Przegląd Prawa Konstytucyjnego
-----ISSN 2082-1212-----
DOI 10.15804/ppk.2021.01.18
-----Nr 1 (59)/2021-----

**Agnieszka Brzostek**[1]

# Organy władzy publicznej w zakresie ochrony cyberbezpieczeństwa w wybranych strategiach cyberbezpieczeństwa[2]

**Słowa kluczowe**: konstytucja, systemy rządów, cyberbezpieczństwo, strategia cyberbezpieczeństwa, organy władzy publicznej
**Keywords**: constitution, systems of government, cybersecurity, cybersecurity strategy, public authorities

**Streszczenie**

Spójny system cyberbezpieczeństwa jest gwarantem bezpieczeństwa sieci. Zasadniczą rolę w jego organizacji, zarządzaniu i monitorowaniu odgrywa rząd i podlegle mu organy. W oparciu o konstytucyjne uprawnienia i obowiązujące prawo, organy władzy publicznej poszczególnych państw, tj. USA, Francji i Niemiec wpływają na kształt polityki poprzez stworzenie strategicznych planów działania w zakresie cyberbezpieczeństwa.

**Abstract**

## Public authorities competent in cyberspace protection in selected cybersecurity strategies

A consistent cybersecurity system is a guarantee of network security. The government and its subordinate bodies play a key role in shaping, organizing, managing and moni-

[1] ORCID ID: 0000-0002-7444-0186, doktor, Instytut Prawa, Akademia Sztuki Wojennej w Warszawie. E-mail: a.brzostek@akademia.mil.pl.

[2] Artykuł powstał w ramach Grantu Badawczego MON „System cyberbezpieczeństwa RP – model rozwiązań prawnych". Umowa MON Nr GB/4/2018/208/2018/DA, Zadanie nr 62.

toring it. Based on constitutional powers and applicable law, public authorities of individual countries, i.e. the USA, France and Germany, influence the shape of politics by creating strategic action plans in the field of cybersecurity.

*

## I.

Cyberprzestrzeń stała się elementem życia codziennego, wszechobecnym i tak oczywistym, ale jej działanie wymaga szczególnej ochrony przed zagrożeniami. Na poziomie rozwiązań globalnych i krajowych opracowywane są systemy, które ochronią i zapewniają ciągłość, a przede wszystkim bezpieczeństwo cybernetyczne. Główna rola w tym zakresie spoczywa na rządzie. Celem artykułu jest analiza systemowych rozwiązań, jakie zostały przyjęte przez rządy w wybranych krajach, tj. Stanach Zjednoczonych, Francji i Niemiec. Uwaga zostanie skupiona na rozwiązaniach prawnych określających kompetencje organów władzy publicznej w tym zakresie, zwłaszcza, że każde z tych państw dokonało już próby budowy spójnego systemu ochrony cyberprzestrzeni. Próby te można sprowadzić do kompleksu przedsięwzięć, prowadzonych wspólnie przez instytucje państwa, przedstawicieli IT i użytkowników sieci oraz systemów technologicznych. Oparte one zostały na ocenie zagrożeń w kontekście narodowym i pośrednio, wynikają także ze stanu zaawansowania technologicznego tych państw, powszechności usług teleinformatycznych oraz Internetu jako obszaru aktywności obywateli. Podstawą polityki ochrony przestrzeni cybernetycznej muszą być narodowe strategie, wynikające z uwarunkowań wewnątrzpaństwowych. Warto jednak wskazać na rozwiązania, które umożliwiają przeciwdziałanie zagrożeniom i które można próbować implementować do rozwiązań narodowych[3].

Strategia jest dokumentem politycznym, w którym dość szczegółowo opisano plany i zamierzenia, jakie poszczególny rząd chce realizować w polityce

[3] P. Mickiewicz, *System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, vol. 11, nr 1, s. 68–69.

wewnętrznej i co do zasady ma charakter otwarty[4]. W polityce wewnętrznej, najważniejsza jest współpraca rządu i powołanych agencji oraz współpracy organów właściwych w zakresie cyberbezpieczństwa z samorządem i przedsiębiorcami czy operatorami usług kluczowych, w celu wypracowania wspólnej, spójnej ochrony sfery cyberprzestrzeni. Określenie rodzaju zadań, jakie ma realizować system ochrony cybernetycznej, determinuje kształt jaki przyjmuje struktura organizacyjna, gdzie rozróżnieniem jest poziom centralizacji instytucjonalnej, które w każdym państwie funkcjonuje jako centralny organ koordynujący prowadzone działania. Podlegają mu instytucje niższego szczebla, których zadaniem jest koordynacja i kontrola sektorowych systemów ochrony cybernetycznej lub prowadzenie działań ochronnych. Zakres kompetencji zarówno organu centralnego, jak i podległych mu instytucji jest uzależniony od wizji prowadzenia polityki ochrony cybernetycznej[5].

## II.

Jak już zaznaczono, co do zasady, za kształt polityki w zakresie cyberbezpieczeństwa odpowiadają organy władzy wykonawczej, czyli rząd lub prezydent w zależności od systemu rządów[6]. W systemie prezydenckim w Stanach Zjednoczonych[7] całość władzy wykonawczej podporządkowana jest prezydentowi, co oznacza podporządkowanie wszystkich organów podległych i departamentów, poza wyjątkami wskazanymi w ustawie. Wyrazem tego podporządkowania jest sformułowana w Konstytucji zasada, że prezydent może żądać od kierowników departamentów, czyli najważniejszych komórek administracji federalnej, pisemnych opinii w każdej sprawie dotyczącej obowiązków tych urzędów, a także prawo do zmieniania rozstrzygnięć podejmowanych przez podporządkowane mu organy oraz prawo do wydawania przepisów prawnych

[4] M. Zajko, *Canada's cyber security the changing threat landscape*, „Critical Studies on Security" 2015, nr 3(2), s. 151–152.

[5] P. Mickiewicz, op.cit., s. 72.

[6] Szerzej: M. Podolak, M. Żmigrodzki, *System polityczny i jego kwalifikacje*, [w:] *Współczesne systemy polityczne*, red. M. Żmigrodzki, B. Dziemidok-Olszewska, Warszawa 2013, s. 28–30.

[7] Konstytucja odzwierciedla przyjęcie podstawowej zasady systemu rządów, a więc podziału władzy, zarówno w aspekcie rozdziału funkcji na szczeblu centralnym, jak i relacji federacja – stany; zob. *Ustroje państw współczesnych*, t. I, red. W. Skrzydło, Lublin 1992, s. 161.

w zakresie kierowania administracją federalną[8]. Zgodnie z postanowieniami Konstytucji to Prezydent Stanów Zjednoczonych jest organem odpowiedzialnym za bezpieczeństwo narodowe[9]. Amerykańska strategia cyberbezpieczeństwa[10] podpisana przez Prezydenta Donalda Trumpa 20 września 2018 r.[11] wskazała, że głównym priorytetem jest ochrona bezpieczeństwa narodowego Ameryki i promowanie dobrobytu narodu amerykańskiego, a zapewnienie bezpieczeństwa cyberprzestrzeni ma fundamentalne znaczenie dla obu tych przedsięwzięć. Potrzebę stworzenia nowej Strategii uzasadniono coraz liczniejszymi, uporczywymi i złośliwymi atakami Chin, Rosji, Iranu i Korei Północnej na podmioty amerykańskie. W odpowiedzi administracja pla-

[8] P. Sarnecki, *Ustroje konstytucyjne państw współczesnych*, Warszawa 2013, s. 112–114.

[9] Dokładnie w Konstytucji USA (Constutuion of United States of America) z 1787 r. w art. II, sekcji 2, klauzuli 1 wskazano, że Prezydent jest Naczelnym Wodzem armii i marynarki wojennej Stanów Zjednoczonych oraz milicji stanów w przypadku powołania jej do czynnej służby na rzecz Stanów Zjednoczonych; Prezydent może żądać od kierowników departamentów rządowych pisemnych opinii we wszystkich sprawach należących do kompetencji tych urzędów; zob. P. Laidler, *Konstytucja Stanów Zjednoczonych. Przewodnik*, Kraków 2007, s. 79. Szerzej na temat roli Prezydenta Stanów Zjednoczonych zob. M. Jagielski, *Prezydent USA jako szef administracji ogólnej,* Kraków 2000.

[10] Nie jest to pierwsza strategia cyberbezpieczeństwa. Pierwsze próby w tym zakresie podjął prezydent G.W. Bush. W ramach dyrektywy National Security Presidential Directive/NSPD-54 Homeland Security/Direcive/HSPD-23, https://fas.org/irp/offdocs/nspd/nspd-54.pdf (15.11.2020). Na podstawie dyrektywy opracowano główne założenia polityki cyberbepiczeństwa w USA dzieląc je na 12 obszarów inicjatyw zalecanych do wprowadzenia przez instytucje federalne, stanowe, przedsiębiorców i użytkowników. Zob. P. Mickiewicz, *System bezpieczeństwa narodowego, w rozwiązaniach systemowych wybranych państwach*, Warszawa 2018, s. 121; R. Lemos, *Bush unvelis final cybersecurity plan*, https://www.cnet.com/news/bush-unveils-final-cybersecurity-plan (17.11.2020). Podczas prezydentury B. Obamy problem cyberprzestrzeni był podnoszony w wielu aktach: *National Security Strategy 2010; White House International Strategy for Cyberspace 2011; Departament of Defense Strategy for Opearting in Cyberspace (US DoD) 2011; National Security Strategy 2015; Departament of Defense Cyber Strategy 2015; Departament of State International Cyberspace Policy Strategy (US Departament of State*). Zob. V. Weber, *Linking cyber strategy with the grand strategy: the case of the United States,* „Journal Cyber Policy" 2018, vol. 3, iss. 2, s. 5. Poza tematem artykułu pozostają strategie opracowywanie przez Departament of Defence (DoD), niemniej należy zaznaczyć, że takie zostały opracowane i wdrożone; zob. J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Warszawa 2020, s. 238–245.

[11] National Cyber Strategy of United States of America 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (16.11.2020).

nuje skuteczną identyfikację, ochronę i zapewniania odporności sieci, systemów, funkcji i danych poprzez ich wykrywanie, reagowanie i odzyskiwanie[12].

Główną rolę w zakresie realizacji tych postanowień powierzono Radzie Bezpieczeństwa Narodowego *(The National Security Council*) jako organowi właściwemu do planowania i koordynowania pracy z departamentami, agencjami oraz Biuru Zarządzania i Budżetu[13] (*The Office of Management and Budget* – OMB) w celu wdrożenia strategii[14]. Realizacja założeń wskazanych w strategii wymagała podjęcia organizacyjnych i prawnych środków. W dniu 16 listopada 2018 r. Prezydent D. Trump podpisał ustawę o Agencji Cyberbezpieczeństwa i Infrastruktury (*The Cybersecurity and Infrastructure Security Agency Act of 2018*), na mocy której powołano w ramach DHS[15] (*Departament of Homeland Security*) Agencję ds. Cyberbezpieczństwa i Infrastruktury (Cybersecurity & Infrastructure Agency – CISA)[16]. Zadaniem Agencji jest stworzenie organizacyjnych zdolności do obrony przed cyberatakami i współpraca z rządem federalnym w celu zapewnienia narzędzi, usług reagowania na incydenty i możliwości oceny w celu ochrony sieci „gov"[17]. Szczegółowo zostały określone zadania dyrektora, który realizuje program ochrony cyberbezpieczeństwa i infrastruktury krytycznej poprzez koordynację[18] działań realizo-

[12] Ibidem, Wstęp, s. 1.

[13] https://www.whitehouse.gov/omb (17.11.2020).

[14] National Cyber Strategy…, Wstęp, s. 1.

[15] Departament of Homeland Security (DHS) utworzony został przez Prezydenta G. W Busha po zamachach z 11 września 2001 r. dekretem z 8 października 2001 r. (Executive Order 13228 of October 8, 2001) w celu koordynacji służb bezpieczeństwa, wywiadowczych, śledczych i policji stanowej, https://www.dhs.gov (17.11.2020).

[16] https://www.cisa.gov (17.11.2020). CISA zastąpiła powołaną w 2007 r. Dyrekcję ds. Ochrony Narodowej i Programów (NPPD) była częścią DHS – zadania dotycząca reedukacji i eliminacji zagrożeń dla infrastruktury krytycznej i cybernetycznej USA; zob. J. Wrona, op.cit., s. 238–245.

[17] The Cybersecurity and Infrastructure Security Agency Act of 2018, H.R. 3359. https://www.congress.gov/bill/115th-congress/house-bill/3359 (17.11.2020).

[18] Sec. 2202 b 1–2 i sec.2202 c 1–3 H.R. 3359 – Cybersecurity and Instrastructure Security Agency Act of 2018, https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf (17.11.2020). Wskazano, że koordynacja ta ma dotyczyć kluczowych zasobów i infrastruktury krytycznej, w tym produkcji energii, systemu wytwarzania i dystrybucji, informacji technologicznych i systemu telekomunikacyjnego (w tym satelity), elektronicznego zapisu finansowego i majątkowego systemu magazynowania i przesyłu, awaryjnego systemu komunikacji.

wanych przez inne podmioty federalne[19]. Prezydent USA określił założenia wdrażania ryzyka wskazując na określone środki i sposoby weryfikacji efektów. Szefowie agencji odpowiadają personalnie przed prezydentem i składają sprawozdania z procesu wdrażania, a sekretarz Bezpieczeństwa Wewnętrznego i dyrektor OMB wspólnie oceniają merytorycznie każdy raport, który musi zostać wysłany do prezydenta w ciągu 60 dni po przesłaniu go przez agencje[20].

W strategii wskazano, że to rząd ponosi odpowiedzialność za zabezpieczanie infrastruktury krytycznej i zarządzanie ryzykiem cyberbezpieczeństwa[21]. W tym celu administracja ma za zadanie rozwinąć w sposób kompleksowy monitoring ryzyka krajowego poprzez identyfikację krajowych funkcji krytycznych, ustalając priorytety w siedmiu kluczowych obszarach: bezpieczeństwo narodowe, energia, bankowość i finanse, zdrowie i bezpieczeństwo, komunikacja, technologie informacyjne i transport. Rząd nadzoruje prace nad opracowywaniem i wdrażaniem standardów w zabezpieczeniu procesu wyborczego oraz realizacji projektów w obszarze nowych technologii. Wykonanie tych zamierzeń zakłada szeroką współpracę rządu z sektorem prywatnym[22].

W Strategii podkreślono również rozdzielenie kompetencji pomiędzy departamenty zajmujące się bezpieczeństwem. Kluczową rolę w zakresie zabezpieczenia federalnych sieci departamentów i agencji realizuje DHS, z wyjątkiem tych należących do Departamentu Obrony (DOD) i Wspólnoty Wywiadowczej Systemy (IC). W dokumencie wskazano na wiodącą rolę DHS i OMB jako organów kierowniczych w zakresie zarządzania ryzykiem w federalnych departamentach i agencjach cywilnych. DHS pełni funkcję nadzorczą w stosun-

[19] Ustawa wskazuje konkretne agencje – the Department of State; the Central Intelligence Agency; the Federal Bureau of Investigation; the National Security Agency; the National Geospatial-Intelligence Agency; the Defense Intelligence Agency; Sector-Specific Agencies i każda inna agencja wskazana przez Prezydenta. Zob. Sec. 2202 4 B H.R. 3359 – Cybersecurity and Instrastructure Security Agency Act of 2018, https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf (17.11.2020).

[20] Sec. 1 c Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure (17.11.2020).

[21] National Cyber Strategy…, s. 8.

[22] Ibidem, s. 8–9.

ku do podmiotów realizujących założenia systemu cyberbezpieczeństwa[23]. Pod nadzorem OMB, administracja ma zadanie rozszerzyć zakres prac rozpoczętych na mocy rozporządzenia wykonawczego Prezydenta D. Trumpa (E.O. 13800)[24]. Nie można też pominąć innego rozporządzenia Trumpa wydanego 18 maja 2018 r., którego celem jest zwiększenie skuteczności biura ds. informacji administracji[25] poprzez upoważnienie dyrektorów ds. informacji (CIOs) do skuteczniejszego wykorzystywania technologii w celu realizacji misji agencji, ograniczenia powielania działań i zwiększenia wydajności inwestycji w technologie informatyczne[26].

## III.

W nauce prawa konstytucyjnego wyróżnia się francuskie rozwiązania ustrojowe w postaci systemu rządów, który różni się od klasycznego systemu prezydenckiego sposobem powołania Prezesa Rady Ministrów i jego rządu[27]. Zgodnie z prerogatywami Konstytucji[28], Prezydent przewodniczy posiedzeniom rządu, podpisuje dekrety, obsadza stanowiska administracyjne i wojskowe oraz jest zwierzchnikiem Sił Zbrojnych[29]. Rząd prowadzi bieżącą politykę. Francuską strategię cyberbezpieczeństwa z 2015 r. poprzedziły wielopłaszczyznowe działania rządu w celu zwiększenia ochrony cyberprzestrzeni[30].

---

[23] Ibidem, s. 6–7.

[24] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure z 11.05.2017.

[25] E.O. 13833 Enhancing the Effectiveness of Agency Chief Information Officers, Federal Register (May 18, 2018), v. 83 no 97, p. 23345.

[26] National Cyber Strategy…, s. 6–7.

[27] P. Sarnecki, op.cit., s. 227.

[28] Art. 9 i 13 Konstytucji Republiki Francuskiej z 4 października 1958 r. http://libr.sejm.gov.pl/tek01/txt/konst/francja.html (20.11.2020).

[29] W. Żebrowski, *Współczesne systemy polityczne. Zarys teorii i praktyka w wybranych państwach świata*, Olsztyn 2007, s. 55–56; zob. A. Jackiewicz, *Republika Francuska*, [w:] *Ustroje konstytucyjne wybranych państw europejs*kich, red. S. Bożyk, Warszawa 2020, s. 52–55.

[30] Republika Francuska jest jedynym państwem Unii Europejskiej, której celem polityki bezpieczeństwa cybernetycznego jest także rozwój zdolności o charakterze ofensywnym, pozwalających na wsparcie operacji wojskowych (Livre Blanc 2013, s. 72). Założenie to powoduje, że podsystem militarny ochrony cybernetycznej funkcjonuje samodzielnie,

Przede wszystkim określono, że to Prezes Rady Ministrów ustala politykę i koordynuje działania rządu w zakresie cyberbezpieczeństwa i cyberobrony. W tym celu do dyspozycji ma Krajową Agencję Cyberbezpieczeństwa i ANSSI. W 2009 r. rząd francuski[31] powołał Narodową Agencję Bezpieczeństwa Systemów Informatycznych (ANSSI)[32], jako służbę o kompetencjach krajowych przy Generalnym Sekretariacie Obrony i Bezpieczeństwa Narodowego (SGDSN) z upoważnienia Prezesa Rady Ministrów. ANSSI ma za zadania zapewnić bezpieczeństwo systemów informatycznych państwa i zapewnić bezpieczeństwo krajowych operatorów o kluczowym znaczeniu, koordynować działania obronne systemów informacyjnych, projektować i wdrażać bezpieczne sieci, które odpowiadają potrzebom organów państwowych oraz tworzą warunki bezpieczeństwa sprzyjającego rozwojowi społeczeństwa informacyjnego we Francji i w Europie[33]. W systemie kierowania istotną role odgrywa Komitet Strategiczny Bezpieczeństwa Systemów Informatycznych, którego zadaniem jest koordynacja podejmowanych działań i wdrażanie rozwiązań systemowych w zakresie IT[34].

---

a nadzór nad tymi przedsięwzięciami sprawuje minister obrony; P. Mickiewicz, op.cit., s. 68. Zob. Ustawa z 18 grudnia 2013 r. w sprawie programowania wojskowego na lata 2014–2019 i odnosząca się do różnych przepisów dotyczących obronności i bezpieczeństwa narodowego, nr 2013–1168. LOI n° 2013–1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité national, https://www.legifrance.gouv.fr/affichLoiPreparation.do?idDocument=JORFDOLE000027803764&type=general (17.11.2020).

[31] Było to przede wszystym skutkiem podjęcia ochrony cyberprzestrzeni przez prezydenta Francji Nicolasa Sarkozy w 2008 r. zapoczątkowanej opublikowaniem Białej Księgi. Défense et Sécurité nationale. Le livre Blanc (Biała Księga obrony i bezpieczeństwa narodowego) wydana w 2008 r.; szerzej: D. D'Elia, *Industrial policy: the holy grail of French cybersecurity strategy*, „Journal of Cyber Policy" 2018, vol. 3, s. 386.

[32] Agence nationale de la sécurité des systèmes d'information (Krajowa Agencja Bezpieczeństwa Systemów Informatycznych) utworzona 7 lipca 2009 r. dekretem: Décret n° 2009–834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212&dateTexte=&categorieLien=id (20.11.2020).

[33] O. Kempf, *La cyberstratégie française*, „Recherches internationals", n° 100, juillet-septembre 2014, s. 138, https://www.recherches-internationales.fr/RI100/RI100OlivierKempf.pdf (17.11.2020).

[34] P. Mickiewicz, op.cit., s. 173.

Strategia[35], ogłoszona przez premiera Francji 16 października 2015 r.[36], zakładała stworzenie eksperckiego zespołu ds. zaufania cyfrowego pod egidą Sekretariatu Stanu ds. Technologii Cyfrowych oraz ANSSI. Skład zespołu stanowią premier oraz przedstawiciele ministerstw (edukacji, szkolnictwa wyższego, sprawiedliwości, obrony, spraw społecznych, zdrowia i praw kobiet, gospodarki, przemysłu oraz technologii cyfrowej, spraw wewnętrznych), komisji generalnej ds. inwestycji, Krajowej Agencji Badań oraz zainteresowane organizacje badawcze, przedstawiciele sektora prywatnego i eksperci. Misją tego zespołu jest w szczególności rozwój środowiska cyfrowego w oparciu o nowe technologie w edukacji i w przemyśle. Ze swojej działalności zaspół składa coroczne sprawozdania premierowi[37].

Należy podkreślić, za P. Mickiewiczem, że Republika Francuska jest jedynym państwem Unii Europejskiej, w którym celem polityki bezpieczeństwa cybernetycznego jest także rozwój zdolności o charakterze ofensywnym, pozwalających na wsparcie operacji wojskowych, na podstawie Białej Księgi z 2013 r. Założenie to powoduje, że podsystem militarny ochrony cybernetycznej funkcjonuje samodzielnie, a nadzór nad tymi przedsięwzięciami sprawuje minister obrony[38].

## IV.

W Republice Federalnej Niemiec konstytucyjny system relacji między naczelnymi organami opiera się na zasadzie trójpodziału władzy polegającej

---

[35] Pierwszą Strategię Cyberbezpieczeństwa wydano w 2011 r. – Stratégie de la France, Défense et sécurisent des systèmes d'information. 2011, https://www.ssi.gouv.fr/uploads/IMG/pdf/2011–02–15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf, s. 8 (17.11.2020). Na temat strategii zob. też. C. Guitton, *Cyber insecurity as a national threat: overreaction from Germany, France and the UK?*, „European Security" 2013, 22(1), s. 21–35.

[36] Francuska narodowa strategia bezpieczeństwa cyfrowego (fr. Stratégie nationale pour la sécurité du numérique) 2015, https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques (17.11.2020).

[37] Ibidem, s. 15.

[38] P. Mickiewicz, op.cit., s. 68–69.

na założonym współdziałaniu organów należących do władzy ustawodawczej i wykonawczej[39]. Zgodnie z art. 62 ustawy zasadniczej z 1949 r. rząd federalny składa się z kanclerza i ministrów. Kanclerz Federalny ustala politykę rządu i ponosi za nią odpowiedzialność. W ramach wytycznych Kanclerza każdy minister federalny kieruje samodzielnie i na własną odpowiedzialność swoim resortem[40].

Niemiecki system cyberbezpieczeństwa, w przeciwieństwie do francuskiego, oparty jest na zdecentralizowanej formie działania organów. Niemiecka strategia cyberbezpieczeństwa z 2016 r.[41] określiła cele rządu federalnego w polityce wewnętrznej i zagranicznej[42] i powołała Narodowe Centrum Przeciwdziałania Zagrożeniom dla Cyberprzestrzeni (*Nationales Cyber-Abwehrzentrum* – NCAZ). Zadaniem NCAZ jest koordynacja współpracy operacyjnej między wszystkimi organami państwowymi i reagowania na incydenty informatyczne. Centrum podlega Federalnemu Urzędowi ds. Bezpieczeństwa Informacji (BSI) i współpracuje bezpośrednio z Federalnym Urzędem Ochrony Konstytucji (BfV) oraz Federalnym Urzędem Ochrony Ludności i Pomocy w przypadku katastrof (BBK)[43]. Następnym krokiem było powołanie Narodowej Rady Bezpieczeństwa Cybernetycznego (*Nationaler Cyber-Sicherheit-*

---

[39] Ustawa zasadnicza z 24 maja 1949 r. Grundgesetz für die Bundesrepublik Deutschland, https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl149001.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl149001.pdf%27%5D__1606518267858 (18.11.2020); zob. P. Sarnecki, op.cit., s. 179.

[40] Art. 65 ustawy zasadniczej z 1949 r. http://libr.sejm.gov.pl/tek01/txt/konst/niemcy.html (20.11.2020). Szerzej: S. Bożyk, *Republika Federalna Niemiec*, [w:] *Ustroje konstytucyjne wybranych…*, s. 31.

[41] Strategia cyberbepieczństwa Niemiec 2016 (niem. Cyber- Sicherheitsstrategie für Deutschland 2016), s. 9, https://jaeger.uni-koeln.de/fileadmin/templates/Allgemeines/AIPA_Die_Cyber-Sicherheitsstrategie_fuer_Deutschland_Stephan_Steller.2017.pdf (18.11.2020). Na temat Strategii cyberbezpieczeństwa Niemiec szerzej: K. Sacewicz, *Niemiecka strategia ochrony cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 4, s. 129–130, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-16bb4b57–485e-4981-bcf0––04289b50c143/c/przeglad_7.130–136.pdf (18.11.2020); I. Oleksiewicz, *Polityka bezpieczeństwa cybernetycznego RFN*, „Studia Bobolanum" 28, 2017, nr 3, s. 41, http://bobolanum.pl/images/studia-bobolanum/2017/03/StBob_2017_3_Oleksiewicz.pdf (18.11.2020); C. Guitton, op.cit., s. 23.

[42] Strategia cyberbepieczństwa Niemiec 2016, s. 9.

[43] Ibidem, s. 4–5.

*srat*) w celu nawiązania współpracy pomiędzy rządem federalnym oraz sektorem publicznym i prywatnym. W skład Rady wchodzą: Kancelaria Federalna i sekretarz stanu z ministerstw federalnych (spraw zagranicznych, spraw wewnętrznych, obrony, gospodarki i technologii, sprawiedliwości, finansów, edukacji i badań) oraz przedstawiciele krajów związkowych. W określonych przypadkach zostaną włączone dodatkowe ministerstwa. Przedstawiciele biznesu zostaną włączeni jako członkowie stowarzyszeni, a w razie potrzeby zaangażowani będą także przedstawiciele środowisk akademickich[44]. Działaniami Rady kieruje pełnomocnik rządu ds. teleinformacyjnych[45].

W strategii dokonano rozróżnienia i podziału zadań pomiędzy organy i urzędy federalne. W Federalnym Urzędzie ds. Bezpieczeństwa Informacji (BSI) powoływane są mobilne zespoły reagowania na incydenty (MIRT), które analizują i usuwają incydenty cybernetyczne w instytucjach. Na żądanie MIRT, BSI będzie w stanie zapewnić wsparcie organom konstytucyjnym, władzom federalnym i operatorom infrastruktury krytycznej oraz podobnie ważnych obiektów lokalnych w celu szybkiego przywrócenia sprawności technicznej danego obiektu[46]. Specyficzna cecha niemieckich rozwiązań jest powierzenie BSI kontroli nad sposobem wdrożenia szczegółowych procedur ochronnych w tych działach infrastruktury krytycznej, które decydują o sposobie funkcjonowania społeczeństwa. Za takie uznano systemy: bankowy, energetyczny, wodociągowy (dostaw wody pitnej), wyżywienia, telekomunikacyjny oraz technologii informatycznych. Z racji tego, że zadania odnoszą się do operatorów sieci teleinformatycznych i instytucji je wykorzystujących w zakresie ochrony danych, form zabezpieczenia w przypadku ich digitalizacji oraz prób włamania do osobistych kont w systemie, zdecydowano o takim rozdziale kompetencji instytucji federalnych. BSI jest uprawniona do wdrażania procedur dotyczących sposobu wykorzystywania przez elementy infrastruktury krytycznej systemów informatycznych, odnoszących się zarówno do sposobu ich wykorzystywania, jak i wprowadzanych zmian i inwestycji dokonywanych w celu zabezpieczenia ich funkcjonalności[47].

---

[44] Ibidem, s. 5–6.

[45] P. Mickiewicz, op.cit., s. 74.

[46] Strategia cyberbepieczństwa Niemiec 2016, s. 29.

[47] P. Mickiewicz, op.cit., s. 76.

Ataki cybernetyczne mogą również wymagać działania lokalnych federalnych agencji bezpieczeństwa. W tym celu Federalne Biuro Policji Kryminalnej (BKA) powołuje wyspecjalizowaną jednostkę dochodzeniową (Quick Reaction Force (QRF)), która w porozumieniu z właściwą prokuraturą lub prokuraturą federalną przeprowadza pierwsze postępowanie karne dla organów ścigania[48].

## V.

Przedstawione powyżej instytucje właściwe w zakresie cyberbepiczeństwa wskazują na różnorodność przyjętych systemowych rozwiązań. Państwa tworząc narodowe strategie w zakresie cyberbezpieczeństwa dostosowują zakres działania i ich funkcje do systemu politycznego, bieżącej działalności politycznej, ale też roli jaką odgrywają i chcą odgrywać w polityce międzynarodowej. Sama strategia jest dokumentem politycznym, planem działania określonego rządu, a precyzując, wizji jego własnej polityki w zakresie cyberbezpieczeństwa. Działalność organów władzy publicznej, ich kreacja i wyposażenie w kompetencje jest już realną formą realizacji tej polityki. Założeniem każdego rządu jest stworzenie takiego systemu, który w sposób kompletny będzie monitorował i zapobiegał atakom w cyberprzestrzeni. Najważniejszym priorytetem jaki stawiała sobie administracja Trumpa w polityce wewnętrznej było wyposażanie organów federalnych w takie kompetencje, które umożliwiałyby systemową współpracę rządu federalnego i lokalnego z przedsiębiorcami w celu wypracowania wspólnej, spójnej ochrony amerykańskiej cyberprzestrzeni. Administracja tworząc cały system cyberbezpieczństwa chce być bardziej ofensywna i wyprzedzać ataki. Francja, od 2008 r. systematycznie buduje własny system ochrony cyberprzestrzeni, konsekwentnie tworzy system prewencji i reakcji, najpierw na szczeblu rządowym, po to aby następnie wdrożyć go w administracji terenowej. Niewątpliwym, przemyślanym sukcesem było stworzenie Krajowej Agencja Bezpieczeństwa Systemów Informatycznych (ANSSI) i wyposażenie jej w szerokie kompetencje w zakresie ochrony cyberprzestrzeni. Widać znaczącą rolę ANSSI w budowaniu francuskiego systemu ochrony cyberprzestrzeni. Dokonując analizy strategii opra-

[48] Strategia cyberbepieczństwa Niemiec 2016, s. 29.

cowanych przez francuski rząd dostrzega się świadomość cyberzagrożeń. Określone cele w przygotowanych strategiach tylko to potwierdzają. Natomiast niemiecka polityka ochrony cyberprzestrzeni i obrony cybernetycznej jest spójna i konsekwentnie wskazuje na najważniejsze elementy, takie jak ochrona infrastruktury krytycznej i infrastruktury sieci. Włączenie sektora prywatnego, częściowo w ramach współpracy, częściowo w ramach koordynacji z instytucjami państwowymi, rządowymi skutecznie wpływa na budowę struktury organizacyjnej organów koordynujących i monitorujących. Wskazane organy pełnią różną, określoną przepisami prawa rolę. Wszystkie, w zakresie swoich działań mają spełniać funkcję monitorującą, a większość z nich także koordynującą te działania systemowe. W każdej ze wskazanych strategii, organy współpracują z agencjami rządowymi, operatorami i innymi instytucjami publicznymi i prywatnymi. Przyjęte rozwiązania wskazują na ich narodowy charakter, mogą one stanowić wzór do implementacji uniwersalnych założeń systemowych.

**Literatura**

Bożyk S., *Republika Federalna Niemiec*, [w:] *Ustroje konstytucyjne wybranych państw europejs*kich, red. S. Bożyk, Warszawa 2020.

D'Elia D., *Industrial policy: the holy grail of French cybersecurity strategy*, „Journal of Cyber Policy" 2018, vol. 3.

Guitton C., *Cyber insecurity as a national threat: overreaction from Germany, France and the UK?*, „European Security" 2013, nr 22(1).

Jackiewicz A., *Republika Francuska*, [w:] *Ustroje konstytucyjne wybranych państw europejs*kich, red. S. Bożyk, Warszawa 2020.

Jagielski M., *Prezydent USA jako szef administracji ogólnej,* Kraków 2000.

Kempf O., *La cyberstratégie française,* „Recherches internationals", n° 100, juillet-septembre 2014, https://www.recherches-internationales.fr/RI100/RI100OlivierKempf.pdf.

Laidler P., *Konstytucja Stanów Zjednoczonych. Przewodnik*, Kraków 2007.

Lemos R., *Bush unvelis final cybersecurity plan*, https://www.cnet.com/news/bush-unveils-final-cybersecurity-plan.

Mickiewicz P., *System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, vol. 11, nr 1.

Mickiewicz P., *System bezpieczeństwa narodowego, w rozwiązaniach systemowych wybranych państw*, Warszawa 2018.

Oleksiewicz I., *Polityka bezpieczeństwa cybernetycznego RFN*, „Studia Bobolanum" 2017, nr 3 (28), http://bobolanum.pl/images/studia-bobolanum/2017/03/StBob_2017_3_Oleksiewicz.pdf.

Podolak M., Żmigrodzki M., *System polityczny i jego kwalifikacje*, [w:] *Współczesne systemy polityczne*, red. M. Żmigrodzki, B. Dziemidok-Olszewska, Warszawa 2013.

Sacewicz K., *Niemiecka strategia ochrony cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 4.

Sarnecki P., *Ustroje konstytucyjne państw współczesnych*, Warszawa 2013.

*Ustroje państw współczesnych*, t. I, red. W. Skrzydło, Lublin 1992.

Weber V., *Linking cyber strategy with the grand strategy: the case of the United States,* „Journal Cyber Policy" 2018, vol. 3, iss. 2.

Worona J., *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Warszawa 2020.

Zajko M., *Canada's cyber security the changing threat landscape*, „Critical Studies on Security" 2015, nr 3(2).

Żebrowski W., *Współczesne systemy polityczne. Zarys teorii i praktyka w wybranych państwach świata*, Olsztyn 2007.