https://www.doi.org/10.12797/9788381383899.02

Robert Siudak
Uniwersytet Jagielloński w Krakowie

Od jednolitego rynku do cyberobrony

Ewolucja polityk cyberbezpieczeństwa UE w latach 1993-2016

Abstract: The European Union (EU) is currently one of the most active stakeholderst of the global debate on cybersecurity standards and regulations. To understand the source of that this article is analyzing the evolution of the EU stance towards the security of information and communication technologies between 1993 and 2016. The initial focus on the economic security paradigm (single market) has been extended successively with elements of social and civil security (judiciary and internal security systems), to national security and international relations (cyber defense, cyber diplomacy). The key document setting the directions of the EU actions in that area has been the *EU cyber security strategy: An open, safe and secure cyberspace* from 2013. The most impactful European law from that period has been *Directive on security of network and information systems* passed in 2016 (NIS Directive).

Keywords: European Union, cybersecurity, critical infrastructure

Unia Europejska (UE) to aktualnie jeden z najbardziej aktywnych uczestników globalnej debaty dotyczącej norm i regulacji w zakresie cyberbezpieczeństwa. Tak rozbudowana działalność UE w dziedzinie bezpieczeństwa technologii informacyjno-

-komunikacyjnych (TIK) jest jednak dopiero kwestią ostatnich lat, szczególnie po roku 2013. Dość wspomnieć, że Europejska Strategia Bezpieczeństwa z roku 2003 nie odnosiła się w ogóle do problematyki cyberbezpieczeństwa. Żeby zrozumieć źródła takiego stanu rzeczy, w ramach niniejszego artykułu prześledzono ewolucję podejścia do kwestii bezpieczeństwa TIK w UE w latach 1993-2016. Analizę oparto na oficjalnych dokumentach Wspólnoty oraz upublicznionych materiałach roboczych instytucji i organów UE.

Na przykładzie problematyki cyberbezpieczeństwa prześledzić można realizację tak zwanego efektu *spill-over* w UE, polegającego na rozszerzaniu i pogłębianiu z biegiem czasu współpracy w określonych obszarach. W tym wypadku obserwować można wyjście od paradygmatu bezpieczeństwa ekonomicznego (wspólny rynek), przez bezpieczeństwo społeczne i cywilne (system sądowniczy i policyjny), aż po bezpieczeństwo narodowe i stosunki międzynarodowe (cyberobrona, cyberdyplomacja). W ramach artykułu dokonano szczegółowego omówienia sześciu podstawowych faz ewolucji podejścia UE w latach 1993-2016, z których każda rozszerzała oraz pogłębiała zakres rozumienia i podejmowania tematyki cyberbezpieczeństwa przez Wspólnotę:

1. bezpieczeństwo TIK jako element rozwoju jednolitego rynku;
2. rozszerzenie polityk UE o temat cyberprzestępczości oraz problem szkodliwych i nielegalnych treści w Internecie;
3. rozszerzenie polityk UE o kwestie związane z zagrożeniem terrorystycznym;
4. rozszerzenie polityk UE o zagadnienie cyberobrony;
5. rozszerzenie polityk UE w celu wsparcia europejskiego rynku cyberbezpieczeństwa oraz wypracowania wspólnych standardów przemysłowych;
6. rozszerzenie polityk UE o zagadnienia związane z cyberdyplomacją.

1993-2009: Jednolity rynek, *high-tech crime*, terroryzm

Pierwsze trzy fazy włączania analizowanej tematyki w zakres działań UE można postrzegać jako próby wprowadzania treści związanych z bezpieczeństwem TIK do trzech kolejnych filarów współpracy unijnej zgodnie z architekturą wspólnoty ustanowioną traktatem z Maastricht[1]. Pierwszym dokumentem w ramach UE, który podnosił kwestie bezpieczeństwa TIK, była opublikowana przez Komisję Europejską (KE) w 1994 roku Biała Księga *Growth, Competitiveness, Employment. The Challenges and Ways Forward into the 21st century*. W ramach zawartego w niej planu działań

[1] I filar – Unia gospodarcza, II filar – Wspólna Polityka Zagraniczna i Bezpieczeństwa (WPZiB), III – Współpraca policyjna i sądowa w sprawach karnych.

wyróżniono pięć głównych priorytetów, w tym kwestie stworzenia odpowiednich ram regulacyjnych, które m.in. „będą chronić prywatność oraz zapewnią bezpieczeństwo systemów informacyjno-komunikacyjnych”[2]. Rok później w raporcie grupy Bangemanna zwrócono uwagę na dwa wymiary wyzwań związanych z bezpieczeństwem cyfrowym na wspólnym rynku. Pierwszy z nich, techniczny, dotyczył głównie szyfrowania i rozważany był szczególnie w kontekście bezpieczeństwa handlu elektronicznego. Drugi, prawny, odnosił się do pewności i zaufania do usług oferowanych poprzez technologie teleinformatyczne, a także przeciwdziałania piractwu. Konkludując wskazane w raporcie rekomendacje, Parlament Europejski (PE) w swojej rezolucji z 1996 roku wezwał Komisję oraz państwa członkowskie do „stworzenia niezbędnych regulacji uzupełniających oraz ram prawnych w zakresie […] bezpieczeństwa danych i poufności”[3].

Rozszerzenie zainteresowania UE w omawianym temacie na cyberprzestępczość oraz szkodliwe i nielegalne treści w Internecie przyniósł dopiero koniec lat 90. XX wieku. W 1998 roku KE zaprezentowała Radzie Europejskiej (RE) wyniki badania dotyczącego przestępczości komputerowej (ang. *computer-related crime*). Rok później w konkluzjach RE z Tampere wprowadzono pojęcie przestępczości związanej z wykorzystaniem zaawansowanych technologii (ang. *high-tech crime*). Wskazano jednocześnie, że kategoria ta powinna zostać ujednolicona w zakresie prawa karnego państw członkowskich[4]. Kolejnym krokiem był komunikat KE *Tworzenie bezpiecznego społeczeństwa informacyjnego poprzez poprawę bezpieczeństwa infrastruktury teleinformatycznej oraz walkę z przestępczością komputerową* z roku 2001. Zawarty w nim szeroki wachlarz działań na poziomie ponadnarodowym wynikał z diagnozy wskazującej, że „przestępstwa komputerowe są popełniane w cyberprzestrzeni, a przez to nie zatrzymują się na progu konwencjonalnych granic państwowych”[5].

---

[2] European Commission, *Growth, Competitiveness, Employment. The Challenges and Ways Forward into the 21st Century*, COM (93) 700 final, Brussels, 5 XII 1993, s. 24.

[3] European Parliament, *Resolution on 'Europe and the global information society – Recommendations to the European Council' and on a communication from the Commission of the European Communities: 'Europe's way to the information society: an action plan' (COM(94)0347 – C4–0093/94)*, 1996, [on-line:] https://publications.europa.eu/en/publication-detail/-/publication/93dee954-b8b9-495e-af03-e678161b06ab – 18 VI 2019.

[4] European Council, *Tampere European Council 15 and 16 October 1999. Presidency Conclusions*, 1999, [on-line:] http://www.europarl.europa.eu/summits/tam_en.htm#c – 19 VI 2019.

[5] European Commission, *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, 2001, s. 7, [on-line:] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0890&from=CS – 19 VI 2019.

Oprócz poszerzania zakresu zainteresowania UE w kierunku cyberprzestępczości następowało równoczesne pogłębianie problematyki bezpieczeństwa technologii informacyjno-komunikacyjnych (ang. *Information and Communication Technologies*, ICT) w kontekście jednolitego europejskiego rynku. Oprócz aspektu ekonomicznego zaczęto coraz częściej podnosić aspekt społeczny, w ramach którego bezpieczeństwo cyfrowe stanowi nie tylko jeden z elementów niezbędnych do rozwoju rynku, ale także jedno z ważnych praw obywatelskich. Odpowiedzią na to był plan działań *Społeczeństwo informacyjne dla każdego*, a także komunikat KE z roku 2001 *Network and Information Security: Proposal for A European Policy Approach*[6]. Znalazły się w nim zapisy, które w decydujący sposób ukształtowały debatę na kolejne lata, w tym pojęcie „bezpieczeństwa sieci i informacji" jako kluczowego celu[7]. Komisja przedstawiła także szereg działań, które należało podjąć, m.in. wymianę informacji pomiędzy krajowymi zespołami reagowania na incydenty komputerowe, wsparcie techniczne dla rozwoju i rozprzestrzenienia bezpiecznych TIK (np. IPv6, IPSec) czy harmonizację prawa w zakresie nieskrępowanego obrotu produktami kryptograficznymi. Realizacja tak ambitnie nakreślonych celów wymagała stałego wsparcia w ramach struktury unijnej, m.in. dlatego też w roku 2004 powołano do życia Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ang. European Union Agency for Network and Information Security, ENISA)[8]. Podsumowaniem dotychczasowego podejścia UE była uchwalona w 2006 roku Strategia na rzecz bezpiecznego społeczeństwa informacyjnego, która skupiała się na trzech podnoszonych już wcześniej tematach:

1. bezpieczeństwie sieci i informacji;
2. regulacjach dla łączności elektronicznej, w tym ochrony danych oraz prywatności;
3. zwalczaniu przestępczości internetowej[9].

---

[6] European Parliament, *Resolution on 'Europe and the global information society – Recommendations to the European Council' and on a communication from the Commission of the European Communities: 'Europe's way to the information society: an action plan' (COM(94)0347 – C4–0093/94)*, 1996, [on-line:] https://publications.europa.eu/en/publication-detail/-/publication/93dee954-b8b9-495e-af03-e678161b06ab – 18 VI 2019.

[7] *Ibidem*.

[8] European Commission, *Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance)*, 2004, [on-line:] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML – 21 VI 2019; European Union Agency for Network and Information Security, *ENISA Strategy 2016-2020*, [on-line:] https://www.enisa.europa.eu/publications/corporate/enisa-strategy – 21 VI 2019.

[9] Komisja Europejska, *Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – „Dialog, partnerstwo i przejmowanie inicjatywy" {SEC(2006) 656} /* COM/2006/0251*

Ostatnim obszarem w ramach trójfilarowej struktury UE, który aż do końca pierwszej dekady XXI wieku nie uwzględniał szerzej wyzwań związanych z bezpieczeństwem TIK, była Wspólna Polityka Zagraniczna i Bezpieczeństwa. Pierwszym elementem łączącym te dwa tematy było rozpoznanie przez Wspólnotę zagrożenia terrorystycznego związanego z atakami na systemy teleinformatyczne. Zwrócono na tę kwestię uwagę w decyzji ramowej Rady z roku 2005[10]. Debatę w tym zakresie poszerzył komunikat KE *Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności* z roku 2009, który stanowił pokłosie debaty wywołanej przez kryzys estoński z roku 2007. Wprowadził on pojęcie krytycznej infrastruktury informatycznej (ang. *critical information infrastructures* CII), która stanowić miała potencjalny cel ataku dla działań terrorystycznych[11]. Aby zapewnić bezpieczeństwo CII, Komisja zaproponowała plan działania oparty na pięciu filarach, które dotyczyły zarówno poziomu technicznego, operacyjnego, jak i regulacyjnego[12]. Z kolei potrzebę szerszej inkorporacji perspektywy obronnej oraz międzynarodowej w ramach debaty nad cyberbezpieczeństwem zasygnalizowało *Sprawozdanie na temat wdrażania europejskiej strategii bezpieczeństwa – utrzymanie bezpieczeństwa w zmieniającym się świecie* z roku 2008, w którym zauważono, że „ataki skierowane na prywatne lub rządowe systemy informatyczne w państwach członkowskich UE nadały mu [zagrożeniu] nowy wymiar, jako potencjalnej nowej broni ekonomicznej, politycznej i wojskowej"[13]. Pomimo nakreślenia samego wyzwania UE w znacznej mierze nie zaadresowała problematyki cyberbezpieczeństwa w ramach funkcjonowania drugiego filaru wspólnoty. Dopiero ewolucja samej UE, rozpoczęta traktatem lizbońskim z roku 2009, w tym zarzucenie filarowej struktury, pozwoliła na rozwój horyzontalnego podejścia do cyberbezpieczeństwa, czego owocem stała się pierwsza wspólnotowa strategia w tym zakresie.

---

*końcowy */*, 2006, [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52006DC0251&from=EN – 21 VI 2019.

[10] Dz. Urz. UE L 69/67 z 16.3.2005 r., [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32005F0222&from=EN – 24 VI 2019.

[11] Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ochrony krytycznej infrastruktury informatycznej – „Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności" {SEC(2009) 399} {SEC(2009) 400} /* COM/2009/0149 końcowy */*, 2009, [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52009DC0149&from=EN – 24 VI 2019.

[12] *Ibidem*.

[13] Zob. Rada Unii Europejskiej, *Europejska Strategia Bezpieczeństwa. Bezpieczna Europa w lepszym świecie,* 2009, s. 13, [on-line:] https://www.bbn.gov.pl/ftp/dok/01/strategia_bezpieczenstwa_ue_2003.pdfm – 24 VI 2019.

2010-2016: Obrona, przemysł ITSEC, dyplomacja

Proces dochodzenia do horyzontalnego podejścia UE do kwestii cyberbezpieczeństwa rozpoczęty został już w ramach programu sztokholmskiego „Otwarta i bezpieczna Europa dla dobra i ochrony obywateli z lat 2010-2014"[14]. Stanowił on sygnał do wielu działań, od zrealizowanego jeszcze w 2013 roku utworzenia Europejskiego Centrum do spraw Walki z Cyberprzestępczością przy Europolu (EC3)[15], po opracowanie modelowej umowy o partnerstwie publiczno-prywatnym na rzecz walki z cyberprzestępczością. Jeszcze w roku 2010 w Strategii Bezpieczeństwa Wewnętrznego Unii Europejskiej wyróżniono działania z wykorzystaniem TIK jako jedno z siedmiu kluczowych wyzwań dla Wspólnoty, skupiając się na wymiarze związanym z cyberprzestępczością transnarodową[16]. W odpowiedzi na to w tym samym roku w ramach Europejskiej Agendy Cyfrowej wskazano na potrzebę powołania Zespołu Reagowania na Incydenty Komputerowe przeznaczonego dla instytucji unijnych – CERT UE (ang. Computer Emergency Response Team, CERT) oraz wzmocnienia współpracy pomiędzy CERT-ami z krajów członkowskich[17]. CERT EU rozpoczął swoją pełną działalność w roku 2012, a w tym samym roku w ramach Rady Unii Europejskiej (RUE) zawiązano Grupę przyjaciół prezydencji ds. zagadnień cyber (przemianowaną w roku 2016 na Horyzontalną Grupę Roboczą ds. cyberzagadnień)[18]. Jednak to dopiero rezolucja PE *Cyberbezpieczeństwo i obrona*, także z roku 2012, stanowiła realny impuls do poszerzenia debaty na poziomie UE o kolejny obszar – cyberobronę[19]. Wprost wskazywała ona na „konieczność przyjęcia globalnego i skoordynowanego podejścia do tych wyzwań na szczeblu UE poprzez opracowanie kompleksowej unijnej strategii bezpieczeństwa

---

[14] Dz. Urz. UE C 115/1 z 04.05.2010 r., [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:52010XG0504(01) – 24 VI 2019.

[15] Europol, *European Cybercrime Centre – EC3*, [on-line:] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 – 24 VI 2019.

[16] European Council, *Internal security strategy for the European Union. Towards a European security model*, 2010, [on-line:] https://www.consilium.europa.eu/media/30753/qc3010313enc.pdf – 13 VII 2019.

[17] Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Europejska agenda cyfrowa*, 2010, [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52010DC0245&from=en – 13 VII 2019.

[18] Ang. Friends of the Presidency Group on Cyber Issues, za: Council of the European Union, *Horizontal Working Group on Cyber Issues – Establishment and adoption of its Terms of Reference*, 20 X 2016, [on-line:] http://data.consilium.europa.eu/doc/document/ST-13114-2016-INIT/en/pdf – 13 VII 2019.

[19] Dz. Urz. UE C 419/145 z 16.12.2015 r., [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52012IP0457&from=PL – 13 VII 2019.

cybernetycznego, która powinna zapewnić wspólną definicję bezpieczeństwa cybernetycznego i cyberobrony oraz cyberataku z nią związanego, wspólną wizję działań"[20].

W odpowiedzi na tak postawione zadanie Komisja Europejska w roku 2013 opublikowała *Strategię bezpieczeństwa cybernetycznego UE: otwarta, bezpieczna i chroniona cyberprzestrzeń*[21]. Wyróżniono w niej pięć priorytetowych celów:

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. rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa;
5. ustanowienie spójnej międzynarodowej polityki dotyczącej cyberprzestrzeni oraz promowanie podstawowych wartości UE.

Realizując pierwszy z celów priorytetowych Strategii, w roku 2016 przyjęto *Dyrektywę Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*, zwaną dyrektywą NIS (ang. *Network and Information Systems*). W praktyce stanowiła ona przełomowy akt prawny, do dziś będący najbardziej rozpoznawalnym elementem legislacji UE nakierowanej na zwiększanie poziomu cyberbezpieczeństwa w Europie. Dyrektywa NIS posiada trzy główne cele:

1. poprawę zdolności do podejmowania skoordynowanych działań na poziomie poszczególnych krajów członkowskich;
2. rozwijanie współpracy pomiędzy państwami na poziomie UE;
3. zobligowanie operatorów usług kluczowych i dostawców usług cyfrowych do wdrożenia odpowiednich procedur w zakresie zarządzania ryzykiem oraz zgłaszania incydentów.

Dyrektywa jest aktem UE implementowanym do porządku prawnego państw członkowskich pośrednio, poprzez odpowiednią legislację na poziomie narodowym. W przypadku dyrektywy NIS przewidziano transpozycję zapisów do prawa krajowego do 9 maja 2018 roku. W celu wsparcia procesu implementacji w 2017 roku Komisja

---

[20] *Ibidem*.

[21] European Commission, *Joint Communication to the European Parliament, the Council, the European Economic And Social Committee And the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013*, [on-line:] https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf – 13 VII 2019.

opublikowała komunikat *Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji*[22], doprecyzowujący oraz objaśniający szereg zapisów samej dyrektywy.

Drugi obszar priorytetowy strategii, dotyczący ograniczenia cyberprzestępczości, stanowił kontynuację działań podejmowanych jeszcze od końca lat 90. XX wieku. Realizację celów w tym zakresie zapewnić miała *Dyrektywa dotycząca ataków na systemy informatyczne* z 2013 roku, której celem jest przede wszystkim zbliżenie prawa karnego państw członkowskich, m.in. poprzez harmonizację definicji przestępstw dotyczących ataków na systemy informatyczne oraz odpowiadających im kar[23]. Dyrektywa stawia sobie za cel także poprawę transnarodowej współpracy organów policyjnych oraz dedykowanych agencji i instytucji na poziomie UE, w tym Eurojustu, Europolu oraz ENISA. Kolejnym dokumentem, który potwierdził wagę problematyki przestępczości cyfrowej w UE, była *Europejska agenda bezpieczeństwa* z roku 2015, w której w ramach trzech największych wyzwań dla bezpieczeństwa obywateli wspólnoty wskazano cyberprzestępczość, obok terroryzmu oraz zorganizowanej przestępczości.

Za trzeci obszar kluczowy w strategii uznano rozwój ram oraz zdolności w zakresie cyberobrony. W celu jego realizacji już w 2014 roku Rada Unii Europejskiej zatwierdziła „Ramy polityki UE w zakresie cyberobrony"[24], które wskazują cyberprzestrzeń jako piąty obszar działań wojskowych, obok tradycyjnych domen. W dokumencie wyróżniono także pięć priorytetów UE w zakresie cyberobrony:

1. wspieranie rozwijania związanych ze Wspólną Polityką Bezpieczeństwa i Obrony (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 szerzej pojętymi politykami cybernetycznymi UE, odpowiednimi instytucjami i agencjami UE, a także z sektorem prywatnym;
4. poprawę możliwości w zakresie szkolenia, kształcenia i ćwiczeń;
5. zacieśnianie współpracy z odpowiednimi partnerami międzynarodowymi (wskazując przede wszystkim NATO, OBWE oraz ONZ).

---

[22] Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego i Rady: Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji – zapewnienie skutecznego wdrożenia dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*, 2017, [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52017DC0476&from=EN – 13 VII 2019.

[23] Dz. Urz. UE L 218/8 z 14.08.2013 r., [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32013L0040&from=PL – 14 VII 2019.

[24] Rada Unii Europejskiej, *Ramy polityki UE w zakresie cyberobrony*, 18 listopada 2014, [on-line:] http://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/pl/pdf – 15 VII 2019.

Aktywną rolę w wypełnianiu tak nakreślonych celów przejęła w kolejnych latach m.in. Europejska Agencja Obrony (ang. European Defence Agency, EDA), która w ramach realizowania Capability Development Plan z roku 2014 koordynuje szereg działań, m.in. szkolenie funkcjonariuszy publicznych państw UE, wspieranie wykrywania ataków typu APT (ang. *Advanced Persistent Threat*) czy wykorzystanie informatyki śledczej na potrzeby wojska[25]. Kolejnym kluczowym elementem w tym obszarze stała się współpraca ze strukturami Sojuszu Północnoatlantyckiego. Na początku 2016 roku CERT EU oraz NATO Computer Incident Response Capability (NCIRC) podpisały porozumienie techniczne w zakresie wymiany informacji oraz współpracy operacyjnej. Następnie na szczycie NATO w Warszawie tego samego roku podpisano wspólną deklarację NATO-EU, w ramach której określono siedem priorytetowych obszarów kooperacji, w tym współpracę w zakresie cyberbezpieczeństwa i cyberobrony[26].

Czwarty cel strategii stanowi rozbudowa zaplecza technologicznego oraz rozwój branży cyberbezpieczeństwa w UE. Zgodnie ze zleconym przez KE badaniem europejski rynek bezpieczeństwa TIK był wart w 2016 roku 157 miliardów euro, co stanowiło 26,3% globalnego rynku[27].

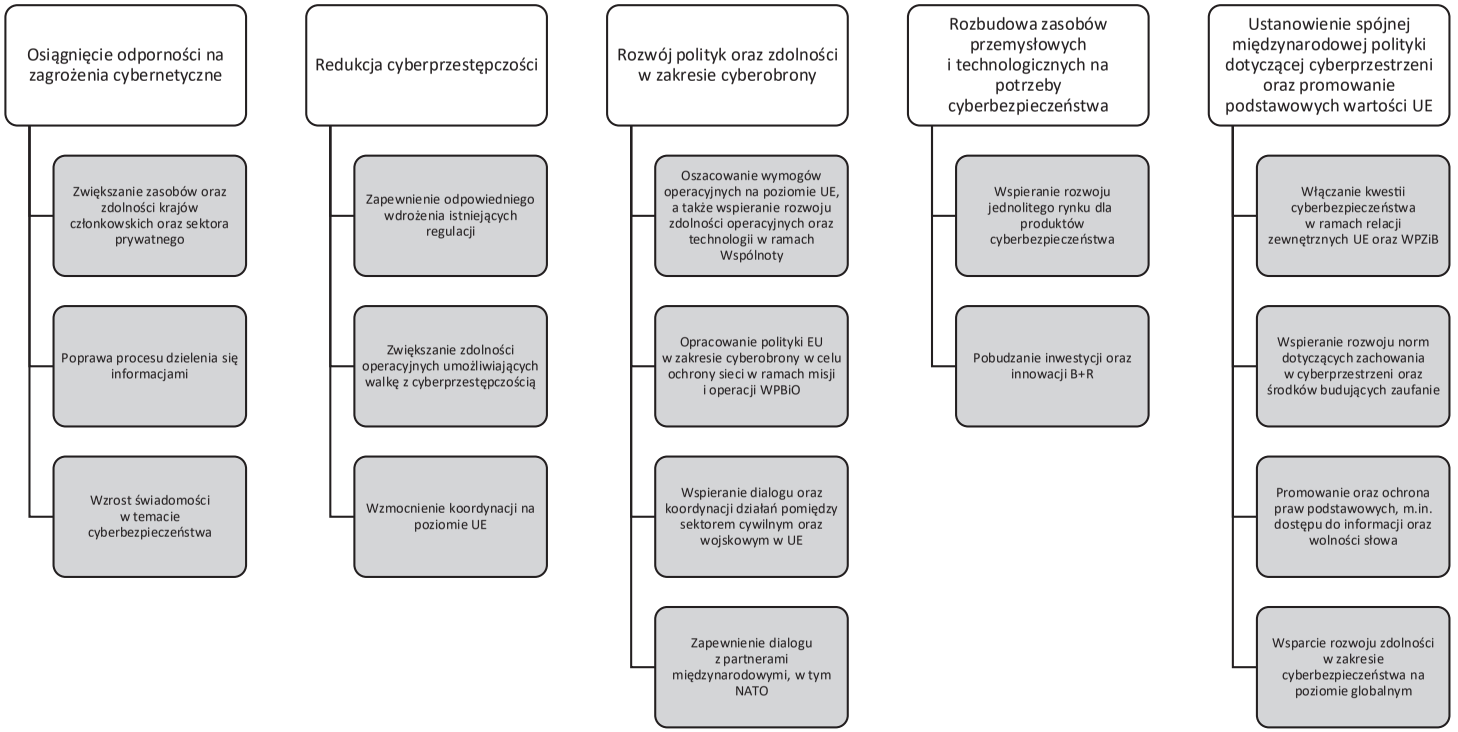
---

[25] M. Szczygieł, *Polityka cyberbezpieczeństwa Unii Europejskiej – początek drogi do strategicznej autonomii*, „Sprawy Międzynarodowe" 2018, nr 2, s. 175; por. European Defence Agency, *Cyber Defence*, [on-line:] https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence – 15 VII 2019.

[26] NATO, *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*, 08.07.2016, [on-line:] www.nato.int/cps/en/natohq/official_texts_133163.htm?selectedLocale=en – 15 VII 2019.

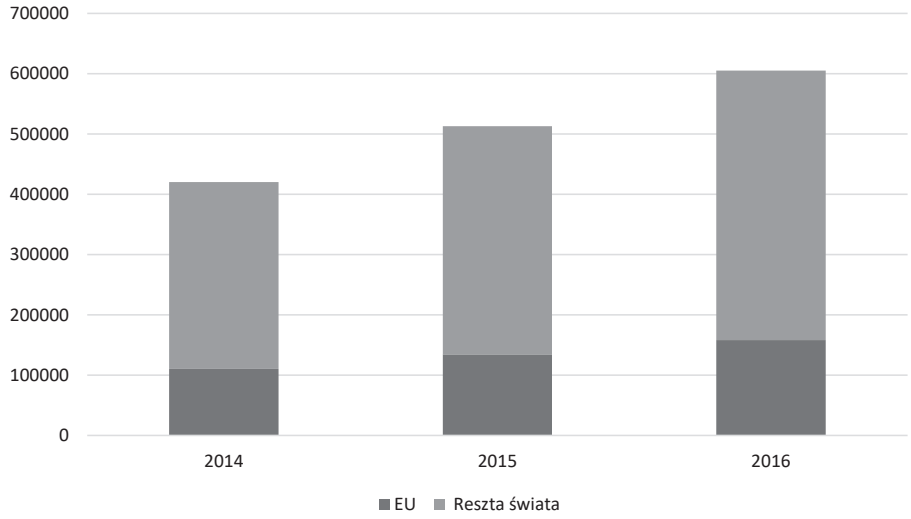
[27] LSEC, *CIMA – LSEC European Cyber Security Industry Market Analysis*, 2017, [on-line:] https://www.leadersinsecurity.org/projects/cima-lsec-european-cyber-security-industry-market-analysis.html – 15 VII 2019.

Rys. 1. Cele Strategii bezpieczeństwa cybernetycznego UE: otwarta, bezpieczna i chroniona cyberprzestrzeń (2013)



Źródło: European Commission, *Commission Staff working document. Assessment of the EU 2013 Cybersecurity Strategy*, 2017, s. 5, [on-line:] https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF – 13 VII 2019.

Rys. 2. Wartość globalnego rynku cyberbezpieczeństwa (mld, euro)



Źródło: European Commission, *Commission Staff working document. Impact Assessment accompanying the document Proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")*, 2017, [on-line:] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017SC0500&from=EN – 15 VII 2019.

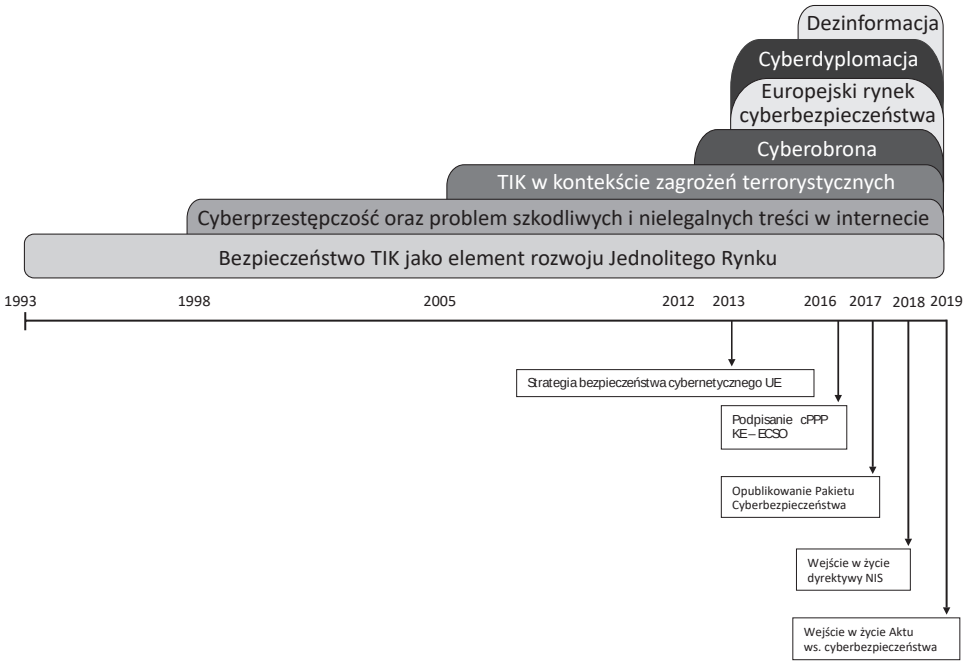
W 2016 roku KE w komunikacie *Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego* wskazała na potrzebę stworzenia jednolitego europejskiego rynku produktów i usług dla cyberbezpieczeństwa, który poprzez swoją innowacyjność oraz zaawansowanie technologiczne będzie konkurencyjny globalnie[28]. Głównymi przeszkodami na drodze do osiągnięcia tak nakreślonego celu są:

1. odmienne ramy certyfikacyjne w różnych krajach członkowskich;
2. wysoka zależność rynku od zamówień publicznych – szczególnie z sektora obronnego (co skutkuje często wykluczaniem lub nierównym traktowaniem produktów i usług z innych krajów);

[28] Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego*, 2016, [on-line:] https://ec.europa.eu/transparency/regdoc/rep/1/2016/PL/1-2016-410-PL-F1-1.PDF – 18 VII 2019.

3. problemy z komercjalizacją technologii oraz skalowaniem sprzedaży;
4. brak kadr oraz rozproszenie wiedzy i kompetencji na rynku.

Rys. 3. Rozszerzanie oraz pogłębianie zakresu działań UE w odniesieniu do cyberbezpieczeństwa w latach 1993-2019



Opracowanie własne.

W celu wspierania rozwoju europejskich technologii, a także ich komercjalizacji, Komisja Europejska jeszcze w ramach perspektywy finansowej 2007-2013 alokowała 334 milionów euro na projekty badawczo-rozwojowe w obszarze cyberbezpieczeństwa. W latach 2014-2016 w ramach projektu Horyzont 2020 przeznaczono kolejne 160 milionów na ten cel[29]. Ważnym krokiem w tym zakresie było podpisane w roku 2016 partnerstwo publiczno-prywatne w dziedzinie bezpieczeństwa cyfrowego pomiędzy KE i Europejską Organizacją Cyberbezpieczeństwa (ang. European Cyber Security Organization, ECSO)[30]. Do roku 2020 ma ono umożliwić do 1,8 miliarda

[29] European Commission, *EU cybersecurity initiatives – working towards a more secure online environment*, 2017, [on-line:] http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf – 18 VII 2019.

[30] European Commission, *Press release: Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats*, 2016, [on-line:] http://europa.eu/rapid/press-release_IP-16-2321_en.htm – 18 VII 2019.

euro inwestycji, z czego 450 milionów pokryje strona publiczna, w tym wypadku budżet Unii Europejskiej, resztę zaś branża. Warto podkreślić także, że wydatki na rozwój oraz wdrożenie europejskich technologii z zakresu cyberbezpieczeństwa mają zostać znacząco powiększone w kolejnych latach. Zgodnie z propozycją ram finansowych EU na lata 2021-2026 w programie Cyfrowa Europa alokowano 2 miliardy euro na inwestycje w sektorze bezpieczeństwa TIK[31].

Rys. 4. Współpraca UE w zakresie cyberdyplomacji

Źródło: [on-line:] https://eucyberdirect.eu.

Piąty obszar wskazany w ramach strategii stanowiło budowanie pozycji oraz relacji międzynarodowych UE w kontekście cyberbezpieczeństwa. W *Globalnej Strategii UE* z roku 2016 wskazano, że „Unia Europejska będzie aktywnym cybergraczem, chroniącym zarówno swoje kluczowe zasoby, jak i wartości w cyberprzestrzeni"[32]. W celu operacjonalizacji tych założeń w 2017 roku RUE zatwierdziła „Ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne", będące tzw. zestawem narzędzi dla cyberdyplomacji[33]. Wskazano w nich, że ofensywne działania w cyberprze-

[31] European Commission, *EU budget: Commission proposes €9.2 billion investment in first ever digital programme*, 2018, [on-line:] http://europa.eu/rapid/press-release_IP-18-4043_en.htm – 20 VII 2019. Szersze omówienie polityk publicznych UE wspierających przemysł cyberbezpieczeństwa zob. P. Timmers, *The European Union's cybersecurity industrial policy*, "Journal of Cyber Policy" 2018, Vol. 3, No. 3, s. 363-384.

[32] European External Action Service, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy*, 2016, s. 42, [on-line:] http://www.eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf – 18 VII 2019.

[33] Rada Unii Europejskiej, *Projekt konkluzji Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej")*, 2017, [on-line:] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/pl/pdf – 19 VII 2019.

strzeni mogą być traktowane przez UE za niezgodne z prawem międzynarodowym, a co za tym idzie, żadne państwo nie powinno prowadzić, wspierać ani świadomie dopuszczać do podejmowania takich bezprawnych działań ze swojego terytorium. Równolegle Unia prowadzi bezpośredni dialog dotyczący kwestii cyberbezpieczeństwa z sześcioma strategicznymi partnerami: Brazylią, Chinami, Indiami, Japonią, Koreą Południową oraz Stanami Zjednoczonymi.

Podsumowanie

Opisana w ramach niniejszego artykułu dynamika rozwoju polityk Unii Europejskiej względem problemów cyberbezpieczeństwa pokazała, iż w latach 1993-2016 nastąpiło zarówno poszerzanie zakresu merytorycznego podejmowanych inicjatyw, jak i pogłębienie poszczególnych wątków współpracy w ramach UE. Pogłębienie to przyjęło formę powoływania dedykowanych instytucji czy zespołów, nowych narzędzi współpracy, ale też harmonizacji poszczególnych wymagań regulacyjnych na poziomie wspólnotowym. Warto w tym kontekście zwrócić uwagę na fakt, że ze względu na dynamicznie zmieniające się środowisko zagrożeń cyfrowych w wielu krajach członkowskich nie rozwijano odpowiednich regulacji czy polityk publicznych wobec określonych problemów cyberbezpieczeństwa, i dopiero akty unijne stanowiły kluczową stymulację w tym zakresie. Koronny przykład stanowić może dyrektywa NIS, która w procesie implementacji jej do prawa krajowego niejako wymusiła na wielu państwach, w tym na Polsce, podjęcie szerszego namysłu oraz wdrożenie systemu cyberbezpieczeństwa na poziomie kraju.

Przytoczone w artykule zakresy merytoryczne adresowane przez Unię Europejską w kontekście bezpieczeństwa cyfrowego, takie jak wymiar gospodarczy, karny czy antyterrorystyczny, następnie także obronny, konkurencyjny (przemysł ICT) i dyplomatyczny, wpisują się w zakres wielu polityk wspólnotowych, nie dając się zamknąć w obszarze prerogatyw wybranego Komisarza UE czy też jednej wybranej Rady UE. Co ważne, w ramach swoich działań Komisja oraz Parlament Europejski przyjęły nie tylko rolę retroaktywnego reagowania na dynamikę globalnej debaty dotyczącej bezpieczeństwa i nowych technologii. Chęć aktywnego kształtowania regionalnego, ale też globalnego procesu regulacyjnego w zakresie bezpieczeństwa ICT, widać m.in. w ramach takich dokumentów jak dyrektywa NIS czy Ogólne rozporządzenie o ochronie danych. Zadanie adresowania najbardziej aktualnych problemów związanych z cyberbezpieczeństwem potwierdzone zostało także w ramach wniosków roboczej oceny Strategii bezpieczeństwa cybernetycznego UE dokonanej przez samą

KE w 2017 roku[34]. Jak wskazano w dokumencie, pięć pierwotnych celów jest tak samo aktualnych w roku 2017 jak cztery lata wcześniej, a efektywność ich realizacji przez UE należy określić jedynie jako „częściową". Zwrócono jednocześnie uwagę na fakt, że Strategia nie adresuje nowych zagrożeń i wyzwań, które pojawiły się po roku 2013 i aktualnie zyskują na znaczeniu. Są nimi m.in. bezpieczeństwo Internetu rzeczy, stan sektorów gospodarki nieobjętych dyrektywą NIS, ewolucja modeli biznesowych cyberprzestępców czy podział odpowiedzialności w zakresie bezpieczeństwa cyfrowego pomiędzy użytkownikiem a producentem/dostarczycielem produktu lub usługi[35].

Bibliografia

Council of the European Union, *Horizontal Working Group on Cyber Issues – Establishment and adoption of its Terms of Reference*, 20.10.2016, [on-line:] http://data.consilium.europa.eu/doc/document/ST-13114-2016-INIT/en/pdf.

Dz. Urz. UE C 419/145 z 16.12.2015 r., [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52012IP0457&from=PL.

Dz. Urz. UE L 218/8 z 14.08.2013 r., [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32013L0040&from=PL.

Dz. Urz. UE L 69/67 z 16.03.2005 r., [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32005F0222&from=EN.

European Commission, *Growth, competitiveness, employment. The challenges and ways forward into the 21st century*, COM (93) 700 final, Brussels, 05.12.1993, s. 24.

European Commission, *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, 2001, s. 7, [on-line:] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0890&from=CS.

European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – Network and Information Security: Proposal for A European Policy Approach / * COM/2001/0298 final */*, 2001, [on-line:] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52001DC0298&from=EN.

European Commission, *Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security*

[34] European Commission, *Cybersecurity package 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'*, 2017, [on-line:] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu – 22 VII 2019.

[35] European Commission, *Commission staff working document assessment of the EU 2013 Cybersecurity Strategy*, 2017, s. 57, [on-line:] https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF – 22 VII 2019.

Agency (Text with EEA relevance), 2004, [on-line:] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.

European Commission, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013*, [on-line:] https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

European Commission, *EU cybersecurity initiatives – working towards a more secure online environment*, 2017, [on-line:] http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.

European Commission, Press release: *Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats*, 2016, [on-line:] http://europa.eu/rapid/press-release_IP-16-2321_en.htm.

European Commission, *EU budget: Commission proposes €9.2 billion investment in first ever digital programme*, 2018, [on-line:] http://europa.eu/rapid/press-release_IP-18-4043_en.htm.

European Commission, *Cybersecurity package 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'*, 2017, [on-line:] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu.

European Commission, *Commission staff working document assessment of the EU 2013 Cybersecurity Strategy*, 2017, s. 57, [on-line:] https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF.

European Council, *Internal security strategy for the European Union. Towards a European security model*, 2010, [on-line:] https://www.consilium.europa.eu/media/30753/qc3010313enc.pdf.

European Council, *Tampere European Council 15 and 16 October 1999. Presidency Conclusions*, [on-line:] http://www.europarl.europa.eu/summits/tam_en.htm#c.

European Defence Agency, *Cyber Defence*, [on-line:] https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence.

European External Action Service, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy*, 2016, [on-line:] http://www.eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

European Parliament, *Resolution on 'Europe and the global information society – Recommendations to the European Council' and on a communication from the Commission of the European Communities: 'Europe's way to the information society: an action plan' (COM(94)0347 – C4-0093/94)*, 1996, [on-line:] https://publications.europa.eu/en/publication-detail/-/publication/93dee954-b8b9-495e-af03-e678161b06ab.

European Union Agency for Network and Information Security, *ENISA Strategy 2016 – 2020*, [on-line:] https://www.enisa.europa.eu/publications/corporate/enisa-strategy.

Europol, European Cybercrime Centre – EC3, [on-line:] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Komisja Europejska, *Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – „Dialog, partnerstwo i przejmowanie inicjatywy" {SEC(2006) 656} /* COM/2006/0251 końcowy */*, 2006, [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52006DC0251&from=EN.

Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ochrony krytycznej infrastruktury informatycznej – „Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności" {SEC(2009) 399} {SEC(2009) 400} /* COM/2009/0149 końcowy */*, 2009, [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52009DC0149&from=EN.

Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu*, Dz. Urz. UE C 115/1 z 04.05.2010 r., [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:52010XG0504(01).

Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Europejska agenda cyfrowa*, 2010, [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52010DC0245&from=en.

Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego i Rady: Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji – zapewnienie skutecznego wdrożenia dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*, 2017, [on-line:] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52017DC0476&from=EN.

Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego*, 2016, [on-line:] https://ec.europa.eu/transparency/regdoc/rep/1/2016/PL/1-2016-410-PL-F1-1.PDF.

LSEC, *CIMA – LSEC European Cyber Security Industry Market Analysis*, 2017, [on-line:] https://www.leadersinsecurity.org/projects/cima-lsec-european-cyber-security-industry-market-analysis.html.

NATO, *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*, 08.07.2016, [on-line:] www.nato.int/cps/en/natohq/official_texts_133163.htm?selectedLocale=en.

Rada Unii Europejskiej, *Projekt konkluzji Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej")*, 2017, [on-line:] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/pl/pdf.

Rada Unii Europejskiej, *Ramy polityki UE w zakresie cyberobrony*, 18 listopada 2014, [on-line:] http://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/pl/pdf.

Szczygieł M., *Polityka cyberbezpieczeństwa Unii Europejskiej – początek drogi do strategicznej autonomii*, „Sprawy Międzynarodowe" 2018, nr 2, s. 161-188, https://doi.org/10.35757/sm.2018.71.2.09.

Timmers P., *The European Union's cybersecurity industrial policy*, "Journal of Cyber Policy" 2018, Vol. 3, No. 3, s. 363-384, https://doi.org/10.1080/23738871.2018.1562560.