zagranicznych misjach i operacjach. W ramach tego nadrzędnego zadania jednostka może m.in. przeprowadzać ćwiczenia wewnątrz państwa, jak i poza jego granicami.

Ważnym punktem na mapie potencjału armii w cyberprzestrzeni jest Zespół Reagowania na Incydenty Komputerowe Bundeswehry (*Computer Emergency Response Team der Bundeswehr* – CERTBw), który rozpoczął działalność w 2002 r. w Euskirchen. Jego zadaniem jest monitorowanie,

[30] *Überblick: Cyber-Abwehr der Bundeswehr,* dostęp 7 lipca, 2017, http://www.bmvg.de/.

[31] cirbw.de umziehen, dostęp 7 lipca, 2017.

utrzymywanie i ewentualne przywracanie sprawności systemom IT Bundeswehry. Zespół zatrudnia ok. 60 specjalistów[32].

Warto wspomnieć również o jednostce badawczej – Centrum Badań Forschungszentrum Cyber Operational Defense (CODE), które działa w ramach Uniwersytetu Bunderswehry w Monachium[33]. Zadania omawianego organu skupiają się na przeciwdziałaniu i zwalczaniu zagrożeń w cyberprzestrzeni przez wymianę informacji, ocenę incydentów, opracowywanie mechanizmów ochrony i prewencji, usuwanie skutków ataków oraz analizę skuteczności strategii cyberbezpieczeństwa. NCAZ okresowo przedstawia wytyczne Narodowej Radzie Cyberbezpieczeństwa. W sytuacjach nadzwyczajnych Centrum podlega bezpośrednio sztabowi kryzysowemu w Ministerstwie Spraw Wewnętrznych.

* * *

Niemcy są państwem, w którym bezpieczeństwo cybernetyczne postrzegane jest jako istotne dobro publiczne. Nie jest to temat poboczny, a rządzący zdają sobie sprawę z wymierności strat powodowanych przez zaniechania w dziedzinie cyberbezpieczeństwa. W ciągu ostatnich lat doszło do kilku skandali, poczynając od kwestii szpiegostwa najwyższych urzędników państwowych ze strony USA, a kończąc na kolejnych doniesieniach prasowych o zawirusowanych komputerach najważniejszych polityków[34]. Jako państwo bazujące na rozwiniętych technologiach i będące w sposób ponadprzeciętny zglobalizowane, Republika Federalna Niemiec jest narażona na ataki w cyberprzestrzeni w wysokim stopniu. Zgodnie z szacunkami z 2011 r. ponad 70% dużych niemieckich przedsiębiorstw padło ofiarą cyberataku, a liczba i stopień złożoności takich incydentów są coraz wyższe[35].

W Niemczech już kilka lat temu podjęto wysiłek przyjęcia i usystematyzowania polityki antycyberterrorystycznej. Jednym z pierwszych aktów prawnych dotyczących cyberbezpieczeństwa był tzw. *Plan realizacji KRITIS – narodowy plan ochrony infrastruktury informacyjnej* (*Umsetzungsplan*

[32] bundeswehr.de: Startseite Bundeswehr, dostęp 11 lipca, 2017, https://www.bundeswehr.de.

[33] *Forschungszentrum Cyber Operations Defence* (*CODE*), dostęp 11 lipca 2017, http://www.kooperationssysteme.de/2013/04/05/forschungszentrum-cyber-operations-defence-code/lang-pref/de/.

[34] *Niemiecka agencja cyberbezpieczeństwa: poważne skutki ataku hakerów*, dostęp 7 lipca, 2017, http://www.cyberdefence24.pl/625839,niemiecka-agencja-cyberbezpieczenstwa-powazne-skutki-ataku-hakerow.

[35] Tamże.

KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen) z 2007 r. opracowany przez Ministerstwo Spraw Wewnętrznych[36]. Skupia się on na ochronie infrastruktury krytycznej, a jego adresatami są przede wszystkim prywatne przedsiębiorstwa działające w wybranych obszarach, ważnych z punktu widzenia zapewniania dóbr publicznych.

Niemcy niewątpliwie należą do państw, które poważnie traktują zagrożenia cybernetyczne. W Republice Federalnej opracowano nie tylko dokumenty o charakterze polityczno-programowym, jak *Strategia cyberbezpieczeństwa dla Niemiec z 2011 r.,* lecz przyjęto również ustawę, która porządkuje kompetencje organów i systematyzuje proces zapewniania bezpieczeństwa IT.

W niewielu państwach funkcjonuje podobne tak kompleksowe rozwiązanie prawne w omawianej dziedzinie. Warto dodać, że Berlin stara się, aby przyjmowane rozwiązania pozostawały w zgodzie z wytycznymi międzynarodowymi.

W odniesieniu do istniejącej siatki organów i instytucji zajmujących się bezpieczeństwem cybernetycznym należy stwierdzić, że słowem-kluczem jest koordynacja. Federalny Urząd Bezpieczeństwa Teleinformatycznego, który funkcjonuje w ramach Ministerstwa Spraw Wewnętrznych, oraz nadzorowane przez niego Narodowe Centrum Przeciwdziałania Cyberzagrożeniom spełniają funkcję integrującą informacje i kompetencje z różnych obszarów działalności federacji. Co ważne – istnieje platforma współpracy między organami cywilnymi i wojskowymi. Jest to efektywne rozwiązanie, zapobiegające dublowaniu kompetencji oraz pułapce braku adresata ważnej informacji. Najciekawszą cechą systemu stworzonego przez Niemcy jest wysoki stopień włączenia w tworzenie bezpieczeństwa cybernetycznego prywatnych operatorów infrastruktury krytycznej. Są oni nie tylko wykonawcą licznych obowiązków ustawowych, ale także partnerem – m.in. w ramach Narodowej Rady Cyberbezpieczeństwa. Na mocy Ustawy z 2015 r. biznes może również wprowadzać rozwiązania w typie samoregulacji.

Bibliografia:

Cyber Security Strategy for Germany. Berlin: Bundesministerium des Innern, 2011.

[36] *Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen* (Berlin: Bundesministerium des Innern, 2007), 10.

Cyber-Sicherheitsstrategie für Deutschland 2016. Berlin: Bundesministerium des Innern, 2016.

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009 (BGBI. I S. 2821).

Gesetz über das Zollkriminalamt und die Zollfahndungsämter (*Zollfahndungsdienstgesetz* – ZFdG) vom 16. August 2002 (BGBl. I S. 3202).

Gesetz über den Bundesnachrichtendienst (BND – Gesetz – BNDG) vom 20 Dezember 1990 (BGBI. S. 2576).

Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (*Zivilschutz- und Katastrophenhilfegesetz* – ZSKG) vom 25.03.1997 (BGBI. I S. 726).

Gesetz über die Bundespolizei (*Bundespolizeigesetz* – BPolG) vom 19. Oktober 1994 (BGBl. I S. 2978, 2979).

Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (*Bundesverfassungsschutzgesetz* – BVerfSchG) vom 20 Dezember 1990 (BGBI. I S. 2576).

Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt z 25.12.2008 r. BGBI. I. S. 3083).

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-*Sicherheitsgesetz*) vom 17. Juli 2015 (BGBI. I S. 1324).http://di.com.pl.

Konwencja Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r. Dz.U. 2015, poz. 728.

Nationale Strategie zum Schutz Kritischer Infrastrukturen. Berlin: Bundesministerium des Innern, 2009.

Oleksiewicz Izabela, Michalski Krzysztof, Sienkiewicz Ewelina. *Bezpieczeństwo w społeczeństwie informacyjnym. Zagadnienia w wymiarze online i offline*. Warszawa: Oficyna Wydawnicza PRz, 2017.

Oleksiewicz Izabela, *Polityka antyterrorystyczna Unii Europejskiej*. Lublin: UMCS, 2013.

Raport RFN dla ONZ dok. nr S/AC.37/2003/(1455)/10.

Sacewicz Kamila. „Niemiecka strategia ochrony cyberprzestrzeni". *Przegląd Bezpieczeństwa Wewnętrznego,* nr 7 (2012): 129-135.

Strafgesetzbuch (StGB) vom 15.05.1871 (BGBI, I S. 3083).

Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg, 2015. https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium

Telekommunikationsgesetz vom 22.06.2004 (BGBI, I S. 1963).

Überblick: Cyber-Abwehr der Bundeswehr. http://www.bmvg.de/.

Urheberrechtsgesetz (UrhG) vom 09.09.1965 (BGBI, I S. 3037). www.coe.int/cybercrime.

Polityka bezpieczeństwa cybernetycznego RFN

Streszczenie

Konstrukcja współczesnego modelu społeczeństwa informacyjnego, którego niezaprzeczalnym katalizatorem są technologie stosowane podczas komunikacji elektronicznej, przybierającej w wyniku konwergencji formę cyfrową, wyzwala potrzebę refleksji nad fenomenem informacji. Cyberprzestrzeń jest w modelu równoległą przestrzenią niefizyczną, niekonkurencyjną w stosunku do przestrzeni trójwymiarowej. Budulcem cyberprzestrzeni są dane i informacje, które przez wzajemne oddziaływania na siebie kreują mikrokorelacje.

Niemcy są państwem, w którym bezpieczeństwo cybernetyczne postrzegane jest jako istotne dobro publiczne. Nie jest to temat poboczny, a rządzący zdają sobie sprawę z wymierności strat powodowanych przez zaniechania w dziedzinie cyberbezpieczeństwa. W ciągu ostatnich lat doszło do kilku skandali na omawianym tle, poczynając od kwestii szpiegostwa najwyższych urzędników państwowych ze strony USA, a kończąc na kolejnych doniesieniach prasowych o zawirusowanych komputerach najważniejszych polityków. Jako państwo bazujące na rozwiniętych technologiach i będące w sposób ponadprzeciętny zglobalizowane, Republika Federalna Niemiec jest narażona na ataki w cyberprzestrzeni w wysokim stopniu.

Artykuł analizuje zmiany, jakie nastąpiły w strategii i w prawie niemieckim od 2009 r. w zakresie polityki antycyberterrorystycznej, a w szczególności na poziomie jej realizacji. Autorka podkreśla, że w niewielu państwach Unii Europejskiej funkcjonuje tak kompleksowe rozwiązanie prawne w omawianej dziedzinie, która porządkuje kompetencje organów i systematyzuje proces zapewniania bezpieczeństwa IT.

Słowa kluczowe: polityka antycyberterrorystyczna, RFN, cyberbezpieczeństwo, strategia Niemiec

Cybernetic Safety Policy of Federal Republic of Germany

Summary

The construction of a contemporary information society model whose an undeniable catalyst is the technology used in electronic communications which converts through convergence into digital form, triggers the need for reflection on the phenomenon of information. Cyberspace is in that model a spatial nonphysical parallel, non-competitive in relation to the three-dimensional space. The building material for cyberspace is data and information that, by interacting with each other, create – micro-correlations.

Germany is a country in which cyber security is perceived as an important public good. This is not a side issue, and the authorities are aware of the severity of losses caused by cyber-security failures. There have been several scandals over the above in the past few years, beginning with the issue of espionage of top government officials by the USA, and ending with subsequent press reports about the virus-infected computers of key politicians. As a state basing on high technology and being exceptionally globalised, the Federal Republic is exposed to cyber attacks in a high degree.

The article analyses the changes that have taken place in the strategy and in the German legislature since 2009 in the field of anti-cyber-terrorist policy, and in particular at the level of its implementation. The author tries to emphasise that in a few EU Member States there functions a similar comprehensive legal solution in the discussed field, which organises the competence of the authorities and systematises the process of IT security.

Keywords: anti-cyber-terrorist policy, Federal Republic of Germany, cyber security, German strategy