Teka of Political Science and International Relations – OL PAN/UMCS, 2018, 13/2, 49–63

DOI: 10.17951/teka.2018.13.2.49-63

KIERUNKI DZIAŁAŃ INSTYTUCJI EUROPEJSKICH NA RZECZ PODNOSZENIA POZIOMU BEZPIECZEŃSTWA PODMIOTÓW PAŃSTWOWYCH I NIEPAŃSTWOWYCH W CYBERPRZESTRZENI – WYBRANE PRZYKŁADY

Jolanta Cichosz

Wydział Prawa, Administracji i Zarządzania
Uniwersytet Jana Kochanowskiego w Kielcach
ORCID ID: https://orcid.org/0000-0003-0853-742
e-mail: jcichoszr1@op.pl

Streszczenie: Artykuł analizuje stan europejskiego bezpieczeństwa cybernetycznego na wybranych przykładach. W obliczu rosnących wyzwań w zakresie bezpieczeństwa cybernetycznego w Unii Europejskiej (legislacyjnych, instytucjonalnych, badawczych, przemysłowych) konieczne jest zweryfikowanie modeli zapewniających bezpieczeństwo cybernetyczne. Ponadto weryfikacja ta powinna dotyczyć spójności strategii jednolitego rynku cyfrowego, realizacji dużych projektów i przydzielania obowiązków zainteresowanym przedstawicielom. Jednocześnie zmiany powinny dotyczyć doskonalenia spójności przepisów prawnych i uaktualnienia definicji związanych z zagrożeniami cybernetycznymi. Priorytetowe działania w dziedzinie bezpieczeństwa cybernetycznego powinny obejmować: zwiększenie wymaganych zdolności i gotowości do reagowania na zagrożenia cybernetyczne, wzmocnienie współpracy i koordynacji między państwami członkowskimi Unii Europejskiej, a także między instytucjami, agencjami, władzami oraz przemysłem.

Słowa kluczowe: cyberbezpieczeństwo, europejskie cyberbezpieczeństwo, wyzwania, cyberzagrożenia

WPROWADZENIE

W pierwszych dwóch dekadach XXI wieku nastąpił szybki rozwój nowych technologii teleinformatycznych, powodując powstanie licznych zmiennych zależnych od siebie, które wpływają na funkcjonowanie państw. Państwa współuczestniczą w zmieniającym się cyfrowym środowisku i są odpowiedzialne za ochronę swojej cyberprzestrzeni. Identyfikacja potencjalnych zagrożeń bezpieczeństwa państw w cyberprzestrzeni jest często niejednoznaczna. Zagrożenia bezpieczeństwa w cyberprzestrzeni mogą wynikać z nasilających się cyberataków

[European… 2017d: 40] na infrastrukturę państw oraz ich obywateli, nielegalnej i szkodliwej ekonomicznie działalności, nieprzychylnych akcji propagandowych, pogorszających wizerunek państwa na płaszczyźnie międzynarodowej [Szubrycht 2006: 141]. Atakującymi mogą być zarówno grupy przestępcze, działające z chęci zysku, pobudek terrorystycznych, jak i grupy, za którymi mogą stać reprezentanci obcych państw. Działania takie służą pozyskaniu informacji, destabilizacji gospodarczej lub politycznej albo też wywołaniu niezadowolenia społecznego [Krajowe… 2017: 20–30]. Asymetria potencjałów pomiędzy licznymi podmiotami w cyberprzestrzeni powoduje, iż wyzwania i zagrożenia mają rzeczywisty wpływ na bezpieczeństwo globalne.

Wobec powyższego celem artykułu jest dokonanie analizy i oceny kształtującego się paradygmatu zapewniania cyberbezpieczeństwa przez Unię Europejską w obliczu nowych wyzwań. Treści artykułu są rezultatem rozwiązywania następującego problemu badawczego: Jak zapewnić cyberbezpieczeństwo Unii Europejskiej w kontekście nowych wyzwań? Autor dokonał analizy danych w zakresie wyzwań cyberbezpieczeństwa, które są istotne dla bezpieczeństwa Unii Europejskiej. Na podstawie analizy literatury i legislacji przedstawił istotne wnioski w odniesieniu do przygotowania potencjału europejskiego cyberbezpieczeństwa. Do zweryfikowania problemu badawczego zastosowano metody: analizy, porównania, normatywna i segmentacji.

CYBERBEZPIECZEŃSTWO UE W OBLICZU WYZWAŃ

Trudności w utrzymaniu globalnego bezpieczeństwa wobec licznie pojawiających się wyzwań i zagrożeń w cyberprzestrzeni przedstawiają raporty z branży bezpieczeństwa (np.: Europol, Gartner, Ipacso, Visiongain). Według raportu Europolu z 2017 r., aż 85% użytkowników Internetu odczuwało obawy przed zagrożeniem w cyberprzestrzeni [EU, 2017: 12–30].

Biorąc pod uwagę rozważania dotyczące zdefiniowania cyberbezpieczeństwa, zasadne jest odwołanie się do definicji ustanowionej przez Parlament Europejski oraz Międzynarodowy Związek Telekomunikacyjny – ITU (*International Telecommunication Union*). Definicja cyberbezpieczeństwa przedstawiona przez Parlament Europejski obejmuje „wszystkie działania niezbędne do ochrony przed cyberzagrożeniami sieci i systemów informatycznych, ich użytkowników oraz osób, których te zagrożenia dotyczącą" [European… 2017d: 40]. Pojęcie cyberbezpieczeństwa dokładnie opisuje organizacja ITU, ustanowiona w celu standaryzowania oraz regulowania rynku telekomunikacyjnego i radiokomunikacyjnego, jako „zbiór narzędzi, polityk, koncepcji bezpieczeństwa, zabezpieczeń, wytycznych, metod zarządzania ryzykiem, działań, szkoleń, najlepszych praktyk, zapewnień i technologii, które mogą być wykorzystywane do ochrony cyberprzestrzeni i organizacji oraz zasobów użytkownika. Organizacja i zasoby użytkownika obejmują podłączone urządzenia komputerowe, personel, infrastruk-

turę, aplikacje, usługi, systemy telekomunikacyjne oraz całość przekazanych i/lub przechowywanych informacji w środowisku cybernetycznym. Cyberbezpieczeństwo dąży do zapewnienia osiągnięcia i utrzymania właściwości bezpieczeństwa organizacji i zasobów użytkownika względem odpowiednich zagrożeń bezpieczeństwa w środowisku cybernetycznym" [EOS 2015: 2–3].

Brak jednolitości definicyjnej cyberbezpieczeństwa w wymiarze globalnym może umożliwiać podmiotom nieuprawnionym do korzystania z zasobów cyfrowych tworzenie i stosowanie nowych form wykorzystania cyberprzestrzeni (co jest niezgodnie z zasadami funkcjonowania państw demokratycznych). W niniejszym artykule zasadne jest zatem odwoływanie się do definicji, jaką precyzuje ITU.

W roku 2013 stworzono podwaliny dla europejskiego cyberbezpieczeństwa. Parlament Europejski i Rada Unii Europejskiej zatwierdziły Dyrektywę NIS dotyczącą wspólnego poziomu bezpieczeństwa sieci i systemów informacyjnych [Dyrektywa… 2013: 13–23]. Stanowi ona podstawę legislacyjną dotyczącą kształtowania polityki w cyberprzestrzeni na szczeblu UE i państw członkowskich wchodzących w jej skład, pomimo że nie jest ona bezpośrednio związana ze Wspólną Polityką Bezpieczeństwa i Obrony wyżej wymienionych państw. Rok 2016 był ważny dla europejskiej cyberprzestrzeni z racji przyjęcia wspólnej deklaracji UE–NATO [The EU–NATO 2016: 1–2], która głównie dotyczyła kluczowej roli cyberbezpieczeństwa.

Obecnie w Unii Europejskiej obserwuje się zwiększenie ilości instytucji oraz organizacji zaangażowanych w kwestie polityki cyberbezpieczeństwa. Wśród nich należy wymienić: Komisję Europejską, Parlament Europejski, Radę Unii Europejskiej, ENISA (Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji), EC3/Europol, Europejską Agencję Obrony, CERT-UE, External Action Service, EIT ICT Labs, europejskie organizacje normalizacyjne. Powyższe instytucje europejskie przyjęły wiele kluczowych inicjatyw politycznych dotyczących cyberbezpieczeństwa, w tym: Europejską politykę przemysłową w zakresie bezpieczeństwa (2012 r.), Strategię cyberbezpieczeństwa Unii Europejskiej (2013 r.), Rozporządzenie w sprawie elektronicznej identyfikacji i usług zaufania – eIDAS (2014 r.), poprawioną Dyrektywę w sprawie usług płatniczych – PSD2 (2015 r.), Unijny pakiet ochrony danych (2016 r.), Strategię jednolitego rynku cyfrowego (2017 r.) [EOS 2015: 3–4]. W obliczu nasilających się cyberzagrożeń w europejskiej cyberprzestrzeni przewodniczący Komisji Europejskiej Jean-Claude Juncker ogłosił w 2017 r. wzmocnienie działań Europejskiej Agencji ds. Bezpieczeństwa Cybernetycznego w zakresie obrony Europy przed cyberzagrożeniami [European… 2017f: 1–2].

Zgodnie z Dyrektywą NIS, zarządzanie bezpieczeństwem cybernetycznym powierzono: władzom państw członkowskich UE, Zespołom ds. bezpieczeństwa komputerowego i reagowania na incydenty sieci CSIRT, „Grupie Współpracy", „centrom kontaktowym". Wzmocnienie koordynacji w zakresie cyberbezpieczeństwa wyznaczono jednostkom CSIRT oraz ENISA. Pomagają one państwom członkowskim UE w podnoszeniu świadomości cyberzagrożeń i rozwiązywaniu

problemów związanych z cyberbezpieczeństwem [European… 2017d: 8, 14]. Ponadto w UE istnieją instytucje i organy [CERT UE, COMMISSION DGs, EDA, EUROPOL (EC3)] zajmujące się cyberbezpieczeństwem, które mają własne uprawnienia i obowiązki. Wyżej wymienione, mając na uwadze zapewnienie społeczeństwu bezpieczeństwa, przygotowują oferty i usługi w zakresie obrony przed cyberzagrożeniami. Nadmiar podmiotów może prowadzić do luk w spójności przekazywanych informacji, kompatybilności standardów i metodologii, a także doprowadzić do powstania „ryzyka utraty perspektywy ekonomicznej Unii Europejskiej". W związku z powyższym zasadne byłoby opracowanie przez ENISA projektu współpracy ze wszystkimi zainteresowanymi stronami na poziomie UE [ENISA 2017: 17], włączając do działania Centra Bezpieczeństwa i Analiz Informacji, ISAC (*The Information Security and Analysis Centres*) oraz „Grupy Współpracy" [Achieving… 2017: 105].

Dotychczasowe działania agencji ENISA w zakresie cyberbezpieczeństwa UE przynoszą pozytywne efekty w ramach wsparcia ochrony infrastruktury krytycznej, inicjowania współpracy między sektorem publicznym a prywatnym oraz w obszarze sektora prywatnego w ustanowieniu sektorowych ośrodków wymiany i analizy informacji, dzięki którym udostępniane są najlepsze praktyki w zakresie narzędzi, procedur oraz regulacji [European… 2017e: 15]. Należy dodać, że ENISA aktywnie uczestniczy również w badaniach naukowych oraz kampaniach edukacyjnych, skierowanych do użytkowników końcowych, mających na celu propagowanie bezpieczniejszych zachowań użytkowników w Internecie, np. na temat ataków phishingowych (wyłudzeń informacji), botnetów, oszustw finansowych i bankowych). Ze względu na złożoność działań, dotyczących cyberprzestrzeni oraz potencjał agencji ENISA, jest ona predysponowana do zajmowania się transgranicznymi cyberincydentami na dużą skalę oraz cyberkryzysami. W tym celu ENISA powinna rozwijać i utrzymywać unijny „portal informacyjny", stanowiący punkt kompleksowej obsługi, zapewniający społeczeństwu informacje w zakresie cyberzagrożeń pochodzących od unijnych i krajowych instytucji, agencji i organów, wśród których są: CSIRT i CERT-UE, Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu, Europejska Agencja Obrony (EDA), Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi (eu-LISA), Europejska Agencja Bezpieczeństwa Lotniczego (EASA), a także pozostałe agencje UE zaangażowane w kwestie cyberbezpieczeństwa [European… 2017d: 7–8].

W orędziu wygłoszonym przez przewodniczącego Komisji Europejskiej Jeana-Claude'a Junckera 13 września 2017 r. istotny punkt dotyczył przemian polityczno-gospodarczych Europy. Zdaniem J.-C. Junckera: „Europa ma nas chronić, wzmacniać i bronić. Trzeba dokończyć tworzenie różnych obszarów, w tym jednolitego rynku cyfrowego. O przyszłości Europy nie może decydować rozporządzenie. Musi być to wynik demokratycznej debaty, ostatecznie, szerokiego konsensusu". Stosownie do tej wypowiedzi są wypracowywane zmiany legislacyjne. Pierwsze z nich weszły w życie 25 maja 2018 r. w zakresie unijne-

go modelu ochrony danych osobowych w cyberprzestrzeni [*Polska*… 2017: 6]. Należy podkreślić, że od wielu lat w Polsce toczy się debata dotycząca kierunków rozwoju, strategii i polityki w zakresie cyberbezpieczeństwa oraz cyfrowych technologii przyszłości [Cybersec 2018].

KIERUNKI DZIAŁAŃ W ZAKRESIE CYBERBEZPIECZEŃSTWA UNIJNYCH PODMIOTÓW

Bezpieczeństwo narodowe i obrona państw należących do wspólnoty Unii Europejskiej zależy od dojrzałości narodowych strategii cyberbezpieczeństwa i gotowości do dzielenia się informacjami na temat zagrożeń. Problem ten dostrzegają również liderzy europejskiego przemysłu (Airbus Group, Atos, BBVA, BMW, Cybernetica, Deutsche Telekom, Ericsson, FSecure, Infineon i Thales). Wskazali oni, że dla stworzenia jednolitego rynku cyberbezpieczeństwa najważniejsza jest współpraca między państwami członkowskimi UE w zakresie Zespołów Reagowania w Sytuacjach Kryzysowych CERT oraz powołanie w przedsiębiorstwach osób odpowiedzialnych za politykę cyberbezpieczeństwa. Jednocześnie uznali także potrzebę powołania nowej instytucji – Centrum Cybernetycznego, które zintegruje krajowe i europejskie CERT-y oraz umożliwi przegląd informacji w czasie rzeczywistym. Ponadto liderzy europejskiego przemysłu dostrzegają konieczność zdefiniowania kryteriów cyberbezpieczeństwa na poziomie europejskim, przez zaangażowanych przedstawicieli z sektora przemysłu (dla produktów, rozwiązań, usług, procesów współpracy oraz wymagań w zakresie wykorzystania poufnych informacji). Według nich organem definiującym europejskie kryteria cyberbezpieczeństwa powinna być agencja ENISA, lecz zatwierdzenie tych kryteriów należałoby do wszystkich zainteresowanych przedstawicieli przemysłu UE [European… 2015: 13].

W roku 2016 przeprowadzone badania w zakresie wykorzystania Internetu w przedsiębiorstwach we wszystkich państwach członkowskich UE wykazały, że około 92% firm ma dostęp do zasobów online. Jednocześnie 77% z nich posiada własną stronę internetową [Eurostat… 2016]. W związku z tak znaczącą zmianą, dotyczącą wykorzystania zasobów internetowych przez firmy, podmioty te stoją w obliczu wyzwań w zakresie zapewnienia cyberbezpieczeństwa. Kluczowe znaczenie dla wyżej wymienionych działań ma realizacja polityki bezpieczeństwa ICT na poziomie państwa (państwowych i niepaństwowych podmiotów). W celu zweryfikowania poziomu wdrożenia polityki ICT przez podmioty Unii Europejskiej przeanalizowano dane z bazy Komisji Europejskiej [Eurostat… 2015]. Wyniki pozwoliły ustalić, że w 2015 r. europejskie podmioty, zatrudniające powyżej 10 pracowników tylko w 32% (wartość uśredniona) realizowały politykę bezpieczeństwa ICT. Inaczej przedstawiają się dane procentowe dotyczące: polityki uwzględniającej ryzyko ujawnienia poufnych danych w formie ataku typu: *pharming*, *phishing* – 22%; polityki uwzględniającej ryzyko niedostępności

usług ICT z powodu ataku *Denial of Service* – 26%; polityki uwzględniającej ryzyko zniszczenia, uszkodzenia, ujawnienia poufnych danych i niedostępności usługi ICT z powodu ataku lub innego wypadku – 32%. Jednocześnie na podstawie szczegółowej analizy danych Eurostatu ustalono, że największą troskę o cyberbezpieczeństwo wykazały państwa, takie jak: Portugalia (44%), Irlandia (40%), Szwecja (39%), Chorwacja (38%), Malta (38%), Słowacja (38%), Włochy (37%), Cypr (37%). Natomiast najmniejsze przygotowanie do wdrożeń polityki ICT prezentowały podmioty z następujących państw: Węgier (9%), Polski (12%), Estonii (15%), Łotwy (15%), Bułgarii (17%), Grecji (21%) [European… 2015]. Powyższe wyniki obrazują, że europejskie podmioty wymagają wsparcia i zdyscyplinowania w postaci wdrożeń polityki bezpieczeństwa ICT. Niski poziom realizacji polityki bezpieczeństwa ICT stwarza ryzyko zniszczenia, uszkodzenia czy ujawnienia danych. Taka sytuacja znacznie wpływa na obniżenie cyberbezpieczeństwa w wymiarze narodowym i międzynarodowym.

Problematyka cyberbezpieczeństwa podmiotów w różnych sektorach państw unijnych jest związana z poziomem integracji technologicznej, który determinuje zakres działań państwa, jednocześnie stanowi wyzwanie dla zapewnienia optymalnego poziomu bezpieczeństwa. Integracja sieci informatycznych jest jednym z ważniejszych priorytetów bezpieczeństwa dla gospodarki państwa, stanowi podstawę gotowości włączenia się w europejską sieć, ocenianą indeksem NRI (*Networked Readiness Index*), ustanowioną przez Radę Europy z uwzględnieniem 53 indywidualnych wskaźników [*Integration*… 2017: 2]. Według raportu Komisji Europejskiej *EDPR 2017 Integration of Digital Technology Source*, poziom spójności technologicznej w unijnych sektorach jest dość zróżnicowany. Najwyższy poziom spójności technologicznej ustalono w sektorze *e-commerce/Business* w następujących państwach: Danii, Irlandii, Szwecji, Belgii, Finlandii. Natomiast najniższą spójność technologiczną prezentowały: Rumunia, Bułgaria, Polska, Łotwa [*Digital*… 2016: 3]. Obecnie w Unii Europejskiej brakuje ogólnounijnych standardów i systemów certyfikacji cyberbezpieczeństwa, ponadto zwiększa się brak zaufania do zagranicznych rozwiązań w zakresie bezpieczeństwa w cyberprzestrzeni [European… 2016a: 6–7]. Każde państwo członkowskie UE określa własne wymagania w postaci certyfikatów i standardów, które firmy muszą przestrzegać, aby udostępniać swoje produkty na rynku [European… 2015: 10–11]. Europejskie organizacje normalizacyjne EON określają normy regionalne zgodnie z rozporządzeniami, m.in. UE nr 1025/2012 [ENISA 2016: 6]. W efekcie zarówno publiczne, jak i prywatne podmioty kupują produkty dostosowane do krajowych norm lub certyfikatów, przyczyniając się do tworzenia odizolowanych rynków cyberbezpieczeństwa w Unii Europejskiej [European… 2016b: 4]. Należy dodać, że międzynarodowe standardy cyberbezpieczeństwa (w zakresie oprogramowania, sprzętu, usług) są ustalane przez 152 podmioty na forum światowym [ENISA… 2016: 6].

Standaryzacja wymogów bezpieczeństwa w cyberprzestrzeni jest „procesem rynkowym", wymaga stałego doskonalenia [European Parliament… 2016b: 10]. Tworzenie unijnej standaryzacji cyberbezpieczeństwa wspiera artykuł 19 Dy-

rektywy NIS (2013/40/UE). Promuje on organy, które „zachęcają do korzystania z europejskich i międzynarodowych norm i specyfikacji", co z dużym prawdopodobieństwem odnosi się do norm określanych przez powołane organy publiczne. Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1025/ 2012 oraz Dyrektywą NIS, za konieczne uznano opracowanie wspólnych norm przy udziale kilku wybranych podmiotów: CEN, CENELEC, ETSI, ISO/IEC i ITU, z wyłączeniem wszystkich prywatnych forów [European Parliament… 2016: 10]. Takie rozwiązanie, według ENISA, nie jest wystarczające dla zapewnienia cyberbezpieczeństwa przy szybko ewoluujących rozwiązaniach technologicznych. Według ENISA, unijna branża cyberbezpieczeństwa powinna uwzględniać standardy przyjęte na poziomie międzynarodowym, w tym powszechnie uznawane, określone również przez prywatne instytucje lub fora [ENISA… 2016: 7]. Dzięki takim działaniom Unia Europejska będzie wychodzić naprzeciw zwiększeniu przejrzystości w zakresie zapewnienia cyberbezpieczeństwa produktów i usług ICT oraz wzmocnienia zaufania do rynku cyfrowego.

Przedsiębiorcy uznani za europejskich liderów w branży cyberbezpieczeństwa dostrzegają potrzebę stworzenia równych szans dla rozwoju tego przemysłu na poziomie globalnym. Wskazują oni, że w światowych zespołach, zajmujących się standaryzacją, powinni uczestniczyć europejscy przedsiębiorcy oraz start-upy, aby promować europejskie rozwiązania i uzyskać odpowiednie miejsce na światowym rynku. Według nich do najlepiej rozwiniętych technologii w UE należą: „e-calls" (e-komunikacja), „car to car communications" (e-łączność między samochodami). W związku z powyższym europejscy przedsiębiorcy proponują ustanowienie systemu delegatów europejskich firm w celu promowania i uznania europejskich certyfikatów za globalne w komitetach normalizacyjnych. Tym samym „certyfikacyjne problemy przemysłu europejskiego" zostaną przeniesione na ekspertów i częściowo odciążą odpowiedzialne za nie podmioty UE [European Cybersecurity… 2016: 12].

UDZIAŁ PODMIOTÓW W EUROPEJSKIM OBSZARZE CYBERBEZPIECZEŃSTWA

Współczesny europejski rynek cyberbezpieczeństwa składa się z tysięcy małych i średnich firm, zatrudniających poniżej 50 pracowników, z obrotem poniżej 5 milionów euro. Jego wartość w 2015 r. była szacowana na 17 mld euro i wzrasta corocznie o około 6% [ECSO 2016a: 5]. Spośród wielu unijnych przedsiębiorstw tylko 336 firm zajmuje się zaawansowanymi technologiami cyberbezpieczeństwa [EOS 2015: 2]. Jednocześnie dostrzega się brak wiodących firm, których zadaniem byłoby zapewnienie bezpieczeństwa i rozwiązywanie problemów w cyberprzestrzeni na poziomie UE. Rozdrobnienie europejskiego przemysłu zapewniającego cyberbezpieczeństwo jest obecnie jedną z głównych przeszkód w rozwoju silnej branży cybernetycznej UE. Według Komisji Europejskiej unijni dostawcy ITC

są w większości ograniczeni do rynków krajowych lub regionalnych. Realizują głównie zamówienia dla organów państwa, w szczególności z sektora obrony [European… 2015: 11]. Koncentrują się oni na współpracy z kilkoma publicznymi podmiotami, co często jest podyktowane optymalizacją działań lub zasobów firmy. W rezultacie zamówienia publiczne mogą być istotną siłą napędową dla rozwoju branży cyberbezpieczeństwa, a jednocześnie mogą przyczyniać się do ograniczenia zdolności tych przedsiębiorstw do wejścia na nowe rynki zbytu.

W celu ustalenia kondycji unijnego przemysłu cybernetycznego prowadzono badania dotyczące określenia poziomu efektywności cyberbezpieczeństwa w odniesieniu do wniesionych wysiłków w tym zakresie. Według jednostki badawczej SANS, możliwości zapewnienia bezpieczeństwa w cyberprzestrzeni przedsiębiorstw kształtowały się w 2015 r. na poziomie poniżej 44,5%. Specyfikację zabezpieczeń cybernetycznych przedstawiono poniżej:

- zapewnienie uwierzytelnienia i dostępu – 45,5%,
- zabezpieczenie punktów końcowych sieci – 43,8%,
- zaawansowana ochrona przed złośliwym oprogramowaniem typu IPS (*Intrusion Prevention System*)/UTM (*Unified Threat Management*) – 42,1%,
- zarządzanie dziennikami „logowania" w kontekście incydentów – 38,0%,
- posługiwanie się narzędziami do reagowania na incydenty – 36,4%,
- śledzenie ruchu sieciowego (monitorowanie, deszyfratory itp.) – 35,5%,
- zarządzanie podatnością (lukami) w systemach, aplikacjach – 31,4%,
- ochrona danych przed wyciekami informacji typu DLP (*Data Leak/Loss Protection/Prevention*) oraz szyfrowanie – 33,1%,
- zabezpieczenie typu: MDM (*Mobile Device Management*)/NAC (*National Digital Archives*), obejmujące identyfikowanie problemów z analizą danych, tworzeniem reguł i procesów korygujących – 33,1%,
- zarządzanie urządzeniami zabezpieczającymi – 28,9%,
- zarządzanie informacją związaną z bezpieczeństwem i zdarzeniami w ramach platform SIEM (*Security Information and Event Management*) – 26,4%,
- zabezpieczenie przed botnetami typu DDoS – 26,4%,
- uzyskanie efektywności usług wywiadowczych w zakresie cyberzagrożeń – 24,0%,
- zabezpieczenia lub monitorowanie urządzeń podłączonych do Internetu – IoT (*Internet of Things*) – 19,0% [Filkins 2016: 14].

Powyższe wyniki uzyskano na drodze badań przeprowadzonych w 169 firmach, o różnej wielkości na świecie (50% stanowiły firmy amerykańskie). Wyniki badań wskazują, że skuteczność zabezpieczeń cybernetycznych firm wymaga zaangażowania i nowych inicjatyw. Świadczy o tym dotychczasowa efektywność zapewnienia cyberbezpieczeństwa w zakresie 30–40% we wcześniej wymienionych obszarach, np. zapewnienie uwierzytelniania i dostępu, ochrona przed złośliwym oprogramowaniem, reagowanie na incydenty, zarządzanie podatnościami oraz zabezpieczenie bezprzewodowe. Odporność na cyberzagrożenia firm jest

mniejsza niż 30%. Należą do nich m.in.: zarządzanie urządzeniami zabezpieczającymi, zabezpieczenie przed botnetami, stosowanie usług wywiadowczych w obszarze cyberzagrożeń. Największe wyzwania napotykają przedsiębiorstwa w zakresie możliwości zapewnienia cyberbezpieczeństwa urządzeń IoT – podłączonych do Internetu. Oszacowano je na poziomie 19%.

Unijne Dyrektywy [Dyrektywa… 2016] określają wiele nadrzędnych zasad i zobowiązań, pozostawiając jednak państwom członkowskim odpowiedzialność za dostosowanie środków zgodnie z ich narodową strategią bezpieczeństwa [Wavestone 2017: 2]. Każde państwo członkowskie w Unii Europejskiej definiuje własne narodowe bezpieczeństwo w cyberprzestrzeni. Wobec powyższego pojawiają się różnice w polityce dotyczącej cyberbezpieczeństwa w poszczególnych państwach unijnych: „niektóre z nich koncentrują się bardziej na wspieraniu wzrostu gospodarczego i dobrobytu przedsiębiorstw, zaś inne kładą nacisk na zwalczanie cyberprzestępczości i budowanie silniejszych programów cyberobrony" [Trimintzios 2017: 23]. Powstałe różnice w polityce cyberbezpieczeństwa 28 państw UE umożliwiają dostawcom usług cyfrowych spoza UE, np. OTT (*Over The Top Players*), wybór najkorzystniejszej legislacji państwa członkowskiego, np. Irlandii. Może to powodować utrudnienia dla konkurencyjności pozostałych państw członkowskich UE [European… 2015: 6, 7].

Zależność podmiotów należących do UE od dostawców nowych zaawansowanych technologii spoza Unii powoduje zagrożenia dla bezpieczeństwa szeroko rozumianej cyberprzestrzeni. I tak, wiele dotychczasowych usług, w tym ochrona kluczowych zasobów i infrastruktury krytycznej, opiera się głównie na technologiach opracowanych przez przedsiębiorstwa spoza UE, np. Microsoft, IBM, CISCO, Symantec. Należy dodać, że główni europejscy nabywcy rozwiązań dotyczących cyberbezpieczeństwa (administracja publiczna, menedżerowie infrastruktury krytycznej i dostawcy usług internetowych), opierają się głównie na znanych i globalnych markach. Małe i średnie innowacyjne firmy z UE nie są atrakcyjne dla wyżej wymienionych nabywców nowych technologii (co może wynikać prawdopodobnie z troski o zapewnienie kompatybilności sprzętowej i programowej). W rezultacie wzrasta zależność państw UE od dostawców spoza obszaru Wspólnoty. Z kolei światowe marki cyberbezpieczeństwa nienależące do Unii Europejskiej wykorzystują swoją pozycję rynkową oraz budżet w celu stworzenia wyzwań utrudniających wejście nowym, mniejszym podmiotom gospodarczym. Działania wyżej wymienionych dostawców nie zawsze są zgodne z europejskimi standardami. Ich interesy mogą się znacznie różnić od założeń i planów przedsiębiorstw UE [European… 2016a: 7–8].

Obecnie w dokumentach dotyczących rozwoju europejskiego przemysłu, np. w komunikacie Komisji Europejskiej *For a European Industrial Renaissance* z 2014 r., brakuje wytycznych odnoszących się do cyberbezpieczeństwa [European… 2014: 1–26]. Istotnym wyzwaniem dla rozwoju infrastruktury krytycznej jest brak tworzenia dedykowanego oprogramowania dla inteligentnych systemów pomiarowych, np.: ICS, SCADA. Należy dodać, że współcześnie produkowane

podzespoły ICS są w większości oparte na standardowych rozwiązaniach – „systemach wbudowanych". Pochodzą one z ogólnej sieci sprzedaży, ze względu na mniejsze koszty i łatwość obsługi. Mając na uwadze, że przemysł boryka się z licznymi cyberzagrożeniami sieci energetycznych oraz rurociągów, powinny być podjęte modyfikacje programistyczne aplikacji przemysłowych w celu zwiększenia odporności cyberbernetycznej [European… 2016a, 3]. Wobec powyższego, ujednolicenie unijnego prawa w zakresie kwestii cybernetycznych jest konieczne w wielu obszarach, m.in.: infrastruktury krytycznej, nawigacji, autonomicznych napędów, „komunikacji między samochodami", mobilnych usług urządzeń medycznych, telematics (zaawansowanej technologii telekomunikacyjnej, nawigacji satelitarnej) [European… 2014: 11–12].

Unia Europejska stoi przed wyzwaniem stworzenia jednolitego, „godnego zaufania" rynku cyfrowego. Państwa członkowskie Unii Europejskiej, zgodnie z narodowymi strategiami bezpieczeństwa cybernetycznego, wspierają działania służące rozwojowi narodowej branży cyberbezpieczeństwa. Obecnie Komisja Europejska oraz Europejska Organizacja ds. Bezpieczeństwa Cybernetycznego – ECSO (*The European Cyber Security Organisation*), koordynują współpracę w zakresie partnerstwa publiczno-prywatnego. Budżet na realizację unijnych programów w okresie 2017–2020 wyniesie 450 mln euro. Programy te są kluczowe dla rozwoju obszarów cyberbezpieczeństwa w UE. Wśród znaczących programów należy wymienić: R&I (H2020), RIA, Pilots & Demonstrators, CEF Digital (*Connecting Europe Facility*), ESIF (*European Structural and Investment Funds*), EFSI (*European Fund for Strategic Investments*), ISF (*Internal Security Fund*) [ECSO 2016: 114].

W ostatnich latach zaobserwowano pozytywne zmiany w tempie prac badawczych. Bieżące sukcesy wynikają: z zapewnienia dofinansowania dla programów badawczo-rozwojowych ze środków publicznych, udziału podmiotów „działań oddolnych" oraz konsultacji ze stronami zainteresowanymi tematem w zakresie dostosowywania wyników badań do potrzeb rynku [European… 2016a: 9]. Jednak szybkie wytwarzanie innowacyjnych produktów i usług związanych z cyberbezpieczeństwem, poczynając od etapu laboratoryjnego do przekazania na rynek, jest wyzwaniem dla UE, ponieważ rynek cybernetyczny ulega szybkim zmianom (często okazuje się, że wyniki badań nie są już aktualne) [ECSO 2016: 50].

Według Europejskiej Organizacji Bezpieczeństwa Cybernetycznego – ESCO, która z ramienia Komisji Europejskiej zajmuje się realizacją umów partnerstwa publiczno-prywatnego w zakresie cyberbezpieczeństwa (cPPP), istnieje potrzeba dalszych istotnych zmian. Dotyczą one zapewnienia większych funduszy na przedsięwzięcia (nie tylko na początkowym etapie, jak dotychczas), konieczności tworzenia oprogramowania dedykowanego odbiorcom oczekującym wysokiego poziomu bezpieczeństwa i prywatności (a nie wieloplatformowego, np. w ramach programu Horyzont 2020) [ECSO 2016a: 17]. Z kolei według analizy unijnej jednostki badawczej *Scientific Foresight Unit STOA* ustanowionej przy Parlamencie Europejskim, państwa UE mają obawy, czy zwiększenie finansów na rzecz sektora

prywatnego zobliguje prywatnych partnerów do wywiązania się z przygotowania produktów i usług dotyczących cyberbezpieczeństwa [Achieving 2017: 101].

Trudności w sektorze cyberbezpieczeństwa wynikają również z braku wykwalifikowanych specjalistów. Według Centrum Bezpieczeństwa Cybernetycznego i Edukacji UE w 2016 r., odnotowano niedobór 350 000 specjalistów cyberbezpieczeństwa na unijnym rynku. W 2022 r. przewiduje się wzrost braku kadry w branży cybernetycznej na poziomie 1,8 miliona pracowników na świecie [Frost 2017: 8]. Komisja Europejska poza kwestią braku personelu dostrzega również problematykę utraty europejskiego *know-how* wynikającego z zatrudnienia unijnych specjalistów poza rynkiem UE [European… 2016a: 8]. W komunikacie zatytułowanym *Wzmocnienie europejskiego systemu cyberbezpieczeństwa* Komisja Europejska wyjaśnia, że ograniczone perspektywy rozwoju firm zajmujących się bezpieczeństwem cybernetycznym wynikają ze sprzedaży europejskich inwestycji, czego skutkiem są liczne fuzje. Trend ten świadczy o zdolności innowacyjnej europejskich przedsiębiorców, jest również zagrożeniem dla europejskiego *know-how* oraz zdobytej wiedzy fachowej [European… 2016c: 9]. W związku z powyższym, jeśli nie zostaną podjęte działania zaradcze, niedobór specjalistów w zakresie cyberbezpieczeństwa może się powiększyć.

KONKLUZJE

Transgraniczny charakter cyberzagrożeń sprawia, że trudno jest stawić im czoła na poziomie państwa. Kompetencje w zakresie cyberbezpieczeństwa nadal pozostają w gestii każdego państwa członkowskiego UE [Carrapico, Barrinha 2017: 1267]. Każde państwo definiuje własną strategię bezpieczeństwa cybernetycznego zgodnie z priorytetami narodowymi. W celu stworzenia silnej branży cyberbezpieczeństwa w Unii Europejskiej należy dążyć do zacieśnienia współpracy publiczno-prywatnej, która zintegruje nie tylko administrację i sektor prywatny, ale także różne podmioty z branży energetycznej, banków, telekomunikacji [Achieving 2017: 101].

Wobec narastających wyzwań w zakresie cyberbezpieczeństwa w Unii Europejskiej (prawnych i instytucjonalnych, badań, przemysłu) niezbędny jest kompleksowy zestaw środków opartych na działaniach unijnych, które będą sprzyjały osiąganiu wzajemnie wspierających się celów. Kluczowym wyzwaniem dla UE jest sprecyzowanie zakresu obowiązków dotyczących zaangażowanych instytucji i podmiotów gospodarczych (przy obowiązujących różnych ramach prawnych państw UE dotyczących cyberbezpieczeństwa). Biorąc pod uwagę złożoność problemu i różnorodność uczestniczących podmiotów (państwowych i niepaństwowych), scentralizowany nadzór europejski nie jest właściwym rozwiązaniem. Rządy krajowe są najlepiej przygotowane do zapobiegania i reagowania na incydenty i ataki cybernetyczne. Dotyczy to współpracy sektora państwowego z prywatnym oraz indywidualnymi użytkownikami w sieci w ramach ustalonych

strategii politycznych i ram prawnych. Skuteczna reakcja państw wymaga często zaangażowania się ich na szczeblu krajowym oraz unijnym. Do priorytetowych działań w tym zakresie należy wymienić: zwiększenie potencjału i gotowości do reagowania na zagrożenia, zacieśnienie współpracy i koordynacji wśród państw unijnych (dotyczy instytucji, agencji i organów), ujednolicenie przepisów prawnych oraz definicji odnoszących się do terminologii związanej z cyberzagrożeniami [European… 2013: 5–6].

Unia Europejska powinna weryfikować system zapewniający bezpieczeństwo cybernetyczne, strategię jednolitego rynku cyfrowego, realizację dużych projektów angażujących wszystkie zainteresowane tą tematyką podmioty w Europie. Działania w zakresie zapewnienia cyberbezpieczeństwa powinny obejmować trzy kluczowe obszary, tj.: zestawy norm (np. Dyrektywę NIS), współpracę instytucji (organy ścigania) oraz zadania dotyczące obronności. Wyżej wymienione funkcjonują w różnych ramach prawnych. Spójna unijna polityka przemysłowa powinna być ukierunkowana na następujące wyzwania: ICT – technologie informacji i komunikacji, DSM – projektowanie i tworzenie systemów, wspieranie konkurencyjności europejskich rozwiązań informatycznych w kluczowych obszarach cyberbezpieczeństwa i cybertechnologii. Wśród nich należy wymienić aplikacje typu: *IoT* (urządzenia komunikujące się z sieciami – internet), *Big Data* (olbrzymie zbiory cyfrowych danych), chmurę obliczeniową (dane wirtualizowane w określonej lokalizacji, zapisane na dyskach serwerów), *Mobile and Cyber Physical Systems* (mobilne i stałe systemy cyfrowe), przemysł 4.0 (bezprzewodowe przesyłanie danych z sensorów przemysłowych ICS do internetu), „inteligentne sieci". Powyższe działania umożliwią zwiększenie europejskiego potencjału cybernetycznego, który jest obecnie ulokowany w następujących branżach: energetycznej, transportowej – motoryzacyjnej, lotniczej, handlu detalicznym oraz telekomunikacji. Dotyczy to również dóbr konsumpcyjnych. Wskazane jest również podniesienie zakresu wiedzy obywateli na temat cyberbezpieczeństwa oraz poszerzenie informacji o bezpieczeństwie produktów i usług ICT.

Title: European Cybersecurity – Challenges. Selected Examples

Summary: The article analyzes the state of European cybersecurity on selected examples. In the face of the increasing cybersecurity challenges in the European Union (legislative, institutional, research, industry), it is necessary to verify the models that ensure cybersecurity. In addition, this verification should concern the coherence of the digital single market strategy, the implementation of large projects and the allocation of duties to the interested representatives. At the same time, the changes should include the coherence of legal provisions and definitions relating to cyberthreats. Priority actions in the field of cybersecurity should include: the increasing of the required capabilities and readiness to respond to cyberthreats, the strengthening cooperation and coordination between Member States of the European Union as well as between the institutions, the agencies, the authorities and the industry.

Keywords: cybersecurity, European cybersecurity, challenges, cyberthreats

BIBLIOGRAFIA

1. *Achieving a sovereign and trustworthy ICT industry in the EU*. (2017), European Parliament.
2. Carrapico H., Barrinha A. (2017), *The EU as a Coherent (Cyber) Security Actor?*, "Journal of Common Market Studies" 10.05.2017, http://onlinelibrary.wiley.com/doi/10.1111/jcms.12575/abstract [dostęp: 15.03.2018]. DOI: https://doi.org/10.1111/jcms.12575.
3. CEN, CENELEC. (2016), *CEN and CENELEC response to the European Commission Public*
4. *Consultation on the contractual public-private partnership and possible accompanying measures*, 01.03.2016, https://www.cencenelec.eu/news/policy_opinions/PolicyOpinions/ReplyPPPcybersecurity.pdf [dostęp: 15.03.2018].
5. *Cybersec.* (2018), https://cybersecforum.eu/pl/ [dostęp: 15.03.2018].
6. *Digital Technology Source*. (2016), 28.09.2016, https://ec.europa.eu/digital-single-market/en/european-digital-progress-report [dostęp: 15.03.2018].
7. Dyrektywa. (2016), Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r., w sprawie środków na rzecz wysokiego poziomu bezpieczeństwa sieci systemów informatycznych na terytorium Unii (Dz.U. UE, PL 19.7.2016, L. 194/1).
8. Dyrektywa. (2013), Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienia wspólnego poziomu bezpieczeństwa sieci w obrębie Unii, COM(2013) 49 final, 2013/0027 (COD), Bruksela, 07.02.2013.
9. ECSO. (2016a), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership. European Cyber Security Organisation*, 01.06.2016, http://ecs-org.eu/documents/ecs-cpppindustry-proposal.pdf [dostęp: 15.03.2018].
10. ECSO. (2016b), *European Cybersecurity Strategic Research and Innovation Agenda (SRIA) for a contractual Public-Private Partnership (cPPP)*, 01.06.2016, http://www.ecs-org.eu/documents/ecs-cpppsria.pdf [dostęp: 15.03.2018].
11. EOS. (2015), *Cybersecurity for a trusted EU single digital market – Market Study for a Cybersecurity Flagship Programme*, 01.12.2015, http://be-wiser.eu/admin/resources/eos-study-on-a-eu-cybersecurity-flagship-extend-summ-dec2015.pdf [dostęp: 15.03.2018].
12. ENISA. (2015), *Definition of Cybersecurity. Gaps and overlaps in standardisation* (No. v1.0), 01.12.2015, https://www.enisa.europa.eu/publications/definition-of-cybersecurity/at_download/fullReport [dostęp: 15.03.2018].
13. ENISA. (2016), *Gaps in NIS standardisation. Recommendations for improving NIS in EU standardisation policy*, 01.11.2016, https://www.enisa.europa.eu/publications/gaps-eustandardisation/at_download/fullReport [dostęp: 15.03.2018].
14. ENISA. (2017), *Principles and opportunities for a renewed EU cyber security strategy. ENISA's contribution to the Strategic review*, 01.07.2017, https://www.enisa.europa.eu/publications/enisa-positionpapers-and-opinions/enisa-input-to-the-css-review-b [dostęp: 15.03.2018].
15. EU. (2017), T*errorism Situation and Trend Report 2017*, https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-201 [dostęp: 15.03.2018].
16. European Commission. (2013), Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.
17. European Commission. (2014), For a European Industrial Renaissance (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions No. COM(2014) 14 final.

18. European Commission. (2015), Eurostat, Security policy: risks addressed and staff awareness, http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cisce_ra&lang=en [dostęp: 15.03.2018].
19. European Commission. (2016a), Contractual Public Private Partnership on Cybersecurity. Accompanying Measures Accompanying the document Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research an innovation between the European Union, represented by the Commision, and the stakeholder organisation (Commission Staff Working Document No. SWD (2016) 216 final, Brussels.
20. European Commission. (2016b), ICT Standardisation Priorities for the Digital Single Market (Communication from the Commission to the European Parliament, the European Economic and Social Committee and the Committee of the Regions No. COM (2016) 176 final), Brussels.
21. European Commission. (2016c), Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions No. COM (2016) 410 final), Brussels.
22. European Commission. (2017d), *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") (No. COM(2017) 477 final)*, Brussels.
23. European Commission. (2017e), *Summary report on the public consultation on the evaluation and review of the European Union Agency for Network and Information Security (ENISA)*, Brussels, https://ec.europa.eu/digital-single-market/en/news/summary-report-publicconsultation-evaluation-and-review-european-union-agency-network-and [dostęp: 15.03.2018].
24. European Commission. (2017f), *Press release-President Jean-Claude Juncker's State of the Union Address 2017*, Brussels, http://europa.eu/rapid/pressrelease_SPEECH-17-3165_en.htm [dostęp: 15.03.2018].
25. European Cybersecurity Industry Leaders. (2016), Recommendations on Cybersecurity for Europe, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=13326 [dostęp: 15.03.2018].
26. European Parliament. (2014), *Mass Surveillance. Part 1 – Risks and opportunities raised by the current generation of network services and applications.* Scientific and Technology Options Assesment (STOA).
27. European Parliament and the Council. (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, Brussels.
28. *European Union*, 06.02.2017, https://www.wavestone.com/app/uploads/2017/02/cybersecuritynis-directive-europe-2.pdf [dostęp: 15.03.2018].
29. *Eurostat.* (2015), 31.12.2015, http://ec.europa.eu/eurostat/data/database [dostęp: 15.03.2018].
30. Filkins B., (2016), *It Security Spending Trends*, *A Sans surveys*, SANS Institute InfoSec Reading Room.
31. *Frost Sullivan. (ISC)2, Alta Associates, Booz Allen Hamilton.* (2017), *2017 Global Information Security Workforce Study. Benchmarking Workforce Capacity and Response to Cyber Risk. Center for Cyber Security and Education*, 2017, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS.pdf [dostęp: 15.03.2018].
32. *Integration of Digital Technology Europe's Digital Progress Report 2017*. (2017), 09.07.2017, https://ec.europa.eu/digital-single-market/en/european-digital-progress-report [dostęp: 15.03.2018].

33. *Integration of Digital Technology Europe's Digital Progress Report 2017*. (2017), https://ec.europa.eu/digital-single-market/en/european-digital-progress-report, 15.03.2018.
34. Kissel R. (2013), *NISTIR, 7298, Revision 2, Glossary of Key Information Security Terms., National Institute of Standards and Technology Interagency or Internal Report,* U.S. Department of Commerce, USA.
35. Komisja Europejska. (2017), *Polska debata wokół białej księgi w sprawie przyszłości Europy. Jakie scenariusze dla Unii Europejskiej?*, Brussels, 13.09.2017.
36. *Krajowe Ramy Polityki Cyberbezpieczeństwa GOV.pl*. (2017), https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/0bbc7a32-64df-b45e-b08c-dac59415f109 [dostęp: 15.03.2018].
37. Szubrycht T. (2006), *Analiza podobieństw operacji militarnych innych niż wojna oraz działań pozwalających zminimalizować zagrożenia asymetryczne*, „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 1 (164).
38. *The EU-NATO joint declaration*, 28.07.2017, http://www.css.ethz.ch/en/services/digital-library/articles/article.html/57da453c-b94e-44dd-b1c2-a35d12eed6e2/pdf [dostęp: 15.03.2018].
39. Trimintzios P., Chatzichristos G., Portesi S., Drogkaris P., Palkmets L., Liveri D., Dufkova A. (2017), *Cybersecurity in the EU Common Security and Defence Policy (CSDP), Challenges and risks for the EU, Brussels: European Parliament*, 01.05.2017, http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN. pdf [dostęp: 15.03.2018].
40. Wavestone. (2017), *Cybersecurity and the NIS Directive. A challenge of consistency for the European Union*, 06.02.2017, https://www.wavestone.com/app/uploads/2017/02/cybersecuritynis-directive-europe-2.pdf [dostęp: 15.03.2018].