DOI: 10.35757/SM.2018.71.2.09

MAREK SZCZYGIEŁ
Ministerstwo Spraw Zagranicznych

Polityka cyberbezpieczeństwa Unii Europejskiej – początek drogi do strategicznej autonomii

Cybersecurity Policy of the European Union: Towards Strategic Autonomy

Although cybersecurity as an unified domain is still a recent field of common policy for the EU, it is widely perceived as an area of growing importance for the global position and security of the Union. This development of EU's cybersecurity policy is taking place in the context of the broader efforts, namely Europe's ambition to increase its strategic autonomy. For the EU the main challenge remains how to achieve the coherent and holistic approach to cybersecurity, encompassing it's all dimensions – network and information security, cybercrime and cyber defence. New initiatives undertaken recently by Brussels try to address this problem. This article's aim is to contribute to the better understanding of the potential of the EU's cybersecurity policy to frame the future of European security and defence. The article describes the process of development of the cybersecurity policy of the EU in the XXI century. It provides a brief overview of the instruments and institutions of this policy. Then, the article discusses the EU's potential in cybersecurity field. The final part deals with the three dimensions of EU's strategic autonomy – political, operational and industrial and how they relate to cybersecurity.

Keywords: cybersecurity, strategic autonomy, European Union, cyber defence, cybercrime, network and information security, resilience, cyberpower, strategy, Common Security and Defence Policy, deterrence, cyberspace.

Upowszechnienie internetu to kwestia zaledwie 25 ostatnich lat. Na początku 2018 r. liczba jego użytkowników przekroczyła 50% globalnej populacji. Nic zatem dziwnego, że cyberprzestrzeń staje się coraz bardziej ważną sferą aktywności, współpracy, ale też rywalizacji, w której uczestniczą zarówno państwa, jak i aktorzy niepaństwowi. W czasie ostatniej dekady zyskaliśmy większą świadomość negatywnych aspektów upowszechnienia internetu. Szeroko rozumiana cyberprzestrzeń jest nie tylko miejscem, w którym ludzie

pracują, zdobywają wiedzę, komunikują się ze sobą, czy też poszukują rozrywki, ale również stała się miejscem, w którym ludzie są narażeni na różne zagrożenia[1]. Te o charakterze cybernetycznym dawno już wykraczają poza poziom odosobnionych incydentów zakłócających funkcjonowanie poszczególnych komputerów, sieci lub systemów teleinformatycznych. Skala przeprowadzanych w dzisiejszych czasach ataków cybernetycznych stanowi wręcz wyzwanie dla bezpieczeństwa narodowego państw i ich wewnętrznej stabilności. Rozwój technologii teleinformatycznych oraz internetu spowodował, że wprowadzono w obszarze bezpieczeństwa międzynarodowego zupełnie nowe pojęcia, takie jak „cyberkryzys" i „cyberkonflikt"[2]. Jednocześnie pojawiły się narzędzia służące do prowadzenia w cyberprzestrzeni, jako tzw. piątej domenie, operacji wojskowych[3] o charakterze zarówno defensywnym, jak i ofensywnym. Same zaś cyberataki stanowią dziś często integralną część kryzysów i konfliktów polityczno-militarnych, realizowanych zwłaszcza w ramach scenariusza hybrydowego.

Potencjał i zdolności cybernetyczne (tzw. *cyberpower*[4]) stają się istotnym składnikiem potęgi i znaczenia państw w relacjach międzynarodowych. Jednocześnie podatność lub odporność na zagrożenie atakami cybernetycznymi w coraz większej mierze przesądza o ogólnej percepcji bezpieczeństwa. Przyczyniają się do tego bardzo nagłaśniane przykłady kolejnych spektakularnych ataków cybernetycznych[5], których skutki mają poważny wymiar gospodarczy, zakłócają funkcjonowanie struktur państwowych, a także bezpośrednio wpływają na życie obywateli i ich poczucie bezpieczeństwa[6]. Według ubiegłorocznego badania Pew Research Center[7] ataki cybernetyczne ze strony

1 R. Tadeusiewicz, *Zagrożenia w cyberprzestrzeni*, „Nauka" 2010, nr 4, s. 32.

2 M. Schmitt (red.), *The Law of Armed Conflict Generally. In Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge 2017, s. 375−400.

3 Oprócz lądu, mórz, powietrza i kosmosu.

4 Więcej nt. pojęcia „cyberpower" zob.: J.S. Nye, *Cyber Power*, Harvard Kennedy School Belfer Center for Science and International Affairs, Cambridge 2010; D.J. Betz, T. Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, Routledge, Abingdon 2011; A. Klimburg, *Mobilising Cyber Power*, „Survival" 2011, vol. 53, nr 1, s. 41−60.

5 Atak cybernetyczny WannaCry z czerwca 2017 r. dotknął swoim zasięgiem 230 tys. komputerów w ponad 100 państwach.

6 Special Eurobarometer 464a Report, *Europeans' Attitudes Towards Cyber Security*, September 2017, s. 5−7, https://ec.europa.eu/digital-single-market/en/news/special-eurobarometer--europeans-attitudes-towards-cyber-security (dostęp: 21.03.2018).

7 *Globally, People Point to ISIS and Climate Change as Leading Security Threats*, Pew Research Center, August, 2017, www.pewglobal.org/2017/08/01/globally-people-point-to-isis-and-climate-change-as-leading-security-threats (dostęp: 21.03.2018).

innych państw są wymieniane na trzecim miejscu wśród globalnych zagrożeń. Dla 56% mieszkańców Unii Europejskiej zagrożenia cybernetyczne stanowią „bardzo ważne" wyzwanie dla bezpieczeństwa. Ze względu na jeden z najwyższych na świecie poziomów upowszechnienia internetu i usług cyfrowych[8] państwa UE są szczególnie zagrożone atakami cybernetycznymi, a co za tym idzie, będą ponosiły tego również rozliczne konsekwencje.

Dla Unii Europejskiej szeroko rozumiana polityka cyberbezpieczeństwa dosyć późno nabrała całościowego wymiaru strategicznego. Stało się to w zasadzie dopiero wraz z przyjęciem dokumentu *Strategia cyberbezpieczeństwa UE* w 2013 r. Od tego momentu rozpoczął się jednak intensywny rozwój polityki UE w odniesieniu do cyberprzestrzeni we wszystkich jej wymiarach: gospodarki cyfrowej, bezpieczeństwa sieci i systemów informatycznych, zwalczania cyberprzestępczości, jak też Wspólnej Polityki Zagranicznej i Bezpieczeństwa oraz cyberobrony. Dotyczy to także współpracy UE z innymi podmiotami bezpieczeństwa, jak NATO. Ewolucja podejścia do tej problematyki widoczna jest zwłaszcza w *Globalnej strategii na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej*, w której cyberbezpieczeństwo wymieniane jest wśród integralnych elementów bezpieczeństwa Unii.

Uznając, że technologia informacyjna stała się podstawą funkcjonowania i dobrobytu europejskich społeczeństw, UE uczyniła cyberbezpieczeństwo jednym ze swoich głównych priorytetów w dziedzinie bezpieczeństwa. Jednocześnie ostatnie wydarzenia wokół i wewnątrz UE, takie jak agresja Rosji na Ukrainę, Brexit i niepewność dotycząca przyszłości relacji transatlantyckich po wyborze Donalda Trumpa na prezydenta USA, spowodowały intensyfikację debaty nad wzmocnieniem niezależności UE w sferze bezpieczeństwa i obrony, jej odporności (*resilience*) oraz nad zwiększeniem zakresu jej strategicznej autonomii. Nie brak głosów, że właśnie polityka cyberbezpieczeństwa, jako dziedzina dość nowa i nieobciążona politycznymi zaszłościami, może stać się zalążkiem i swoistym poligonem strategicznej autonomii UE[9]. W artykule autor będzie się starał ocenić strategiczny potencjał problematyki cyberbezpieczeństwa w ramach Unii i szanse na materializację takiego scenariusza.

Jakkolwiek nie ma zgody w literaturze przedmiotu w kwestii powszechnie akceptowalnej definicji pojęcia „cyberbezpieczeństwo", to na potrzeby tego

8 Ponad 85% mieszkańców UE korzysta na co dzień z internetu. Pod tym względem UE ustępuje nieznacznie jedynie regionowi Ameryki Północnej (USA i Kanada), www.internetworldstats.com/stats2.htm (dostęp: 21.03.2018).

9 J. Katainen, J. Limnell, *Cybersecurity and Defence for the Future of Europe*, „EUobserver", 10 IV 2018, https://euobserver.com/opinion/141556 (dostęp: 8.06.2018).

tekstu przyjęto ogólną definicję terminu sformułowaną w *Strategii cyberbezpieczeństwa UE*: „Cyberbezpieczeństwo ogólnie odnosi się do zabezpieczeń i działań, które mogą być wykorzystywane do ochrony domeny cybernetycznej, zarówno cywilnej, jak i wojskowej, przed tymi zagrożeniami, które dotyczą jej współzależnych sieci i infrastruktury informatycznej oraz które mogą te sieci i tę infrastrukturę uszkodzić. Cyberbezpieczeństwo polega na działaniach mających na celu zachowanie dostępności i integralności sieci i infrastruktury oraz zachowanie poufności zawartych w nich informacji”[10]. Ze względu na zakres tematyczny artykułu uwzględnione zostały tu przede wszystkim polityczno-strategiczne aspekty tego zagadnienia.

Proces kształtowania polityki UE wobec cyberprzestrzeni

Bruksela nie od razu dostrzegła przełomowe znaczenie pojawienia się globalnej sieci na początku lat 90. XX w. W ramach EWG, a potem UE początkowo traktowano internet jako nowinkę technologiczną o znaczeniu raczej gospodarczym niż politycznym. Wprawdzie tzw. raport Bangemanna z 1994 r. wskazywał na znaczenie technologii teleinformatycznych dla rozwoju wspólnego rynku i jego konkurencyjności, jednak nie od razu poszły za nim konkretne działania[11]. Tymczasem w krótkim czasie burzliwy rozwój i upowszechnienie się internetu sprawiły, że Europa zaczęła pozostawać w tyle pod względem wykorzystania potencjału zachodzącej rewolucji informatycznej. Internet, mający swoje pierwotne korzenie w programach wojskowych USA lat 50. XX w., wciąż pozostawał organicznie powiązany z administracją amerykańską. W latach 90. XX w. UE popierała pomysł, aby główną funkcję przyznawania nazw domen pełniła międzynarodowa struktura wielostronna pod nazwą International Ad-Hoc Committee (IAHC). W interesie Europejczyków leżało, aby IAHC miał siedzibę w Szwajcarii, co, wraz z sąsiedztwem Międzynarodowej Unii Telekomunikacyjnej (ITU), zapewniłoby mu odpowiedni stopień umiędzynarodowienia[12]. Ostatecznie administracja USA przeforsowała swoją wizję

10 *Strategia cyberbezpieczeństwa Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*, Bruksela, 2013, www.europarl.europa.eu/meetdocs/2009_2014/documents/join/com_join(2013)0001_/com_join(2013)0001_pl.pdf (dostęp: 8.06.2018).

11 *Report on Europe and the Global Information Society: Recommendations of the High-level Group on the Information Society to the Corfu European Council*, Bulletin of the European Union, Supplement No. 2/94. [followup to the White Paper] (commonly called the Bangemann Report), http://aei.pitt.edu/1199 (dostęp: 23.03.2018).

12 K.E. Jørgensen, K.V. Laatikainen (red.), *Routledge Handbook on the European Union and International Institutions: Performance, Policy, Power*, Routledge, Abingdon 2013, s. 349.

zarządzania internetem zawartą w tzw. *green paper* i *white paper*[13], której realizacją stało się powołanie we wrześniu 1998 r. Internet Corporation for Assigned Names and Numbers (ICANN). Struktura ta funkcjonuje jako organizacja *non-profit* na gruncie prawa amerykańskiego, ale zachowuje ścisłe powiązania z Departamentem Handlu USA. Chociaż kształt ICANN nie w pełni odpowiadał oczekiwaniom Brukseli, to od początku funkcjonowania korporacji UE troszczyła się o odpowiednie zabezpieczenie swoich interesów, m.in. przez wejście w skład Governmental Advisory Committee[14].

W zasadzie dopiero podsumowania szczytu UE z Lizbony z 2000 r. przyniosły zmianę pierwotnego podejścia i pełne uznanie potencjału gospodarki cyfrowej opartej na wiedzy, w celu osiągnięcia większej konkurencyjności oraz tworzenia nowych miejsc pracy. Przywódcy UE uznali wówczas, że „wykorzystanie całego potencjału Europy w dziedzinie informatyki zależy od stworzenia warunków dla elektronicznego handlu oraz internetu, tak by Unia mogła dogonić swoich konkurentów"[15]. Pod hasłem „Społeczeństwo informacyjne – oferta dla wszystkich" w Strategii Lizbońskiej nakreślono kierunki rozwoju działań w dziedzinie cyfrowej zmierzających do powszechnego rozwoju społeczeństwa informacyjnego w Europie i jednocześnie osiągnięcia takiego poziomu rozwoju europejskiej gospodarki innowacyjnej, aby mogła ona być konkurencyjna z innymi gospodarkami świata – amerykańską i japońską[16].

Nadal jednak w pierwszej dekadzie XXI w. podejściu UE do domeny cybernetycznej brakowało ujęcia całościowego. Dominowała natomiast podzielona perspektywa wynikająca z trzech istniejących wówczas filarów traktatowych. Z perspektywy funkcjonowania wspólnego rynku i obszaru wspólnotowego (I filar) uznano, że dobrobyt Europy jest coraz bardziej zależny od sprawnie funkcjonujących systemów teleinformatycznych, a rozwój

13 US Department of Commerce: Improvement of Technical Management of Internet Names and Addresses; Proposed Rule, www.ntia.doc.gov/federal-register-notice/1998/improvement-technical-management-internet-names-and-addresses-proposed- (dostęp: 26.03.2018).

14 Communication from the Commission to the Council and the European Parliament – *The organisation and management of the Internet – International and European policy issues 1998−2000*, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1523121853037&uri=CELEX:52000DC0202.

15 Spotkanie Rady Europejskiej w Lizbonie 23−24 marca 2000 r. – Wnioski Prezydencji http://oide.sejm.gov.pl/oide/images/files/dokumenty/konkluzje/lizbona200003.pdf (dostęp: 02.04.2018).

16 A. Demczuk, *Od raportu Bangemanna do Strategii Europa 2020. Rozwój społeczeństwa informacyjnego w polityce Unii Europejskiej – bilans 15 lat*, „Annales UMCS" 2016, vol. 23, nr 2, s. 25−44.

gospodarczy nie będzie możliwy bez zapewnienia otwartej i bezpiecznej cyberprzestrzeni. I tak, w ramach działań wspólnotowych, poczyniono postępy w budowie podwalin wspólnego rynku cyfrowego, czego odzwierciedleniem był najpierw *Plan działań eEuropa 2002*, a następnie Komunikat Komisji Europejskiej *Bezpieczeństwo sieci i informacji: Propozycje na rzecz europejskiego podejścia* oraz Komunikat KE z 2005 r. i 2010 – *Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia*.

Drugą sferą działań UE, gdzie sprawy cyberprzestrzeni znalazły praktyczne odzwierciedlenie, był obszar Wymiaru Sprawiedliwości i Spraw Wewnętrznych (WSiSW – tzw. III filar). Impulsem było wypracowanie i podpisanie Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie 23 listopada 2001 r., do której przystąpiły wszystkie państwa członkowskie UE[17]. Z początku XXI w. pochodzą też pierwsze regulacje unijne dotyczące ochrony prywatności (*Dyrektywa o prywatności i łączności elektronicznej – e-Privacy*)[18] oraz zwalczania oszustw finansowych online[19]. Istotnym etapem w rozwoju podejścia UE do cyberprzestrzeni w obszarze WSiSW było przyjęcie Decyzji Ramowej Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, która wprowadziła wiele definicji oraz katalog przestępstw przeciwko bezpieczeństwu systemów informatycznych[20]. Z kolei w przyjętej w 2010 r. *Strategii bezpieczeństwa wewnętrznego UE* jako jeden z pięciu celów strategicznych wymieniono: „Podniesienie poziomu ochrony obywateli i przedsiębiorstw w cyberprzestrzeni"[21].

Po zamachach terrorystycznych z 11 września 2001 r. na porządku dziennym w wymiarze globalnym pojawiła się także kwestia cyberterroryzmu i podjęcia

17 Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., Dz. Ustaw 2015, poz. 728, http://dziennikustaw.gov.pl/du/2015/728 (dostęp: 8.06.2018).

18 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32002L0058 (dostęp: 8.06.2018).

19 Decyzja ramowa Rady z dnia 28 maja 2001 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi.

20 Decyzji Ramowej Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, http://eur-lex.europa.eu/legalcontent/PL/TXT/PDF/?uri=CELEX:32005F0222&qid=1523126716983&from=EN (dostęp: 8.06.2018).

21 Komunikat Komisji do Parlamentu Europejskiego i Rady: Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy, KOM(2010) 673, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52010DC0673&from=EN (dostęp: 8.06.2018).

działań obliczonych na zwalczanie tego zagrożenia. Jedną z odpowiedzi było wypracowanie i przyjęcie przez USA 14 lutego 2003 r. *Narodowej Strategii Bezpieczeństwa w Cyberprzestrzeni* (*National Strategy to Secure Cyberspace*). Był to pierwszy na świecie tego typu dokument strategiczny, w którym odniesiono się w sposób całościowy do zagadnienia cyberbezpieczeństwa[22]. W reakcji na te wydarzenia w czerwcu 2004 r. Rada Europejska wezwała do przygotowania ogólnej strategii ochrony infrastruktury krytycznej. Odpowiadając na ten apel, 20 października 2004 r. Komisja Europejska ogłosiła komunikat w sprawie ochrony infrastruktury krytycznej w walce z terroryzmem, zawierający propozycje sposobów usprawnienia europejskich systemów zapobiegania atakom terrorystycznym wymierzonym przeciwko infrastrukturze krytycznej, a także zwiększenia gotowości i zdolności do reagowania na takie ataki.

W Europie świadomość zagrożeń cybernetycznych z trudem wzrastała w obszarze współpracy politycznej czy też Wspólnej Polityki Zagranicznej i Bezpieczeństwa (WPZiB – II filar). W opublikowanej w 2003 r. pierwszej *Strategii bezpieczeństwa UE*[23] próżno szukać odniesień do cyberprzestrzeni. Cyberbezpieczeństwo nie znalazło się wśród najważniejszych zagrożeń dla bezpieczeństwa Unii, za które uznano konflikty regionalne, terroryzm, proliferację broni masowego rażenia, upadające państwa i wybuchające w nich oraz w ich sąsiedztwie konflikty, a także przestępczość zorganizowaną.

Sytuacja ta uległa zmianie pod wpływem ataków cybernetycznych przeciw Estonii w kwietniu i maju 2007 r., których przeprowadzenie powszechnie przypisuje się Rosji. Powszechnie uznaje się, że podczas nich po raz pierwszy masowo wykorzystano internet do ataku na struktury państwowe. Trwająca kilka tygodni fala cyberataków na infrastrukturę informatyczną Estonii była powiązana z estońsko-rosyjskim kryzysem wokół usunięcia sowieckiego pomnika w Tallinie. Dobrze zaplanowane i skoordynowane ataki np. rozproszona odmowa usługi (DDoS – *distributed denial of service*) doprowadziły do unieruchomienia stron internetowych parlamentu, ministerstw obrony i sprawiedliwości, partii politycznych, policji, a nawet szkół publicznych. Cyberataki osiągnęły apogeum 9 maja (rosyjski Dzień Zwycięstwa), gdy ich ofiarą padł również sektor prywatny. Dwa największe banki, Hansapank i SEB Ühispank, musiały zawiesić usługi online i wstrzymać transakcje zagraniczne. Zawiesiła się też

22 Ł. Czebotar, *Strategia Stanów Zjednoczonych wobec problem bezpieczeństwa cyberprzestrzeni*, w: A. Podraza, P. Potakowski, K. Wiak (red.), *Cyberterroryzm zagrożeniem XXI wieku*, Difin, Warszawa 2013, s. 67−69.

23 P. Daniluk, *Kultura strategiczna Unii Europejskiej. Podejście normatywne*, „Rocznik Bezpieczeństwa Międzynarodowego" 2015, vol. 9, nr 2, s. 13−18.

strona największego dziennika „Postimees”[24]. Mimo że władze w Tallinie zwróciły się o pomoc do UE, reakcja instytucji unijnych i państw członkowskich ograniczyła się do wyrazów solidarności i poparcia dla Estonii. W przyjętej wówczas specjalnej rezolucji Parlament Europejski „wezwał Komisję i wszystkie państwa członkowskie do wsparcia analiz «cyberataków» na estońskie strony internetowe oraz do przedstawienia studium na temat tego, jak można rozwiązać kwestię takich ataków i zagrożeń na poziomie UE”[25].

Do zmasowanych ataków na rządowe strony internetowe i serwery doszło także w Gruzji podczas konfliktu gruzińsko-rosyjskiego w sierpniu 2008 r. Działania te stanowiły integralną część rosyjskiej operacji wojskowej przeciwko temu państwu, co nadało terminowi „wojna cybernetyczna” praktycznego wymiaru. Mimo że operacje w cyberprzestrzeni nie doprowadziły do żadnych fizycznych zniszczeń, znacząco osłabiły potencjał obronny Gruzji w kluczowej fazie konfliktu[26]. Wpłynęły również na zdolność rządu w Tbilisi do komunikowania się z własnymi obywatelami oraz opinią publiczną na świecie. Według większości ekspertów za atakami stały zorganizowane grupy hakerów pozostające pod kontrolą rosyjskich służb specjalnych[27].

Wpływ tych wydarzeń widać już w raporcie nt. implementacji *Strategii Bezpieczeństwa UE*, przedstawionym w grudniu 2008 r. Radzie Europejskiej przez ówczesnego Wysokiego Przedstawiciela ds. WPZiB Javiera Solanę, w którym wprost stwierdzono, że kwestie cyberbezpieczeństwa stanowią zagrożenie dla bezpieczeństwa UE[28]. W międzyczasie swoje pierwsze strategie cyberbezpieczeństwa opublikowały: Wielka Brytania (czerwiec 2009 r.), Francja (luty 2011 r.), Niemcy (luty 2011 r.).

Jednak prawdziwym kamieniem milowym było ogłoszenie w lutym 2013 r. *Strategii cyberbezpieczeństwa UE*[29]. Przygotowana wspólnie przez Komisję

24 S. Haataja, *The 2007 Cyberattacks Against Estonia and International Law on the Use of Force: An Informational Approach*, „Law, Innovation and Technology” 2017, s. 159−189.

25 *Rezolucja Parlamentu Europejskiego z dnia 24 maja 2007 r. w sprawie Estonii*, www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2007-0215&language=EN&ring=B6-2007-0220 (dostęp: 12.04.2018).

26 D. Hollis, *Cyberwar Case Study: Georgia 2008*, „Small Wars Journal” 2011, http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf (dostęp: 12.04.2018).

27 M. Lakomy, *Cyberwojna jako rzeczywistość XXI wieku*, „Stosunki Międzynarodowe” 2011, nr 3−4, s. 147.

28 *Report on the Implementation of the European Security Strategy – Providing Security in a Changing World*, www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/104630.pdf (dostęp: 12.04.2018).

29 *Strategia cyberbezpieczeństwa Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*, www.europarl.europa.eu/meetdocs/2009_2014/documents/join/com_join(2013)0001_/com_join(2013)0001_pl.pdf (dostęp: 13.04.2018).

Europejską i Europejską Służbę Działań Zewnętrznych (ESDZ), strategia ta stanowi pierwszy całościowy dokument Unii na ten temat, obejmujący wszystkie aspekty cyberbezpieczeństwa. W dokumencie m.in. stwierdzono, że podstawowe wartości UE mają zastosowanie w świecie cyfrowym w taki sam sposób, jak w świecie rzeczywistym. Unijna wizja przedstawiona w strategii składa się z pięciu priorytetów: 1) osiągnięcie odporności na zagrożenia cybernetyczne; 2) radykalne ograniczenie cyberprzestępczości; 3) opracowanie polityki obronnej i rozbudowa zdolności w dziedzinie bezpieczeństwa cybernetycznego w powiązaniu ze Wspólną Polityką Bezpieczeństwa i Obrony (WPBiO); 4) rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa; 5) ustanowienie spójnej międzynarodowej polityki dotyczącej cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE.

Kolejnym impulsem, który przyczynił się do zwiększenia zaangażowania UE w cyberbezpieczeństwo, była agresja Rosji na Ukrainę w 2014 r. Przeprowadzone wówczas działania hybrydowe, których ważnym elementem były ataki cybernetyczne na infrastrukturę krytyczną (m.in. na system przesyłowy energii elektrycznej), ukazały z całą ostrością skalę zagrożeń. Pod wpływem tych wydarzeń wiele struktur międzynarodowych, w tym NATO i UE, przewartościowały swoje podejście do obszaru cyberbezpieczeństwa i cyberobrony. W przypadku Unii jednym z efektów było wypracowanie dokumentu pod nazwą *Ramy polityki UE w zakresie cyberobrony*, zatwierdzonego przez Radę UE 18 listopada 2014 r. Wskazano w nim pięć obszarów priorytetowych dla cyberobrony w kontekście WPBiO: 1) wspieranie rozwijania związanych z WPBiO zdolności państw członkowskich w zakresie cyberobrony; 2) usprawnienie ochrony sieci łączności związanych z WPBiO wykorzystywanych przez podmioty UE; 3) propagowanie współpracy i synergii cywilno-wojskowych z politykami horyzontalnymi UE, odpowiednimi instytucjami i agencjami UE, a także z sektorem prywatnym; 4) poprawa możliwości szkolenia, kształcenia i ćwiczeń; 5) zacieśnianie współpracy z odpowiednimi partnerami międzynarodowymi[30].

Z kolei w dokumencie *Europejska Agenda Bezpieczeństwa na lata 2015−2020* opublikowanym przez Komisję Europejską w kwietniu 2015 r. cyberprzestępczość została uznana za jedno z trzech, oprócz terroryzmu i zorganizowanej przestępczości, wyzwań dla bezpieczeństwa obywateli UE[31].

30 *Ramy polityki UE w zakresie cyberobrony*, Bruksela, 18 listopada 2014 r., http://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/pl/pdf (dostęp: 8.06.2018).

31 *Komunikat Komisji Europejskiej: Europejska agenda bezpieczeństwa*, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf (dostęp: 8.06.2018).

Wynikiem tej ewolucji jest *Globalna Strategia UE*[32] z 2016 r., w której nadano tej problematyce zasadnicze znaczenie dla bezpieczeństwa Unii (oprócz bezpieczeństwa i obrony, zwalczania terroryzmu, bezpieczeństwa energetycznego i komunikacji strategicznej). Jest to zasadnicza zmiana w stosunku do strategii bezpieczeństwa z 2003 r. W strategii tej podkreślono, że celem Unii jest zachowanie otwartego, wolnego i dostępnego charakteru globalnej sieci. W dokumencie zapowiedziano zacieśnienie współpracy w obszarze cyberbezpieczeństwa z najważniejszymi partnerami, takimi jak USA i NATO, oraz wspieranie odporności na zagrożenia cybernetyczne w regionach sąsiadujących z UE. W strategii określono, że celem UE jest wspieranie globalnego systemu opartego na normach, w tym wypracowanie powszechnie akceptowalnych zasad odpowiedzialnego zachowania państw oraz środków budowy zaufania w cyberprzestrzeni. UE chce wspierać wielostronne zarządzanie cyberprzestrzenią i globalną współpracę związaną z cyberbezpieczeństwem, nie naruszając swobodnego przepływu informacji[33].

W czerwcu 2017 r. Rada UE zatwierdziła *Ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne* (tzw. zestaw narzędzi cyberdyplomacji). Określono w nich zasady, które mają pomóc w zapobieganiu konfliktom, niwelowaniu zagrożeń cyberbezpieczeństwa i utrzymaniu większej stabilności w stosunkach międzynarodowych. Oczekuje się, że będą one sprzyjać współpracy, ułatwią łagodzenie bezpośrednich i długofalowych zagrożeń oraz w dłuższej perspektywie wpłyną na zachowanie potencjalnych agresorów. W przypadku szkodliwych działań cybernetycznych UE ma w pełni wykorzystywać dostępne środki w ramach WPZiB, w tym, w razie potrzeby, środki restrykcyjne i sankcje. Reakcja UE na cyberataki ma być proporcjonalna co do zakresu, skali, czasu trwania, intensywności, złożoności, wyrafinowania i wpływu działalności cybernetycznej. Jednocześnie UE potwierdziła swoje zaangażowanie w rozwiązywanie międzynarodowych sporów w cyberprzestrzeni w sposób pokojowy, w celu promowania bezpieczeństwa i stabilności poprzez współpracę międzynarodową oraz zmniejszenie ryzyka nieporozumień, eskalacji i konfliktów, które mogą wynikać z incydentów cybernetycznych[34].

32 *Globalna strategia na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej – Wspólna wizja, wspólne działanie: Silniejsza Europa*, https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_pl_version.pdf (dostęp: 15.04.2018).

33 J. Maliszewska-Nienartowicz, *Założenia Globalnej strategii na rzecz polityki zagranicznej i bezpieczeństwa UE – przełom czy stagnacja?*, „Sprawy Międzynarodowe" 2017, nr 2, s. 46−62.

34 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf (dostęp: 13.03.2018).

Swoistym podsumowaniem tego etapu kształtowania się polityki UE był opublikowany 13 września 2017 r. *Wspólny Komunikat Komisji i Wysokiego Przedstawiciela Unii do spraw zagranicznych i polityki bezpieczeństwa – Odporność, Odstraszanie, Obrona: Budując silne cyberbezpieczeństwo dla Unii Europejskiej*[35]. W dokumencie tym, będącym częścią szerszego „pakietu cyberbezpieczeństwa", zaktualizowano *Strategię cyberbezpieczeństwa UE* z 2013 r. Komisja stwierdziła w Komunikacie, że UE musi zwiększyć swoją odporność na ataki cybernetyczne, stworzyć skuteczne narzędzia odstraszania i instrumenty prawa karnego pozwalające lepiej chronić obywateli, przedsiębiorstwa i instytucje publiczne w Europie. Zapowiedziała m.in. stworzenie Agencji UE ds. Cyberbezpieczeństwa na bazie istniejącej już Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz ustanowienie i wdrożenie ogólnounijnych ram certyfikacji w obszarze cyberbezpieczeństwa. W komunikacie stwierdzono wprost, że przedstawione w dokumencie podejście będzie „podstawą większej odporności i strategicznej autonomii, wzmocni zdolności w zakresie technologii i umiejętności oraz pomoże w budowie silnego jednolitego rynku".

Rozwój polityki cyberbezpieczeństwa UE w XXI w. odbywał się zasadniczo w sposób reaktywny, mało skoordynowany i bez z góry założonego planu działania. W rezultacie unijny porządek w tej sferze przypomina swoistą mozaikę legislacji, instrumentów politycznych i instytucji, które pojawiały się w odpowiedzi na polityczne zapotrzebowanie wynikające z rosnącej skali zagrożeń cybernetycznych. Tymczasem dla swej skuteczności polityka bezpieczeństwa powinna mieć charakter przekrojowy i horyzontalny. Zdają się ten problem dostrzegać przywódcy unijni, gdyż Rada Europejska w październiku 2017 r. zaleciła przyjąć „wspólne podejście do unijnego cyberbezpieczeństwa".

Instytucje i instrumenty polityki cyberbezpieczeństwa UE

Obszar bezpieczeństwa sieci i systemów teleinformatycznych, wywodzący się z działań służących rozwojowi społeczeństwa informatycznego i rynku cyfrowego, jest regulowany przede wszystkim przez *Dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych*

35 *Wspólny Komunikat Komisji i Wysokiego Przedstawiciela Unii do spraw zagranicznych i polityki bezpieczeństwa – Odporność, Odstraszanie, Obrona: Budując silne cyberbezpieczeństwo dla Unii Europejskiej* http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN (dostęp: 13.03.2018).

na terytorium Unii[36], która została przyjęta 6 lipca 2016 r. (*NIS Directive*). Zobowiązuje ona państwa członkowskie UE do zagwarantowania minimalnego poziomu zdolności krajowych w dziedzinie cyberbezpieczeństwa poprzez ustanowienie organów właściwych oraz jednolitego punktu kontaktowego (*single point of contact*) ds. cyberbezpieczeństwa, powołanie zespołów reagowania na incydenty komputerowe (CSIRT) oraz przyjęcia krajowych strategii w zakresie cyberbezpieczeństwa. W dyrektywie sformułowano obowiązki służące zapewnieniu cyberbezpieczeństwa systemów informacyjnych w sektorach usług mających zasadnicze znaczenie dla utrzymania krytycznej działalności społeczno-gospodarczej, a więc w energetyce, transporcie, bankowości i instytucjach finansowych, sektorach zdrowia, zaopatrzenia w wodę i infrastrukturze cyfrowej. Zgodnie z dyrektywą operatorzy najważniejszych usług są zobowiązani do stosowania odpowiednich zabezpieczeń, szacowania ryzyka oraz do zgłaszania właściwym organom lub CSIRT wszelkich incydentów poważnie zagrażających ich systemom informacyjnym oraz mogących znacząco zakłócić ciągłość działania usług w 2016 r. Państwa członkowskie są zobowiązane do transpozycji Dyrektywy do krajowego porządku prawnego w terminie do 9 maja 2018 r. Do tego obszaru należy zaliczyć także działania służące ochronie infrastruktury krytycznej, w szczególności realizowane w ramach Planu Działań do opublikowanego w 2009 r. przez Komisję Europejską Komunikatu nt. ochrony krytycznej infrastruktury informatycznej[37].

Najważniejszą unijną instytucją w wymienionym obszarze jest ENISA, powołana w 2004 r. Jej mandat został znacząco poszerzony w 2013 r., obecnie zaś trwają prace nad przekształceniem jej w pełnowartościową Agencję UE ds. Cyberbezpieczeństwa. Nowy mandat ENISA służy zapewnieniu stałej, silniejszej i bardziej centralnej roli agencji, w szczególności poprzez wspieranie państw członkowskich we wdrażaniu unijnych przepisów w obszarze cyberbezpieczeństwa, w tym wymienionej już dyrektywy NIS, ale także w zakresie przepisów dotyczących usług zaufania i elektronicznej identyfikacji

36 *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX-%3A32016L1148 (dostęp: 13.03.2018).

37 *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection „Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF (dostęp: 13.03.2018).

oraz w obszarze bezpieczeństwa komunikacji elektronicznej. Istotnym wyznacznikiem roli agencji ENISA jest także realizowanie wsparcia krajów członkowskich i instytucji unijnych w budowaniu zdolności przeciwdziałania, wykrywania, analizowania i reagowania na zagrożenia i incydenty, a także oferowania wsparcia w opracowywaniu strategii cyberbezpieczeństwa.

Co istotne, w przyszłości wzrośnie rola agencji w działaniach związanych ze współpracą operacyjną właściwych instytucji czy ciał w obszarze cyberbezpieczeństwa na poziomie unijnym. Będzie ona koordynować współpracę w ramach mechanizmów takich jak sieć CSIRT oraz organizowanie ćwiczeń na poziomie unijnym. ENISA ma również przygotowywać regularne techniczne raporty sytuacyjne w obszarze cyberbezpieczeństwa na poziomie Unii Europejskiej. Ma ona realizować to zadanie na podstawie źródeł otwartych, własnych analiz oraz raportów państw członkowskich (CSIRT), jednolitych punktów kontaktowych, instytucji unijnych, takich jak Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) czy CERT EU. Agencja ma także zostać przekształcona w ośrodek fachowej wiedzy wspomagający państwa członkowskie i Komisję w sprawie certyfikacji cyberbezpieczeństwa. Warto też wspomnieć o utworzonym w 2012 r. zespole reagowania na incydenty cybernetyczne CERT EU, który realizuje zadania w zakresie cyberbezpieczeństwa na potrzeby instytucji europejskich.

W ramach walki z cyberprzestępczością UE rozwinęła stosunkowo obszerne instrumentarium działań i sprawnie działające instytucje. Wśród aktów prawnych dotyczących cyberprzestępczości należy przede wszystkim zwrócić uwagę na *Dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącą ataków na systemy informatyczne*. Jej celem jest zbliżenie prawa karnego państw członkowskich w dziedzinie ataków na systemy informatyczne przez ustanowienie zasad minimalnych dotyczących definicji przestępstw i odpowiednich kar oraz poprawa współpracy między właściwymi organami w państwach członkowskich, a także właściwymi wyspecjalizowanymi agencjami i organami Unii. Wymaga ona od państw członkowskich wprowadzenia do krajowych systemów prawnych regulacji dotyczących skutecznego działania przeciwko podstawowym typom cyberataków. Ponadto, co ważniejsze, wprowadza wspólną definicję takich ataków. Istotne znaczenia ma także *Dyrektywa 2011/92/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej*. W ramach realizacji tzw. pakietu cyberbezpieczeństwa z września 2017 r. Komisja na początku 2018 r. przedstawiła wnioski mające na celu ułatwienie transgranicznego

dostępu do elektronicznego materiału dowodowego w celu zwiększenia skuteczności prowadzenia dochodzeń i ścigania przestępczości wykorzystującej cyberprzestrzeń. Planuje się także przedstawienie projektu nowej dyrektywy dotyczącej zwalczania fałszerstw i oszustw związanych z bezgotówkowymi środkami płatniczymi. Dodatkowo do października br. Komisja Europejska przedstawi swoje uwagi na temat roli szyfrowania w dochodzeniach karnych.

Najważniejszą instytucją w ramach działań UE w sferze cyberprzestępczości jest EC3, którego zadaniem jest wzmocnienie reakcji organów ścigania na cyberprzestępczość w UE, a tym samym pomoc w ochronie obywateli, przedsiębiorstw i rządów przed przestępczością internetową. Centrum zostało powołane do życia w 2013 r. w ramach Europolu, w 2017 r. liczyło 83 pracowników i dysponowało budżetem w wysokości 11 mln EUR[38]. Przy Europolu działa także Wspólna Grupa Zadaniowa ds. Przeciwdziałania Cyberprzestępczości (J-CAT), która wspiera skoordynowane działania policyjne z wykorzystaniem danych wywiadowczych przeciwko zagrożeniom związanym z cyberprzestępczością i najważniejszym celom poprzez stymulowanie i ułatwianie wspólnego rozpoznawania, hierarchizowania, przygotowywania i wszczynania dochodzeń.

Za najsłabiej rozwinięte należy uznać instrumenty i instytucje w trzecim obszarze polityki cyberbezpieczeństwa UE, odnoszącym się do działań w ramach WPZiB, a zwłaszcza cyberobrony. Przesądza o tym dość późne włączenie tych aspektów do działań UE i ostrożność państw członkowskich w angażowaniu się w projekty dotyczące tego zagadnienia. Odpowiedzialność za zapewnienie cyberbezpieczeństwa spoczywa na państwach członkowskich, które niechętnie dzielą się informacjami o posiadanych zasobach i zdolnościach w tej dziedzinie, również z obawy przed ujawnieniem ewentualnych podatności w narodowych systemach. Dla wielu państw UE głównym forum współdziałania w obszarze cyberobrony pozostaje NATO, które już na szczycie w Walii w 2014 r. uznało cyberprzestrzeń za dziedzinę swojej misji. W świetle rosyjskich działań wobec Ukrainy, NATO i UE uznały, że konieczne jest wzmocnienie współpracy obu organizacji wobec wspólnych zagrożeń w cyberprzestrzeni. W lutym 2016 r. podpisano porozumienie techniczne między NATO's Computer Incident Response Capability a CERT-UE o współpracy operacyjnej i wymianie informacji. Przełomowe znaczenie na szczeblu politycznym miało przyjęcie podczas szczytu Sojuszu

38 www.europarl.europa.eu/cmsdata/137224/2018-02-01%20CONT%20Mission%20to%20Europol_Report.pdf (dostęp: 20.04.2018).

w Warszawie 8 lipca 2016 r. *Wspólnej deklaracji o współpracy NATO–UE*[39]. Wśród siedmiu priorytetowych obszarów współpracy zapowiedziano w deklaracji poszerzenie koordynacji w zakresie cyberbezpieczeństwa i cyberobrony w kontekście zarówno misji i operacji, jak i ćwiczeń, edukacji i treningów. W grudniu 2016 r. NATO i UE zatwierdziły wspólnie przygotowane konkretne propozycje implementacyjne, wśród 42 działań znalazły się cztery dotyczące cyberbezpieczeństwa i cyberobrony[40].

Mimo przewodniej roli NATO w tym obszarze, również Unia, choć w ograniczonej skali, może przyczynić się do podniesienia zdolności państw członkowskich w cyberobronie. Służy temu realizacja wspomnianych *Ram polityki w dziedzinie cyberobrony*. Opublikowane dotychczas cztery półroczne raporty z implementacji tego dokumentu pokazują umiarkowany postęp. Główną rolę w tym zakresie odgrywa Europejska Agencja Obrony, która w przyjętym w 2014 r. *Capability Development Plan* zaliczyła kwestie dotyczące cyberbezpieczeństwa do działań priorytetowych[41]. W ramach tego planu realizowane są dwa rodzaje działań: budowanie wspólnych zdolności do reagowania na zagrożenia cybernetyczne w strukturach wojskowych państw członkowskich i w instytucjach CSDP oraz szkolenia i kursy organizowane przez EDA dla funkcjonariuszy publicznych państw członkowskich. Realizowany jest projekt opracowywania środków odpowiedzi na ataki związane z cyberszpiegostwem, a także projekt dotyczący kryptografii i kodowanie informacji[42]. W maju 2017 r. EDA ogłosiła uruchomienie wspólnego projektu 11 państw w formule *pooling & sharing* dotyczącego rozwoju tzw. poligonów cybernetycznych (*Cyber Ranges Federation Project*)[43].

Duże nadzieje wiąże się z projektem tzw. wzmocnionej współpracy strukturalnej (PESCO). Wśród 17 projektów z pierwszej transzy zaledwie dwa dotyczą

39 *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, www.nato.int/cps/en/natohq/official_texts_133163.htm?selectedLocale=en.

40 *Statement on the Implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, www.nato.int/cps/ua/natohq/official_texts_138829.htm (dostęp: 8.06.2018).

41 *Future Capabilities – Brochure*, www.eda.europa.eu/docs/default-source/eda-publications/futurecapabilities_cdp_brochure (dostęp: 20.04.2018).

42 A. Pieńkoś, *Europejska Agencja Obrony w systemie współpracy przemysłowo-obronnej w Europie*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2017, s. 76.

43 *Cyber Ranges: EDA's First Ever Cyber Defence Pooling & Sharing Project Launched By 11 Member States*, Bruksela, 12 maja 2017, www.eda.europa.eu/info-hub/press-centre/latest-news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states (dostęp: 8.06.2018).

cyberbezpieczeństwa: 1) projekt zacieśnienia współpracy poprzez stworzenie platformy wymiany informacji o zagrożeniach i incydentach cybernetycznych, 2) powołanie szybkich zespołów reagowania cybernetycznego. Oba projekty znajdują się na dość niskim poziomie zaawansowania i mają zasięg ograniczony do kilku państw uczestniczących, w związku z czym trudno uznać je za przełomowe dla budowy zdolności cyberobrony[44]. Wydaje się, że powodem jest niechęć wąskiej grupy państw dysponujących dużymi możliwościami cybernetycznymi do angażowania się w projekty o znikomej z ich punktu widzenia wartości dodanej. Z kolei mniejsze państwa członkowskie muszą oszczędnie dysponować swoimi ograniczonymi zasobami i to przesądza często o ich ostrożności w podejmowaniu nowych zobowiązań. Zachętą w przyszłości dla tej formuły współpracy może być zapewnienie dostępu do środków z budżetu UE, np. w ramach Europejskiego Funduszu Obrony.

Potencjał Unii Europejskiej w dziedzinie cyberbezpieczeństwa

Pisząc o polityce cyberbezpieczeństwa UE, warto zauważyć, że mamy do czynienia z działalnością odnoszącą się do specyficznego środowiska, stworzonego w całości przez człowieka. Próba oceny potencjału Unii Europejskiej w cyberprzestrzeni musi uwzględniać wiele specyficznych cech tej domeny, takich jak: 1) ponadnarodowy i globalny charakter, 2) zasadnicza rola aktorów niepaństwowych, 3) rozproszony sposób zarządzania, 4) asymetryczny charakter zagrożeń cybernetycznych, 5) brak wyraźnej granicy między sferą cywilną i wojskową, 6) wysoki stopień anonimizacji prowadzonych działań oraz 7) dynamicznie zmieniająca się charakterystyka środowiska cybernetycznego.

Jednocześnie sama Unia Europejska stanowi specyficzny byt ponadnarodowy, odmienny w swojej naturze i praktyce działania zarówno od państw narodowych, jak i od typowych organizacji międzynarodowych. Nie do końca przystają więc do UE klasyczne definicje i modele potęgi znane z obszary studiów strategicznych[45]. W przypadku UE, jako aktora polityki międzynarodowej, mamy do czynienia ze zdecydowaną przewagą elementów tzw. łagodnej siły (*soft power*) nad tradycyjnymi, twardymi aspektami siły związanymi z użyciem instrumentów

44 M. Terlikowski, *Pierwsze projekty PESCO: w poszukiwaniu przełomu*, „Biuletyn PISM" 8 V 2018, nr 65.

45 Siła państwa (*state power*) jest postrzegana jako warunek *sine qua non* możliwości urzeczywistnienia interesów państwowych. Składają się na nią trzy główne elementy: polityczny, gospodarczy i militarny. R. Kuźniar, *Polityka i siła. Studia strategiczne – zarys problematyki*, Wydawnictwo Naukowe „Scholar"–Fundacja Studiów Międzynarodowych, Warszawa 2005, s. 177.

przymusu (*hard power*)[46]. Stąd próby ujmowania międzynarodowego potencjału i znaczenia UE w kategoriach „mocarstwa niewojskowego" (*civilian power*) lub też wręcz „mocarstwa pokojowego"[47]. Niewątpliwie, ze względu na wspomnianą specyfikę cyberprzestrzeni, elementy tak opisywanej miękkiej siły Unii mają relatywnie większe znaczenie przy ocenie unijnej polityki cyberbezpieczeństwa.

Ze względu na unikalność środowiska cybernetycznego i jego specyficzny charakter w ostatniej dekadzie w literaturze przedmiotu pojawiło się pojęcie siły cybernetycznej (*cyberpower*), zdefiniowanej przez amerykańskich strategów wojskowości jako „zdolność do użycia cyberprzestrzeni w celu stworzenia przewagi i wywarcia wpływu na zdarzenia w innych przestrzeniach operacyjnych oraz w innych czynnikach składowych siły"[48]. Pojęcie to zostało później spopularyzowane m.in. przez Josepha Nye'a, który określił czynniki *cyberpower* skierowane do wewnątrz i na zewnątrz cyberprzestrzeni. Wyróżnił on trzy oblicza siły w domenie cybernetycznej (przymuszającą, odmawiającą dostępu i grożącą konsekwencjami), w podziale na elementy siły miękkiej i twardej[49]. Inny model do analizy siły cybernetycznej proponuje Alexander Klimburg pod nazwą *Integrated Capability Model*[50]. Ze względu na kompleksowe podejście, nacisk na współpracę i uwzględnienie wszystkich aktorów operujących w cyberprzestrzeni model ten wydaje się bardziej adekwatny do analizy potencjału UE. Jego zastosowanie przez Myriam Dunn Cavelty do zbadania zdolności UE w zakresie cyberbezpieczeństwa przynosi dosyć zniuansowany obraz[51]. Wewnętrznie Unia rozwinęła cały wachlarz zróżnicowanych instrumentów polityki dotyczących cyberprzestrzeni, poczynając od forum dialogu przez platformę współdziałania publiczno-prywatnego aż po specyficzne regulacje prawne. Na zewnątrz natomiast UE promuje

46 O. Barburska, *Argument siły czy siła argumentów? Unia Europejska w stosunkach międzynarodowych jako soft power*, „Rocznik Integracji Europejskiej" 2016, nr 10, s. 335.

47 *Mogherini Calls EU a Peace 'Superpower', in Wake of Trump Win*, EurActiv, 10 XI 2016, www.euractiv.com/section/security/news/mogherini-calls-eu-a-peace-superpower-in-wake-of-trump-win (dostęp: 8.06.2018).

48 D.T. Kuehl, *From Cyberspace to Cyberpower: Defining the Problem*, w: D. Kramer, H. Stuart, L.K. Wentz, *Cyberpower and National Security Policy*, National Defense University, Potomac Books, Inc., Washington 2009, s. 11, http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf (dostęp: 8.06.2018).

49 J.S. Nye, *Cyber Power*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge 2010, s. 3−4, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (dostęp: 8.06.2018).

50 A. Klimburg, *The Whole of Nation in Cyberpower*, „Georgetown Journal of International Affairs" 2011, numer specjalny, *International Engagement on Cyber*, s. 173−179.

51 M.D. Cavelty *Europe's Cyber-Power*, „European Politics and Society" 2018, vol. 19, nr 3, https://doi.org/10.1080/23745118.2018.1430718 (dostęp: 8.06.2018).

współpracę na rzecz wolności i praw podstawowych w cyberprzestrzeni. Generalnie jednak UE nie posiada spójnej wizji projekcji siły cybernetycznej w wymiarze strategicznym[52].

Do oceny potencjału UE konieczna jest jeszcze jedna konstatacja. Nawet najbardziej skuteczny system cyberbezpieczeństwa nie jest w stanie zapobiec wszystkim cyberatakom. Może on jednak efektywnie ograniczyć skutki i zasięg takich działań, pozwalając uniknąć najbardziej katastrofalnego scenariusza. Głównym czynnikiem, który wpływa na skuteczność tak rozumianego cyberbezpieczeństwa, jest odporność (*resilience*). Pojęcie odporności nabrało szczególnego znaczenia w myśleniu o bezpieczeństwie na przestrzeni ostatniej dekady, zwłaszcza w odniesieniu do tzw. nowych lub niekonwencjonalnych zagrożeń dla bezpieczeństwa[53]. Początkowo łączone było głównie z rozważaniami o bezpieczeństwie infrastruktury krytycznej. Znalazło ono jednak szersze zastosowanie zwłaszcza w krajach anglosaskich i nordyckich jako odpowiedź na rosnącą nieprzewidywalność i zmienność środowiska bezpieczeństwa. Warto wspomnieć, że kategoria odporności zajmuje ważne miejsce w narodowych strategiach bezpieczeństwa USA i Wielkiej Brytanii z lat 2010 i 2015. W przypadku UE można mówić o postulacie odporności całego systemu cyberbezpieczeństw[54]. Przejawem tego podejścia jest nadawanie odporności równie istotnego znaczenia, jakie w unijnym podejściu do cyberprzestrzeni mają odstraszanie i obrona, o czym świadczy chociażby tytuł ubiegłorocznego Wspólnego Komunikat Komisji i Wysokiego Przedstawiciela. Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji definiuje odporność w sposób następujący: „zdolność jednostki, systemu, sieci lub usługi do sprostania efektom wydarzenia zakłócającego lub do odzyskania zdolności funkcjonowania na poziomie normalnym lub zbliżonym do normalnego”[55]. Dla UE odporność ma istotny wymiar zewnętrzny, czego przejawem jest dokument Komisji Europejskiej *Strategiczne podejście do kwestii odporności w ramach działań zewnętrznych UE*, opublikowany 7 czerwca 2017 r.[56]

52 *Ibidem*, s. 13.

53 Patrz P. Pawlak w: F. Gaub, N. Popescu (red.), *After the EU Global Strategy – Building Resilience*, EU Institute of Security Studies, 2017, s. 17−21.

54 G. Christou, *Cybersecurity in the European Union*, Palgrave Macmillan, Basingstoke 2016, s. 21−23.

55 S. Górniak (red.), *Enabling and Managing end-to-end Resilience*, ENISA, 2011, s. 9, www.enisa.europa.eu/publications/end-to-end-resilience.

56 *Wspólny komunikat do Parlamentu Europejskiego i Rady. Strategiczne podejście do kwestii odporności w ramach działań zewnętrznych UE*, Bruksela, dnia 7.6.2017, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52017JC0021 (dostęp: 20.04.2018).

Czynniki autonomii strategicznej UE w sferze cyberbezpieczeństwa

Pojawienie się w dyskursie politycznym w Unii Europejskiej koncepcji strategicznej autonomii Europy to z jednej strony wyraz ambicji uzyskania większej podmiotowości na arenie globalnej, z drugiej zaś reakcja na wynik referendum ws. Brexitu i wybór Donalda Trumpa na prezydenta USA. Chociaż idea ta popularność zyskała w ostatnich kilku latach, jej korzenie sięgają okresu bezpośrednio po II wojnie światowej i rodzącej się wówczas idei uniezależnienia się Europy od Stanów Zjednoczonych w zakresie bezpieczeństwa i obrony. Koncepcja niezależności Europy nabrała nowej dynamiki po zakończeniu zimnej wojny, przybrała zrazu postać Europejskiej Tożsamości w Dziedzinie Bezpieczeństwa i Obrony, aby wreszcie ostatecznie otrzymać rangę założenia i myśli przewodniej opublikowanej w 2016 r. *Globalnej Strategii Unii Europejskiej*, w której stwierdzono wprost: „Przedmiotowa strategia jest wyrazem ambicji strategicznej autonomii Unii Europejskiej”[57].

Trzy wymiary autonomii strategicznej	Autonomia polityczna	Zdolność do podejmowania decyzji w zakresie polityki bezpieczeństwa i działania na ich podstawie
	Autonomia operacyjna	Zdolność oparta na koniecznych ramach instytucjonalnych i wymaganych zdolnościach do niezależnego planowania i realizacji operacji cywilnych i/lub wojskowych
	Autonomia przemysłowa	Zdolność do rozwoju i budowy zasobów wymaganych do osiągnięcia autonomii operacyjnej.

Źródło: R. Kempin, B. Kunz, *France, Germany, and the Quest for European Strategic Autonomy*, Notes de L'Ifri, December 2017, s. 10.

Autonomia polityczna. Zasadniczym problemem w rozważaniach na temat autonomii strategicznej jest kwestia wspólnej kultury strategicznej Unii Europejskiej. Jej powstanie to długi proces obejmujący zarówno wypracowanie strategii, jak i stosowanie jej w praktyce. W przypadku UE mamy dopiero dwa dokumenty o charakterze strategii bezpieczeństwa z 2003 i 2016 r. oraz wiele strategii sektorowych, z których niestety nie wszystkie zasługują na to miano. Zwraca na to uwagę Robert Kupiecki, który odnosząc się

57 *Globalna strategia na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej – Wspólna wizja, wspólne działanie...*, s. 3.

do kwestii strategii bezpieczeństwa podmiotów zbiorowych, podkreśla, że wspólna kultura strategiczna powstaje w wyniku mozolnego i raczej powolnego procesu[58]. O wypracowanie takiej właśnie wspólnej kultury strategicznej Europy zaapelował prezydent Francji Emmanuel Macron w przemówieniu programowym *Inicjatywa dla Europy* wygłoszonym 26 września 2017 r. na Sorbonie [59].

W gronie państw członkowskich widoczne są podziały między zwolennikami rozwoju tak pojmowanej autonomii strategicznej UE, a tymi, którzy obawiają się osłabienia więzi transatlantyckich i podważenia kluczowej roli NATO jako fundamentu bezpieczeństwa Europy. Zapewne wiele będzie zależeć od współpracy na linii Berlin–Paryż i zdolności tego tandemu do wypracowania i skutecznej realizacji wizji dalszego rozwoju WPBiO.

Autonomia operacyjna. Do osiągnięcia autonomii operacyjnej konieczne jest posiadanie zarówno zdolności, jak i odpowiedniego poziomu wydatków na ich finansowanie. Zgodnie z „pakietem cyberbezpieczeństwa" zaproponowanym we wrześniu 2017 r. przez Komisję Europejską, ENISA zostanie przekształcona w silniejszą Agencję UE ds. Bezpieczeństwa Cybernetycznego, dysponującą stałym mandatem, większymi środkami operacyjnymi i stabilną bazą na przyszłość. Co istotne, ENISA będzie posiadała pewne, choć ograniczone, zdolności operacyjne. Agencja ma m.in. koordynować współpracę w ramach sieci CSIRT, wzrastają też jej kompetencje w ramach dokonywania np. analiz *ex post* (na wniosek) w związku z otrzymywanymi zgłoszeniami zajścia poważnych incydentów zgodnie z definicją dyrektywy NIS, jak również udziału w zakresie wspólnego reagowania na transgraniczne incydenty dużej skali czy sytuacje kryzysowe w cyberprzestrzeni. Budżet tej agencji UE ma w ciągu 4 lat (2018−2021) wzrosnąć z obecnych 11 mln EUR do 23 mln EUR, a jej struktura personalna z 84 do 125 osób[60]. Należy zauważyć, że w świetle licznych nowych zadań, jakie planowane regulacje nakładają na agencję, taki wzrost jej budżetu wydaje się mocno nieadekwatny.

Trudno o zbiorcze dane dotyczące wydatków na cyberbezpieczeństwo w skali UE. Można mówić o wydatkach z budżetu UE na programy badawcze,

58 R. Kupiecki, *Unia Europejska i problemy strategii bezpieczeństwa podmiotów zbiorowych*, „Sprawy Międzynarodowe" 2014, nr 4, s. 71.

59 Wystąpienie Emmanuela Macrona *Inicjatywa dla Europy*, www.diplomatie.gouv.fr/en/french-foreign-policy/european-union/events/article/president-macron-s-initiative-for-europe-a-sovereign-united-democratic-europe (dostęp: 8.06.2018).

60 Maria Del Mar Negreiro Achiaga, *Enisa and a new cybersecurity act*, Briefing, European Parliamentary Research Service, 2018, www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf (dostęp: 8.06.2018).

rozwój zdolności i kompetencji w tym obszarze, zwłaszcza że są one dosyć rozproszone i często „ukryte" w ramach większych programów i instrumentów sektorowych. Z jednej strony mamy więc dość skromne budżety instytucji unijnych zajmujących się cyberbezpieczeństwem, takich jak ENISA i EC3, z drugiej zaś mało skoordynowane wydatki ponoszone m.in. w ramach rozwoju jednolitego ryku cyfrowego,

Również nie wszystkie państwa specyfikują swoje wydatki w obszarze cyberbezpieczeństwa. Na przykład niemiecki Federalny Urząd ds. Bezpieczeństwa Technologii Informatycznych (Bundesamt für Sicherheit in der Informationstechnik) dysponował w 2017 r. budżetem w wysokości 109 mln EUR i 841 pracownikami. Z kolei w najnowszej brytyjskiej strategii cyberbezpieczeństwa z 2015 r. zapowiedziano wydatki na poziomie 1,9 mld GBP na przestrzeni lat 2016−2021[61]. Francuska minister obrony Florence Parly zapowiedziała w styczniu 2018 r. przeznaczenie kwoty 1,6 mld EUR na cyberobronę w perspektywie najbliższych sześciu lat[62]. Rząd holenderski planuje zwiększenie wydatków na cyberbezpieczeństwo do poziomu 95 mln EUR rocznie[63]. Z kolei rząd Danii zamierza wydatkować 1,4 mld DKK (188 mln EUR) na inwestycje dotyczące cyberbezpieczeństwa i cyberobrony w latach 2018−2022[64].

Problemem pozostaje brak odpowiednio wykwalifikowanych specjalistów. Według Komisji Europejskiej sięga on 350 tysięcy osób. Jednym z proponowanych rozwiązań ma być utworzenie Europejskiego Centrum Badań Naukowych i Kompetencji w dziedzinie bezpieczeństwa cybernetycznego (projekt pilotażowy zostanie zrealizowany w 2018 r.). Współpracując z państwami członkowskimi, Centrum pomoże w opracowywaniu i wdrażaniu narzędzi i technologii koniecznych, by sprostać stale zmieniającym się zagrożeniom i zagwarantuje, że nasza obrona będzie tak nowoczesna, jak broń, którą posługują się cyberprzestępcy. Centrum będzie uzupełniać działania

61 *National Cyber Security Strategy 2016 to 2021*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (dostęp: 8.06.2018).

62 *Discours de Florence Parly: Forum international de la Cybersécurité*, www.defense.gouv.fr/salle-de-presse/tout-discours/discours-de-florence-parly-forum-international-de-la-cybersecurite (dostęp: 8.06.2018).

63 *Professor sounds alarm over Dutch cyber security brain drain*, DutchNews.nl, 23 IV 2018, www.dutchnews.nl/news/2018/04/professor-sounds-alarm-over-dutch-cyber-security-brain-drain (dostęp: 8.06.2018).

64 P. Szymański, *Pozory i konkrety. Polityka bezpieczeństwa i siły zbrojne Danii*, Komentarze OSW, 23 IV 2018.

na rzecz budowy potencjału na poziomie unijnym i krajowym[65]. Z kolei, aby rozwiązać problem niedoboru wykwalifikowanej kadry, w 2018 r. UE stworzy platformę szkoleń i edukacji w zakresie cyberobrony, którą koordynować będzie European Security and Defence College (ESDC)[66].

Ważne dla zdolności operacyjnych są ćwiczenia. „Cyber Europe". To największe cywilne, europejskie ćwiczenia z zakresu ochrony cyberprzestrzeni. Są one organizowane co dwa lata przez (ENISA) we współpracy z państwami członkowskimi UE i EFTA. Do tej pory odbyło się pięć edycji – w latach 2010, 2012, 2014, 2016 i 2018. W ostatnim czasie wzrosła liczba i częstotliwość ćwiczeń UE o silnym wymiarze cyberobrony. We wrześniu 2017 r. prezydencja estońska UE zorganizowała, w ścisłej współpracy z EDA, ćwiczenia cyberbezpieczeństwa na poziomie ministerialnym UE pod nazwą „CYBRID 2017", podczas których unijni ministrowie obrony mieli okazję przetestować procedury zarządzania kryzysowego w czasie kryzysu wywołanego zmasowanymi cyberatakami. Równocześnie odbywały się ćwiczenia EU PACE2017 i NATO CMX-17, które miały również zawartych wiele aspektów cybernetycznych w scenariuszu ćwiczeń. Ćwiczenia stanowiły okazję do przetestowanie procesu decyzyjnego w UE i NATO podczas kryzysu, którego elementami były cyberataki[67].

Autonomia przemysłowa. Posiadanie odpowiedniego zaplecza przemysłowego w postaci rozwiniętego sektora cyberbezpieczeństwa jest niezbędnym czynnikiem potencjału cybernetycznego UE. Jak już wspomniano wcześniej, sektor prywatny w środowisku cyberprzestrzeni odgrywa niewspółmiernie dużą rolę w stosunku do innych domen i stanowi wręcz element składowy systemu i polityki cyberbezpieczeństwa. Jednak w przypadku sektora cyberbezpieczeństwa trudniej oddzielić jego obronną część od części czysto cywilnej. Wielu ważnych graczy europejskiego sektora obronnego rozwinęło swoje segmenty ICT w kierunku dostarczania produktów i usług w zakresie cyberbezpieczeństwa (Airbus Group, Leonardo-, Thales). W większości przypadków mamy jednak do czynienia z firmami oferującymi rozwiązania zarówno dla sektora komercyjnego, jak i państwowego.

65 *Orędzie o stanie Unii w 2017 r. – cyberbezpieczeństwo: Komisja zwiększa zdolności reagowania UE na ataki cybernetyczne*, http://europa.eu/rapid/press-release_IP-17-3193_pl.htm (dostęp: 8.06.2018).

66 *ESDC: Cyber platform for education, training, evaluation and exercise (ETEE)*, https://eeas.europa.eu/delegations/guinea/39848/esdc-cyber-platform-education-training-evaluation-and-exercise-etee_fr (dostęp: 8.06.2018).

67 *Annual Report on the Implementation of the Cyber Defence Policy Framework*, http://data.consilium.europa.eu/doc/document/ST-15870-2017-INIT/en/pdf (dostęp: 8.06.2018).

Już w opublikowanym w 2013 r. komunikacie dotyczącym bardziej konkurencyjnego i wydajnego sektora obronności i bezpieczeństwa, Komisja Europejska stwierdzała: „Europa musi być w stanie przejąć odpowiedzialność za własne bezpieczeństwo, jak również, ogólnie rzecz biorąc, za pokój i stabilność międzynarodową. Wymaga to **pewnej strategicznej autonomii**: aby być wiarygodnym i niezawodnym partnerem, Europa musi mieć możliwość decydowania i działania, nie będąc zależną od potencjału stron trzecich. Decydujące znaczenie mają zatem bezpieczeństwo dostaw, dostęp do kluczowych technologii i suwerenność operacyjna”[68]. Z kolei w *Globalnej strategii na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej* z 2016 r. stwierdzono wprost: „Stabilny, innowacyjny i konkurencyjny europejski przemysł obronny ma **kluczowe znaczenie dla strategicznej autonomii Europy** i dla wiarygodnej WPBiO[69].

Ważnym elementem potencjału UE w dziedzinie cyberbezpieczeństwa jest wysoki poziom cyfryzacji gospodarki i życia społecznego. Pod tym względem UE jako całość nie ustępuje najważniejszym krajom świata. Również pod względem innowacyjności Europa możne mieć powody do zadowolenia. Rola sektora technologii teleinformatycznych (ICT) w gospodarce UE mierzona udziałem w PKB pozostaje na stałym poziomie 4,4% w latach 2010−2014, podczas gdy w USA osiągnęła 5,3%, w Japonii 5,4%, a w Chinach 4,7%. Natomiast zatrudnienie w tym sektorze wynosi 2,5% ogółu zatrudnionych w UE, co oznacza niższy poziom niż w USA (2,7%), Japonii (3,6%), Korei Południowej (4,2%) i tylko nieco wyższy niż w Chinach (1,9%)[70].

Ważnym aspektem potencjału przemysłowego UE w sferze cyberbezpieczeństwa jest duża zależność od zewnętrznych dostawców technologii, sprzętu i oprogramowania. Przy czym chodzi nie tylko o dominację firm z Doliny Krzemowej w USA (m.in. Microsoft, IBM, CISCO, Symantec), ale też o rosnące znaczenie producentów z Dalekiego Wschodu. Dodatkowo nie ma praktycznie przedsiębiorstw europejskich o uznanej pozycji w skali globalnej. W 2017 r. w gronie 500 największych firm światowych z branży

68 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w kierunku bardziej konkurencyjnego i wydajnego sektora obronności i bezpieczeństwa (COM/2013/0542 final), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52013DC0542&from=EN (dostęp: 8.06.2018).

69 *Globalna strategia*..., s. 44.

70 *Science, Research and Innovation Performance of the EU* (SRIP) report, 2018, s. 101−107, https://ec.europa.eu/info/sites/info/files/rec-17-015-srip-report2018_mep-web-20180228.pdf (dostęp: 8.06.2018).

cyberbezpieczeństwa jedynie 62 pochodziło z UE, z czego 24 z Wielkiej Brytanii. W rankingu tradycyjnie dominują firmy z USA – znalazło się ich tam aż 364. Inne kraje ważne w kontekście pochodzenia największych firm z branży cyberbezpieczeństwa to Izrael (36), Kanada (13) i Chiny (11)[71]. Wartość europejskiego rynku branży cyberbezpieczeństwa ocenia się na ok. 22 mld EUR w 2016 r., co stanowi ok. 1/5 wartości rynku światowego[72].

Dość dobrze wygląda pozycja UE w obszarze badań i rozwoju (R&D), unijne wydatki na te cele stanowią 20% wydatków globalnych. Pod tym względem ustępuje ona jedynie USA (27%) i nieznacznie Chinom (21%). Warto jednak zauważyć, że jeszcze w 2000 r. ówczesna UE (15 państw) odpowiadała za 1/4 światowych wydatków na badania i rozwój. Również tempo wzrostu tych wydatków w UE pozostawało na przestrzeni ostatnich lat w tyle za Chinami, USA i Japonią[73]. Natomiast inwestycje sektora prywatnego w badania i rozwój w obszarze ITC w przedsiębiorstwach europejskich były niemal dwukrotnie niższe niż w przypadku przedsiębiorstw amerykańskich[74].

Firmy sektora cyberbezpieczeństwa zrzesza i reprezentuje założona w czerwcu 2016 r. Europejska Organizacja Cyberbezpieczeństwa (ECSO). Obecnie liczy ona 230 członków, wśród których poza przedsiębiorstwami z branży są również ośrodki badawcze, uniwersytety oraz władze lokalne. W ramach programu badawczego UE „Horyzont 2020" na lata 2007−2020 wydatki na projekty dotyczące szeroko rozumianego cyberbezpieczeństwa wyniosły dotychczas ok. 190 mln EUR. Dodatkowo ze strony Komisji Europejskiej przewidziano kwotę 450 mln EUR na projekty badawcze w ramach partnerstwa publiczno-prywatnego w sektorze cyberbezpieczeństwa. Wkład sektora prywatnego do tego projektu wyniesie 1,35 mld EUR. Partnerem ze strony sektora prywatnego jest ECSO.

Podsumowanie

Polityka cyberbezpieczeństwa UE, mimo poczynionego w ostatnich latach wyraźnego postępu, wciąż nie uzyskała w pełni kompleksowej formy, brak

71 Cybersecurity 500 list, https://cybersecurityventures.com/cybersecurity-500/ (dostęp: 24.03.2018).

72 Cyber security: Emerging leaders in Europe, PwC 2017, www.pwc.co.uk/services/strategy/insights/cyber-security--european-emerging-market-leaders.html (dostęp: 8.06.2018).

73 Science, Research And Innovation Performance Of The Eu. 2018, s. 78−85, https://ec.europa.eu/info/sites/info/files/rec-17-015-srip-report2018_mep-web-20180228.pdf (dostęp: 8.06.2018).

74 *Ibidem*, s. 105−107.

jej też niezbędnej spójności. Przejawia się to zarówno na płaszczyźnie regulacyjnej, jak i instytucjonalnej. Dążenie do osiągnięcia przez UE autonomii strategicznej w cyberprzestrzeni nie jest oparte na wystarczająco solidnych podstawach i w dużym stopniu pozostaje na poziomie ambicjonalnym. W wymiarze tradycyjnym (tzw. *hard power*) wizja pełnej autonomii strategicznej, związanej z posiadaniem własnych zdolności do cyberobrony, pozostaje daleka od realizacji[75]. Państwa członkowskie dostrzegają potrzebę wzmocnienia posiadanych zasobów, jednak niechętnie podchodzą do udostępniania posiadanych zdolności. Potencjał poszczególnych państw w dziedzinie cyberbezpieczeństwa jest też mocno zróżnicowany, jaskrawo widoczne są dysproporcje między grupą liderów a resztą. Wystąpienie Wielkiej Brytanii z UE znacząco osłabi potencjał unijny w tej kwestii. Brytyjczycy posiadają dużo różnorodnych zdolności cybernetycznych, w tym jako jedni z nielicznych zdolności ofensywne i zdolności do atrybucji cyberataków. Dodatkowo uczestniczą we współpracy wywiadowczej i rozpoznania elektronicznego państw anglosaskich (tzw. *Five Eyes Alliance*). Zdaje się, że konieczność utrzymania w przyszłości bliskiej, zinstytucjonalizowanej współpracy Wielkiej Brytanii z UE w zakresie cyberbezpieczeństwa dostrzega się zarówno w Londynie, jak i w Brukseli, o czym świadczy dokument rządu brytyjskiego przedstawiony przed rozpoczęciem negocjacji[76].

W obszarze zdolności do cyberobrony państwa europejskie preferują współpracę i podział zadań między UE i NATO, działania unijne zaś traktowane są w znacznej mierze komplementarnie. Warto podkreślić, że współpraca NATO−UE w obszarze cyberobrony rozwija się zasadniczo bez zakłóceń i dotychczas udało się uniknąć jej upolitycznienia. Realizacja Wspólnej deklaracji NATO−UE, podpisanej w czerwcu 2016 r. na marginesie Szczytu Sojuszu w Warszawie, w zakresie cyberbezpieczeństwa i cyberobrony przebiega harmonijnie, o czym świadczy ostatni raport z jej wdrażania[77].

75 Reprezentowana jest ona przez scenariusz trzeci w dokumencie otwierającym debatę na temat przyszłości europejskiej obronności do 2025 r., przedstawionym przez Komisję Europejską w czerwcu 2017 r., https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52017DC0315&from=EN (dostęp: 8.06.2018).

76 *Policy paper. Foreign policy, defence and development – a future partnership*, paperhttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643924/Foreign_policy__defence_and_development_paper.pdf (dostęp: 30.04.2018).

77 *Konkluzje Rady w sprawie realizacji Wspólnej deklaracji przewodniczącego Rady Europejskiej, przewodniczącego Komisji Europejskiej i sekretarza generalnego Organizacji Traktatu Północnoatlantyckiego*, www.consilium.europa.eu/media/31947/st14802en17.pdf (dostęp: 8.06.2018).

Większe szanse zdają się rysować przed UE w wymiarze tzw. miękkiego bezpieczeństwa, wzmacniania zewnętrznego wymiaru polityki unijnej w sprawach cyberbezpieczeństwa, zwiększania odporności sieci i systemów teleinformatycznych na zagrożenia cybernetyczne, wypracowywania zdolności i instrumentów reagowania na cyberataki, skutecznej współpracy w zakresie zwalczania cyberprzestępczości, promocji norm i wartości w cyberprzestrzeni. Postęp w tych obszarach przesądzi o potencjale UE w tym obszarze i jej pozycji na arenie globalnej. Wymagać to będzie jednak w kolejnych latach podjęcia świadomych i skoordynowanych działań, wspartych odpowiednim poziomem finansowania. Przejawem takiego nowego podejścia jest opublikowany we wrześniu 2017 r. tzw. pakiet cyberbezpieczeństwa zawierający wiele różnorodnych propozycji. Pewne powody do optymizmu daje przedstawiony 2 maja 2018 r. projekt nowych, wieloletnich ram finansowych na lata 2021−2027. Zaproponowano w nim znaczące zwiększenie środków na szeroko pojęty obszar cyberbezpieczeństwa, w szczególności w ramach programu badań naukowych i innowacji, programu inwestycji strategicznych „Cyfrowa Europa" oraz Europejskiego Funduszu Obrony[78]. Dopiero realizacja tych zamierzeń stworzy solidne podstawy do budowy autonomii strategicznej UE.

Unia Europejska, ze względu na swoje interesy gospodarcze, globalne ambicje i kierunki zagrożeń dla bezpieczeństwa, musi wypracować i realizować wiarygodną politykę w zakresie cyberbezpieczeństwa, która będzie oparta na odpowiednim instrumentarium i sprawnych instytucjach. Europa nie może się wyrzec prowadzenia aktywnej polityki w cyberprzestrzeni, która staje się kolejnym obszarem strategicznej rywalizacji w skali globalnej. To, czy będzie ona zmierzała w kierunku większej autonomii strategicznej, zależy zarówno od posiadanego przez UE potencjału, jak i woli politycznej państw członkowskich.

Polska powinna być zainteresowana jak najpełniejszym udziałem w formułowaniu polityki cyberbezpieczeństwa UE. Transgraniczny charakter zagrożeń cybernetycznych sprawia, że poziom odporności UE w tej kwestii ma bezpośrednie przełożenie na nasze bezpieczeństwo narodowe. Dotychczasowy kierunek rozwoju potencjału UE w tej kwestii, a zwłaszcza bliska współpraca z NATO, dają szanse na uniknięcie trudnych dylematów politycznych. Jednocześnie obszar szeroko rozumianego cyberbezpieczeństwa stanowi obecnie istotny obszar konwergencji interesów Europy i USA,

78 *Budżet UE: Komisja proponuje nowoczesny budżet dla Unii, która chroni, wspiera i broni*, Bruksela, 2 maja 2018 r., http://europa.eu/rapid/press-release_IP-18-3570_pl.htm (dostęp: 8.06.2018).

zwłaszcza w obliczu rosnącej rywalizacji głównych aktorów globalnych o wpływ na kształt cyberprzestrzeni. We wspólnym interesie całej wspólnoty euroatlantyckiej leży zapobieżenie fragmentacji cyberprzestrzeni oraz zachowanie jej otwartego, wolnego i powszechnego charakteru.

Biblioteka

Barburska O., *Argument siły czy siła argumentów? Unia Europejska w stosunkach międzynarodowych jako soft power*, „Rocznik Integracji Europejskiej" 2016, nr 10.

Betz D.J., Stevens T., *Cyberspace and the State: Toward a Strategy for Cyber-Power*, Routledge, Abingdon 2011.

Cavelty M.D., *Europe's Cyber-Power*, „European Politics and Society" 2018, vol. 19, nr 3, https://doi.org/10.1080/23745118.2018.1430718.

Christou G., *Cybersecurity in the European Union*, Palgrave Macmillan, Basingstoke 2016.

Czebotar Ł., *Strategia Stanów Zjednoczonych wobec problemu bezpieczeństwa cyberprzestrzeni*, w: A. Podraza, P. Potakowski, K. Wiak (red.), *Cyberterroryzm zagrożeniem XXI wieku*, Difin, Warszawa 2013.

Daniluk P., *Kultura strategiczna Unii Europejskiej. Podejście normatywne*, „Rocznik Bezpieczeństwa Międzynarodowego" 2015, vol. 9, nr 2.

Demczuk A., *Od raportu Bangemanna do Strategii Europa 2020. Rozwój społeczeństwa informacyjnego w polityce Unii Europejskiej – bilans 15 lat*, „Annales UMCS" 2016, vol. 23, nr 2.

Globally, People Point to ISIS and Climate Change as Leading Security Threats, Pew Research Center, August, 2017, www.pewglobal.org/2017/08/01/globally-people-point-to-isis-and-climate-change-as-leading-security-threats.

Haataja S., *The 2007 Cyberattacks Against Estonia and International Law on the Use of Force: An Informational Approach*, „Law, Innovation and Technology" 2017.

Hollis D., *Cyberwar Case Study: Georgia 2008*, „Small Wars Journal" 2011, http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

Jørgensen K.E., Laatikainen K.V. (red.), *Routledge Handbook on the European Union and International Institutions: Performance, Policy, Power*, Routledge, Abingdon 2013.

Katainen J., Limnell J., *Cybersecurity and Defence for the Future of Europe*, „EUobserver", 10 IV 2018, https://euobserver.com/opinion/141556.

Klimburg A., *Mobilising Cyber Power*, „Survival" 2011, vol. 53, nr 1.

Klimburg A., *The Whole of Nation in Cyberpower*, „Georgetown Journal of International Affairs" 2011, special issue: *International Engagement on Cyber*.

Kuehl D.T., *From Cyberspace to Cyberpower: Defining the Problem*, w: D. Kramer, H. Stuart, L.K. Wentz, *Cyberpower and National Security Policy*, National Defense University, Potomac Books, Inc., Washington 2009, http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf.

Kupiecki R., *Unia Europejska i problemy strategii bezpieczeństwa podmiotów zbiorowych*, „Sprawy Międzynarodowe" 2014, nr 4.

Lakomy M., *Cyberwojna jako rzeczywistość XXI wieku*, „Stosunki Międzynarodowe" 2011, nr 3−4.

Maliszewska-Nienartowicz J., *Założenia Globalnej strategii na rzecz polityki zagranicznej i bezpieczeństwa UE – przełom czy stagnacja?*, „Sprawy Międzynarodowe" 2017, nr 2.

Mogherini Calls EU a Peace 'Superpower', in Wake of Trump Win, EurActiv, 10 XI 2016, www.euractiv.com/section/security/news/mogherini-calls-eu-a-peace-superpower-in-wake-of--trump-win.

Nye J.S., *Cyber Power*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge 2010, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

Pieńkoś A., *Europejska Agencja Obrony w systemie współpracy przemysłowo-obronnej w Europie*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2017.

Professor Sounds Alarm over Dutch Cyber Security Brain Drain, DutchNews.nl, 23 IV 2018, www.dutchnews.nl/news/2018/04/professor-sounds-alarm-over-dutch-cyber-security-brain-drain.

R. Kuźniar, *Polityka i siła. Studia strategiczne – zarys problematyki*, Wydawnictwo Naukowe „Scholar"–Fundacja Studiów Międzynarodowych, Warszawa 2005.

Schmitt M. (red.), *The Law of Armed Conflict Generally. In Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge 2017.

Szymański P., *Pozory i konkrety. Polityka bezpieczeństwa i siły zbrojne Danii*, Komentarze OSW, 23 IV 2018.

Tadeusiewicz R., *Zagrożenia w cyberprzestrzeni*, „Nauka" 2010, nr 4.

Terlikowski M., *Pierwsze projekty PESCO: w poszukiwaniu przełomu*, „Biuletyn PISM", 8 V 2018, nr 65.

Wystąpienie Emmanuela Macrona *Inicjatywa dla Europy*, www.diplomatie.gouv.fr/en/french--foreign-policy/european-union/events/article/president-macron-s-initiative-for-europe-a--sovereign-united-democratic-europe.