DOI: https://doi.org/10.34862/rbm.2021.2.5

Agata Małecka
Akademia Wojsk Lądowych
agata.malecka@awl.edu.pl
https://orcid.org/0000-0002-5519-9681

Polityka cyberbezpieczeństwa Unii Europejskiej na początku trzeciej dekady XXI wieku

Abstrakt: Charakter polityki cyberbezpieczeństwa UE zmienił się pod wpływem ewolucji katalogu współczesnych zagrożeń. W związku z tym aktywność Unii Europejskiej w obszarze cyberbezpieczeństwa w ciągu ostatnich lat zaczęła wykraczać poza aspekty stricte gospodarcze i ekonomiczne, obejmując także sferę obronności. Instytucje unijne zaangażowały się w budowę bezpiecznej cyberprzestrzeni, zarówno na obszarze europejskim, jak i w ramach globalnej współpracy na rzecz cyberbezpieczeństwa. Przedmiotem badań niniejszego artykułu jest bieżąca polityka cyberbezpieczeństwa UE – jej wyznaczniki oraz charakter. Autor postawił sobie za cel wyjaśnienie przyczyn zaangażowania instytucji i organów unijnych w politykę cyberbezpieczeństwa w ciągu ostatnich pięciu lat: kompetencje Unii w dziedzinie cyberbezpieczeństwa, rozwój rynku cyfrowego i jego znaczenie dla unijnej gospodarki niskoemisyjnej oraz unijne aspiracje do rozszerzania ram wspólnej polityki bezpieczeństwa i obrony o aspekty cyberobrony. Drugim celem artykułu było nakreślenie kształtu polityki cyberbezpieczeństwa UE. Analizie poddane zostały możliwości kreowania przez UE cyberpolityki po wejściu w życie traktatu zmieniającego z Lizbony, priorytety UE w zakresie wzrostu gospodarczego w nawiązaniu do bezpiecznej cyberprzestrzeni, powiązanie aspektów cyberbezpieczeństwa z tzw. Europejskim Zielonym Ładem oraz problematyka cyberobrony w ramach wspólnej polityki bezpieczeństwa i obrony. Do realizacji w/w celów autor zastosował głównie metody jakościowe: analizę instytucjonalno-prawną, metodę śledzenia procesu oraz metodę decyzyjną

Słowa kluczowe: Unia Europejska, cyberbezpieczeństwo, cyberobrona, polityka cyberbezpieczeństwa.

European Union Cybersecurity Policy at the Beginning of the Third Decade of the 21st Century

Abstract: The nature of the EU's cybersecurity policy has been changed as a result of the evolution of the catalog of present-day threats. Hence, the European Union's activity in the cybersecurity area in recent years has begun to extend beyond strictly business and economic aspects to include the defense sphere as well. The EU institutions engaged in building safe cyberspace, both within

the European area and the global cooperation on cybersecurity. The subject matter of research is the current EU cyber security policy - its determinants and nature. The author aimed to explain the reasons for the engagement of EU institutions in cybersecurity policy during the last five years: the Union's authority in the cybersecurity domain, the development of the digital market and its impact on the Union's low-carbon economy, and the Union's aspirations to broaden the framework of the Common Security and Defence Policy by incorporating cyber defence aspect. The second goal of the article was to describe the shape of the EU cybersecurity policy. The study examined the EU's ability to create a cyber policy after the Lisbon Treaty, EU economic growth priorities in relation to safe cyberspace, the connection between cybersecurity aspects and the so-called European Green Deal, and cyber defence issues under the Common Security and Defence Policy. To achieve the above-mentioned aims, the author used mainly qualitative methods: legal analysis, process tracking method and decision-making method.

Keywords: European Union, cybersecurity, cyber defence, cybersecurity policy.

Wstęp

Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę z 16 grudnia 2020 r. (Komisja Europejska, 2020), zmieniona Dyrektywa o bezpieczeństwie sieci i systemów informatycznych (Dyrektywa 1148, 2016; Markopoulou i in., 2019), szereg przepisów dotyczących jednolitego rynku cyfrowego w UE (m.in.: zniesienie opłat roamingowych, ochrona danych, likwidacja nieuzasadnionej geoblokady, możliwość transgranicznego przemieszczania się treści internetowych), zaktualizowane przez Radę 19 listopada 2018 r. Ramy polityki UE w zakresie cyberobrony (Rada Unii Europejskiej, 2018), Akt o Cyberbezpieczeństwie (Rozporządzenie 881, 2019), Rozporządzenie Parlamentu Europejskiego i Rady (UE) z kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Rozporządzenie 679, 2016), przepisy umożliwiające Radzie przyjmowanie sankcji wobec podmiotów odpowiedzialnych za cyberataki (decyzja Rady w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim) (Decyzja Rady 797, 2019) – to kilka z najważniejszych regulacji ogólnounijnych w zakresie cyberbezpieczeństwa. Wszystkie zostały przyjęte przez unijne instytucje w ciągu ostatnich pięciu lat. Część z nich dotyczy kwestii gospodarczych, część reguluje problematykę wpisującą się w ramy wspólnej polityki bezpieczeństwa i obrony. Wszystkie dowodzą zaangażowania Unii Europejskiej w budowanie bezpiecznej i stabilnej cyberprzestrzeni, zarówno na terytorium samej Wspólnoty, jak i w ramach globalnej współpracy na rzecz cyberbezpieczeństwa. Wyjaśnienia wymagają

zatem dwie zasadnicze kwestie: powody, dla których Unia Europejska partycypuje w tworzeniu bezpiecznej cyberprzestrzeni oraz charakter tych działań.

Cel niniejszego opracowania jest dwojaki. W pierwszej kolejności autorka postawiła sobie za zadanie wyjaśnienie przyczyn głębszego zaangażowania się instytucji i organów unijnych w politykę cyberbezpieczeństwa w ciągu ostatnich pięciu lat, zarówno na poziomie europejskim, jak i globalnym. W tym kontekście przeanalizowano możliwości kreowania przez UE cyberpolityki po wejściu w życie traktatu zmieniającego z Lizbony, cele UE w zakresie wzrostu gospodarczego w nawiązaniu do bezpiecznej cyberprzestrzeni, powiązanie aspektów cyberbezpieczeństwa z tzw. Europejskim Zielonym Ładem oraz problematyka cyberobrony w ramach wspólnej polityki bezpieczeństwa i obrony. Drugim zamierzeniem autorki było nakreślenie kształtu polityki cyberbezpieczeństwa UE. W literaturze przedmiotu dominuje pogląd, że działania instytucji unijnych w zakresie cyberprzestrzeni mają przede wszystkich charakter cywilny. Owszem, pierwsze działania Unii w ramach prób regulacji cyberprzestrzeni były podejmowane w celach ochrony głównie przed cyberprzestępczością, co miało związek z realizacją planów i strategii gospodarczych. Nie jest jednak prawdą, że charakter działań UE w kwestiach cyberbezpieczeństwa pozostaje stricte cywilny. W ciągu ostatnich pięciu lat, licząc od momentu powstania niniejszego opracowania, instytucje unijne rozszerzyły zakres zainteresowania cyberprzestrzenią o aspekty cyberobrony, rozwijając tym samym ramy wspólnej polityki bezpieczeństwa i obrony, stając się kolejnym podmiotem na arenie międzynarodowej ustanawiającym standardy działań w cyberprzestrzeni dla realizacji celów militarnych.

Określone wyżej zamierzenia autorka zrealizowała dzięki zastosowaniu teorii neoinstytucjonalizmu, gdzie instytucje unijne traktowane są szeroko, zarówno w wymiarze formalnym, jak i proceduralnym, normatywnym, symbolicznym oraz poznawczym. Analiza neoinstytucjonalna przypisuje instytucjom rolę decyzyjną oraz wskazuje na ich znaczenie w procesie tworzenia struktur współpracy (Hall & Taylor, 2016). W kontekście badań nad polityką cyberbezpieczeństwa UE stosowne jest odwołanie się do jednego z nurtów neoinstytucjonalizmu – instytucjonalizmu racjonalnego wyboru. Podejście to zakłada, że każdy z aktorów w grze politycznej dąży do realizacji własnych interesów. Jednak działania, będące sumą indywidualnych celów, długofalowo nie przynoszą oczekiwanych rezultatów. Instytucje zaś są tymi podmiotami, które jednostkowe zamierzenia i plany łączą

w spójną i słyszalną na arenie międzynarodowej strategię (Wiśniewska-Grzelak i in., 2015).

Zasadniczą metodą badawczą, którą posłużyła się autorka w celu weryfikacji założenia dotyczącego cywilno-wojskowego charakteru działań UE regulujących cyberprzestrzeń, była analiza instytucjonalno-prawna (Reynolds & Johnson, 2011). W kontekście problematyki niniejszego artykułu, polegała ona na badaniu aktów normatywnych odnoszących się do cyberprzestrzeni i cyberbezpieczeństwa, których źródłem powstania były instytucje unijne.

Inną metodą jakościową, użytą dla określenia przyczyn angażowania się UE w szerokorozumianą politykę cyberbezpieczeństwa była metoda śledzenia procesu (Reynolds & Johnson, 2011). Ta metoda, często wykorzystywana w badaniach nad instytucjami unijnymi, zakłada analizę sposobu w jaki określona przyczyna wpływa na obserwowany rezultat. Dla problematyki opracowania istotne stało się zdefiniowanie motywów zaangażowania UE w politykę regulacji cyberprzestrzeni (w kontekście uprawnień i kompetencji instytucji UE, strategii rozwoju gospodarczego UE, dominującego w priorytetach Komisji Europejskiej dyskursu ochrony klimatu i środowiska oraz rozszerzania ram wspólnej polityki bezpieczeństwa i obrony), geneza procesu tworzenia przez UE bezpiecznej i funkcjonalnej cyberprzestrzeni oraz jego aktualny kształt.

Aby unaocznić wpływ decyzji podejmowanych przez Radę Europejską i Radę Unii Europejskiej (i w nieco mniejszym stopniu innych instytucji i organów UE) na bieżącą unijną politykę cyberbezpieczeństwa, autorka posłużyła się metodą decyzyjną (Reynolds & Johnson, 2011). Zastosowanie tej metody umożliwiło uchwycenie znaczenia poszczególnych ośrodków decyzyjnych dla ciągle zmieniającej się i aktualizowanej formy systemu regulującego cyberprzestrzeń w UE.

Możliwości Unii w kształtowaniu polityki cyberbezpieczeństwa

Zaangażowanie Unii Europejskiej w politykę regulacji cyberprzestrzeni jest bezsprzeczne. Wskazuje na to nie tylko analiza debaty, toczącej się w ramach współpracy między instytucjami i krajami członkowskimi oraz wewnętrznie – między samymi instytucjami UE, ale również badania nad unijnymi aktami prawa wtórnego. Dla realizacji celów niniejszego artykułu pytanie zasadnicze nie brzmi: czy Unia Europejska angażuje się w politykę cyberbezpieczeństwa?, ale: dlaczego Unia Europejska angażuje się w politykę cyberbezpieczeństwa? Według

autora istnieją trzy zasadnicze powody, dla których instytucje unijne działają w zakresie kształtowania środowiska cyberprzestrzeni. W pierwszej kolejności należy wskazać na kompetencje Unii w dziedzinie cyberbezpieczeństwa (i szerzej – bezpieczeństwa w ogóle, które zostały jej przekazane przez państwa członkowskie). Druga przyczyna zaangażowania UE w kreowanie europejskiego systemu cyberbezpieczeństwa tkwi w rozwijającym się rynku cyfrowym i jego znaczeniu dla unijnej gospodarki oraz w procesie transformacji europejskiej gospodarki w kierunku niskoemisyjnej, który nie odbędzie się bez udziału technologii cyfrowych. Za ostatni czynnik tworzenia przez Unię autonomicznej polityki cyberbezpieczeństwa należy uznać aspiracje do rozszerzania ram wspólnej polityki bezpieczeństwa i obrony o aspekty cyberobrony, w postaci reagowania na cyberataki, zarówno wymierzone w unijną infrastrukturę krytyczną, jak i te o charakterze państwowym, wykorzystujące na przykład dezinformację do podważania modelu liberalnej demokracji.

Jak zatem wygląda kwestia możliwości UE angażowania się w politykę cyberbezpieczeństwa, których ramy wyznaczone zostały wskutek nadania przez państwa członkowskie instytucjom unijnym określonych kompetencji? Dyskusja nad kreacyjną rolą Unii Europejskiej w zakresie cyberbezpieczeństwa powinna odbywać się w oparciu o rozróżnienie na dwa zasadnicze obszary działalności Wspólnoty – przestrzeń wolności, bezpieczeństwa i sprawiedliwości oraz wspólną politykę zagraniczną i bezpieczeństwa. Na tej podstawie można określić możliwości Unii w ramach tworzenia europejskiego systemu cyberbezpieczeństwa. Możliwości te są wynikiem posiadania przez instytucje unijne różnych, ściśle zdefiniowanych kompetencji, które mają źródło w prawie pierwotnym – w obowiązujących traktatach – Traktacie o Unii Europejskiej (2016) i Traktacie o Funkcjonowaniu Unii Europejskiej (2016). Próba zapewnienia bezpieczeństwa na terenie Unii Europejskiej odbywa się poprzez szereg mechanizmów w zakresie: kontroli granicznej, azylu i imigracji, współpracy sądowej w sprawach cywilnych, współpracy wymiarów sprawiedliwości w sprawach karnych oraz współpracy policyjnej. Inne mechanizmy przypisane są wspólnej polityce zagranicznej i bezpieczeństwa, gdzie przyjmowanie aktów prawodawczych jest wykluczone, a instytucje mają kompetencje do wydawania ogólnych wytycznych, przyjmowania decyzji (dotyczących działań i stanowisk, podejmowanych przez UE oraz zasad wykonywania tych decyzji) i umacniania współpracy między państwami członkowskimi. UE posiada zatem możliwości i mechanizmy wpływania

na kształt bezpieczeństwa europejskiego (w tym cyberbezpieczeństwa). Należy jednak pamiętać, że są to mechanizmy skonkretyzowane, oparte na takich aspektach jak: przyznane Unii przez państwa członkowskie kompetencje, interesy narodowe krajów członkowskich, funkcjonowanie innych sojuszy obronnych (przede wszystkim NATO) oraz potrzeba (lub jej brak) ujednolicenia polityki cyberbezpieczeństwa wewnątrz i na zewnątrz Unii Europejskiej.

Fundamentalną zasadą działania instytucji UE jest tworzenie prawa wtórnego w ramach jasno zdefiniowanych w traktatach kompetencji. Szczególnie Traktat o Funkcjonowaniu Unii Europejskiej stanowi podstawę prawną do funkcjonowania unijnej „machiny" prawnej. Przestrzeń wolności, bezpieczeństwa i sprawiedliwości regulowana jest w ramach tzw. kompetencji dzielonych (Kuś, 2014) między Unię a państwa członkowskie. Przy czym państwa członkowskie mogą regulować prawodawstwo w tym zakresie jedynie wówczas, gdy Unia nie skorzysta z prawa do realizowania własnej kompetencji lub zaprzestanie z niej korzystać. Oznacza to, że instytucje unijne mają pierwszeństwo w stanowieniu prawa dotyczącego przestrzeni wolności, bezpieczeństwa i sprawiedliwości (Skolimowska, 2015). Jednocześnie wszelkie kompetencje, które nie zostały przyznane UE w traktatach należą do państw członkowskich. Państwa członkowskie mogą także zmienić zakres kompetencji instytucji unijnych na konferencji międzyrządowej zgodnie ze zwykłą procedurą zmiany (Traktat o UE, 2016), która prowadzi do modyfikacji postanowień traktatowych. Kompetencje dzielone Unia realizuje przede wszystkim poprzez ustanawianie prawa wtórnego za pomocą zwykłej procedury prawodawczej (Janusz, 2011) oraz zgodnie z zasadą pomocniczości i proporcjonalności (Protokół nr 2, 2008), na straży której stoją państwa członkowskie. Stąd głównymi instytucjami, które mają wpływ na podejmowanie decyzji w zakresie przestrzeni wolności, bezpieczeństwa i sprawiedliwości są: Komisja Europejska (jako instytucja inicjująca proces prawodawczy) oraz Rada i Parlament (instytucje rozpatrujące, wprowadzające poprawki i zatwierdzające wniosek prawodawczy Komisji), a także szereg organów doradczych, które przekazują swoje opinie na temat wniosków Komisji, w zależności od obszarów problemowych.

Traktat zmieniający z Lizbony, który wszedł w życie w 2009 roku, znacznie poszerzył możliwości oddziaływania instytucji UE na „pozaunijną" przestrzeń bezpieczeństwa, w tym na politykę obronności. Państwa członkowskie nadały unijnym instytucjom określone kompetencje, które w kontekście polityki

zagranicznej i bezpieczeństwa, stanowią „wszelkie dziedziny polityki zagranicznej i ogół kwestii dotyczących bezpieczeństwa Unii, w tym stopniowe określanie wspólnej polityki obronnej" (Traktat o UE, 2016). W celu realizacji tych kompetencji powstał spójny system instytucjonalny, oparty na Radzie Europejskiej i Radzie. Rada Europejska określa strategiczne interesy UE oraz ogólne wytyczne w ramach polityki zagranicznej i bezpieczeństwa. Na ich podstawie niezbędne kroki (decyzje, jeśli sytuacja międzynarodowa wymaga działań operacyjnych Unii[1]) podejmuje Rada. Zarówno Rada Europejska, jak i Rada w ramach wspólnej polityki zagranicznej i bezpieczeństwa stanowią jednomyślnie (z wyjątkami przewidzianymi przez Traktaty[2])[3]. Poza Radą Europejską i Radą w politykę bezpieczeństwa i obronności zaangażowanych jest szereg innych instytucji i organów unijnych. Jest to m.in. wysoki przedstawiciel Unii do spraw zagranicznych i polityki bezpieczeństwa, który wraz z państwami członkowskimi odpowiada za realizację decyzji Rady, Parlament Europejski (Traktat o UE w artykule 36 nakazuje wysokiemu przedstawicielowi konsultowanie i informowanie Parlamentu o rozwoju i realizacji polityki bezpieczeństwa i obrony), czy też Komitet Polityczny i Bezpieczeństwa (ciało doradcze, opiniodawcze oraz kontrolne w zakresie kierownictwa strategicznego nad operacjami zarządzania kryzysowego).

W tych wyżej określonych ramach instytucjonalnych UE realizuje zamierzenia z zakresu cyberbezpieczeństwa. Można je wpisać zarówno w politykę bezpieczeństwa wewnętrznego UE (przestrzeń wolności, bezpieczeństwa i sprawiedliwości), jak zewnętrznego (wspólna polityka bezpieczeństwa i obrony). Przy czym unijne zaangażowanie w te dwa rodzaje polityk, chociaż zakłada inne

[1] Według artykułu 28 Traktatu o UE Rada podejmuje decyzje, określające zasięg, cele, zakres i środki, jakie mają być oddane do dyspozycji Unii, warunki wprowadzania w życie i czas trwania działań operacyjnych.

[2] Do takich wyjątków, w myśl art. 31, ust.1 Traktatu o UE, gdzie Rada decyduję większością kwalifikowaną, należą: podjęcie decyzji przez Radę Europejską dotyczącej strategicznych interesów i celów Unii, przyjęcie decyzji zgodnie z propozycją Wysokiego Przedstawiciela po przedłożeniu specjalnego wniosku Radzie Europejskiej, podjęcie decyzji wykonującej decyzję określającą działanie lub stanowisko Unii, mianowanie Specjalnego Przedstawiciela (posiadającego mandat w odniesieniu do poszczególnych spraw politycznych). Przy czym nie można zastosować głosowania w Radzie metodą większości kwalifikowanej w przypadku dziedzin: wojskowej i polityczno-obronnej.

[3] Traktaty (Traktat o UE, art. 31) wprowadzają jednocześnie możliwość wstrzymania się członka Rady od głosu. Wówczas, po złożeniu przez państwo członkowskie oficjalnego oświadczenia, decyzje Rady dotyczące wspólnej polityki zagranicznej i bezpieczeństwa nie są dla tego państwa wiążące, aczkolwiek jego ewentualne działania nie mogę stać w sprzeczności z działaniami UE podejmowanymi w ramach realizacji decyzji. Jednocześnie decyzja nie może zostać przyjęta w przypadku wstrzymania się od głosu 1/3 liczby państw członkowskich, których łączna liczba ludności stanowi 1/3 ludności UE.

działania, wynika z jednej przesłanki – zapewnienia bezpieczeństwa – oraz służy zasadniczemu celowi – rozwojowi gospodarczemu.

Cyberprzestrzeń jako platforma wzrostu gospodarczego i „zielonej" transformacji

Kształt współczesnej UE jest wynikiem procesów integracyjnych, inicjowanych przez państwa członkowskie celem wzrostu gospodarczego, bogacenia się, które można zmierzyć odpowiednimi wskaźnikami ekonomicznymi. Wszystkie główne cele kolejnych strategii rozwoju gospodarczego prowadziły do przekształcenia UE w jedną z największych gospodarek na świecie, z powodzeniem konkurujących z gospodarką amerykańską, czy chińską. Nie było to zadanie łatwe, gdyż przy określaniu celów strategicznych Unia brała pod uwagę nie tylko specyfikę ustrojową, społeczną i polityczną Europy jako kontynentu – kolebki demokracji, ale również wyzwania globalne. W ten sposób najpóźniej do 2020 roku UE planowała osiągnąć co najmniej 75% stopy zatrudnienia osób w wieku od 20 do 64 lat, przy jednoczesnym inwestowaniu w badania i rozwój (na poziomie 3% produktu krajowego brutto) oraz podejmowaniu działań w ramach ochrony klimatu (zmniejszenie o co najmniej 20% emisji gazów cieplarnianych, wzrost udziału energii odnawialnej do poziomu 20% i wzrost efektywności energetycznej o 20%) (Komisja Europejska, 2010).

Przewodnicząca Komisji Europejskiej zaprezentowała w 2019 roku program, który nie odbiegał od wcześniejszych scenariuszy, przewidywanych dla rozwoju gospodarczego UE. Zawarła w nim postulat osiągnięcia dobrobytu dzięki funkcjonowaniu modelu europejskiej społecznej gospodarki rynkowej, przy założeniu uzyskania stanu neutralności klimatycznej przez kontynent do 2050 roku oraz ochrony europejskich mechanizmów i systemów demokratycznych (von der Leyen, 2019). Sześć priorytetów działań Komisji Europejskiej na lata 2019-2024 wpisuje się w schemat rozwoju gospodarczego UE z uwzględnieniem przeszłości w postaci realizowania założeń liberalnej demokracji i państwa prawa oraz przyszłości, odpowiadając na globalne zmiany klimatyczne i konieczność uwzględnienia środowiska w strategiach rynkowych. W ramach każdego z sześciu priorytetów Komisji Europejskiej na lata 2019–2024 można przypisać działaniom w cyberprzestrzeni większą lub mniejszą rolę.

Wydarzenia w roku 2020 oraz w początku roku 2021, związane z gospodarczymi, społecznymi i politycznymi skutkami pandemii wirusa SARS-CoV-2 stały się

dodatkowym motorem napędowym działań Unii w zakresie przyspieszenia procesu transformacji cyfrowej, dla którego aspekty cyberbezpieczeństwa są kluczowe. Nie odbiegały one od wcześniejszych założeń rozwoju gospodarki cyfrowej, ugruntowały jednak przekonanie o potrzebie wdrażania nowoczesnych technologii w celu budowy potencjału cyfrowego UE. W marcu 2021 Rada (po wstępnym porozumieniu z Parlamentem Europejskim w grudniu 2020 r. (Rada Unii Europejskiej, 2020a) przyjęła unijny program „Cyfrowa Europa", z budżetem 7,588 mld EUR, obejmujący lata 2021–2027 z mocą wsteczną od 1 stycznia 2021 roku (Rada Unii Europejskiej, 2021). Wśród kluczowych dziedzin nowej strategii cyfrowej UE znalazły się:

1. suwerenność cyfrowa, rozumiana jako fundament autonomii strategicznej (jednolity rynek cyfrowy, autonomia w ustalania zasad regulujących ten rynek oraz unijne rozwiązania cyfrowe) (Komisja Europejska, 2021a);
2. usługi cyfrowe, gwarantujące bezpieczeństwo użytkowników oraz tworzące wolną i konkurencyjną przestrzeń do funkcjonowania przedsiębiorstw, działających w sektorze cyfrowym (projekt aktu o usługach cyfrowych oraz aktu o rynkach cyfrowych przedstawiony przez Komisję Europejską w grudniu 2020 r.) (Komisja Europejska, 2020b);
3. gospodarka oparta na danych (w tym przyjęcie rozwiązań prowadzących do ponownego wykorzystania danych), której budowa i rozwój stanowią fundamentalny cel w zaproponowanej przez Komisję Europejską w lutym 2020 r. strategii w zakresie danych cyfrowych (Komisja Europejska, 2020c);
4. sztuczna inteligencja i jej znaczenie w tworzeniu innowacji głównie w sektorach bezpieczeństwa, edukacji i opieki zdrowotnej (Rada Unii Europejskiej, 2020b);
5. technologie prorozwojowe w postaci chmury obliczeniowej, technologii kwantowych i obliczeń wielkiej skali;
6. konektywność, której wyrazem ma stać się powszechna łączność, umożliwiająca dostęp do usług cyfrowych (dzięki niezakłóconemu zasięgowi 5G dla obszarów miejskich i szlaków transportowych oraz korzystaniu przez wszystkie europejskie gospodarstwa domowe z łączności o minimalnej przepustowości co najmniej 100 Mb/s) (Rada Unii Europejskiej, 2020c);
7. europejska identyfikacja cyfrowa (e-ID) w postaci przede wszystkim interoperacyjności podpisów cyfrowych w celu umożliwiania obywatelom

UE korzystania z publicznych i prywatnych transgranicznych usług cyfrowych;
8. e-Zdrowie oraz transformacja cyfrowa w sektorze opieki zdrowotnej;
9. umiejętności cyfrowe i edukacja cyfrowa celem zarówno pozyskania wykwalifikowanych specjalistów cyfrowych, jak i podniesienia świadomości istnienia i ochrony przed cybrzagrożeniami;
10. cyfryzacja wymiaru sprawiedliwości, prowadząca do powszechnego używania na terenie UE takich narzędzi cyfrowych, jak: prowadzenie postępowań sądowych drogą cyfrową, stosowanie komunikacji elektronicznej między stronami, elektroniczne przesyłania dokumentów, wideoprzesłuchania i wideokonferencji (Rada Unii Europejskiej, 2020d);
11. cyberbezpieczeństwo, bez którego wszystkie wyżej wymienione aspekty nie będą w pełni funkcjonalne.

W programie „Cyfrowa Europa" cyberbezpieczeństwo odgrywa kluczową rolę. Powodem jest stale rosnąca skala cyberzagorżeń i bezsprzeczne uzależnienie wzrostu wskaźników gospodarczych od efektywności wykorzystania infrastruktury cyfrowej. Bezpieczna, otwarta i powszechna cyberprzestrzeń, która dla UE jest fundamentem rozwoju gospodarczego, nie może funkcjonować bez mechanizmów zwiększających zaufanie do cyfrowych technologii. Dla unijnych przywódców oznaczało to podjęcie niezbędnych działań do uzyskania unijnej strategicznej samodzielności w zakresie cyberbezpieczeństwa.

Charakter niezbędnych kroków, które powinna poczynić Unia, aby stać się wiodącym podmiotem w wyznaczaniu trendów w obszarze cyberbezpieczeństwa został określony w kilku obowiązujących aktualnie dokumentach, z czego najistotniejszymi wydają się być: Strategia bezpieczeństwa UE na lata 2020-2025 (*EU Security Union Strategy*) (Komisja Europejska, 2020d) z lipca 2020 r. oraz Strategia cyberbezpieczeństwa UE (*The EU's Cybersecurity Strategy for the Digital Decade*) z grudnia 2020 r. (Komisja Europejska, 2020a).

W Strategii bezpieczeństwa problematyka cyberbezpieczeństwa została wyróżniona w jednym z czterech obszarów strategicznych, w których planowane jest podejmowanie działań na szczeblu unijnym – *A future-proof security environment* (środowisko bezpieczeństwa, które wytrzyma próbę czasu). Jednym z głównych wyzwań określonych przez Komisję Europejską stało się zapewnienie bezpieczeństwa infrastruktury sieci 5G. Liczne, opublikowane w ciągu ostatnich trzech lat, dokumenty unijne (np. *Recommendation on the Cybersecurity of*

5G networks (Zalecenie Komisji 534, 2019), *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures – 5G Toolbox* (NIS Cooperation Group, 2020) wskazują na duże zainteresowanie UE problematyką rozwoju i ochrony sieci 5G, wynikające z próby znalezienia obszaru w dziedzinie nowoczesnych, cyfrowych technologii, w którym rozwiązania unijne byłyby wiodące (Robles-Carrillo, 2021). W ten sposób urzeczywistniłby się postulat strategicznej autonomii Unii w sferze cyberbezpieczeństwa. Innym obszarem zainteresowań Unii, znajdującym odbicie w Strategii bezpieczeństwa, jest certyfikacja cyberbezpieczeństwa tzw. *cybersecurity by design*. Zakłada ona projektowanie systemów oraz urządzeń dostosowanych do wymogów cyberbezpieczeństwa od samego początku – już na etapie wstępnej koncepcji. W nowym dokumencie strategicznym nie zabrakło odniesień do cyberobrony – powołanie wspólnej jednostki ds. cyberprzestrzeni (*Joint Cyber Unit*), koordynującej współpracę operacyjną, czy też rozwijanie współpracy międzynarodowej w celu zapobiegania cyberatakom (wypracowane przez Unię ramy unijnej reakcji dyplomatycznej na szkodliwe operacje cybernetyczne). Te działania dotyczą wspólnej polityki zagranicznej i bezpieczeństwa i wskazują na próbę współuczestniczenia Unii w wypracowaniu rozwiązań w obszarze cyberobronności. Jest to istotny element unijnej polityki cyberbezpieczeństwa, ponieważ wskazuje na rozwijanie (obok wektora cywilnego, traktowanego jako podstawa tejże polityki), elementu militarnego, ukierunkowanego na operacje cybernetyczne inicjowane bądź/i sponsorowane przez podmioty państwowe. Regulowanie aspektów cyberobronności było dotychczas przypisywane sojuszom o charakterze wojskowym, militarnym (głównie NATO). Od kilku lat UE zacieśnia współpracę w ramach wspólnej polityki bezpieczeństwa i obrony, kładąc nacisk na wzmocnienie obszaru obronności, w tym na poziomie cyber.

Głównym elementem tzw. pakietu cyberbezpieczeństwa, przedstawionego przez Komisję Europejską 16 grudnia 2020 r. była Strategia cyberbezpieczeństwa UE (*The EU's Cybersecurity Strategy for the Digital Decade*). Jest to dokument, który wyznacza kierunek polityki cyberbezpieczeństwa Unii na najbliższe lata i który dowodzi istnieniu unijnych aspiracji w ramach problematyki cyberbezpieczeństwa. Zaproponowane zestawy inicjatyw regulacyjnych, inwestycyjnych oraz politycznych w trzech obszarach wskazują zarówno na gospodarczo-finansowo-ekonomiczny wektor unijnych działań (Odporność, technologiczna suwerenność i przywództwo – *Resilience, Technological Sovereignty and Leadership*), jak i aktywność w ramach obronności (Budowanie

zdolności operacyjnych do zapobiegania, odstraszania i reagowania na incydenty w cyberprzestrzeni – *Building Operational Capacity to Prevent, Deter and Respond*) (Komisja Europejska, 2020a). W pierwszym obszarze Komisja zobowiązała się do działań prawnych, instytucjonalnych oraz inwestycyjnych, celem wykrywania i niwelowania skutków cyberprzestępczości, lepszej obsługi incydentów, wsparcia małych i średnich przedsiębiorstw w procesie podnoszenia kompetencji cyfrowych pracowników oraz finansowania badań naukowych. Katalog inicjatyw objął m.in.: przyjęcie Dyrektywy NIS 2 (Dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii), przyjęcie standardów regulujących bezpieczeństwo Internetu Rzeczy (IoT), przeznaczenie 4,5 mld EUR na inwestycje w obszarze cyberbezpieczeństwa (na lata 2021–2027), budowę Sieci Centrów Operacyjnych ds. Bezpieczeństwa, wsparcie małych i średnich przedsiębiorstw w poprawie konkurencyjności na rynku (poprzez wykorzystanie produktów i usług cyfrowych) dzięki ośrodkom takim, jak *Digital Innovation Hubs*, opracowanie unijnej usługi otwartego serwera DNS oraz pełne wdrożenie *Toolbox 5G* do połowy 2021 roku (Komisja Europejska, 2020a).

Drugi obszar wskazuje na unijne ambicje skierowane ku budowie zdolności obronnych, obejmujących działania zapobiegawcze, odstraszanie oraz zintegrowane reagowanie na cyberincydenty. W ramach działań z zakresu cyberobrony Unia zapowiedziała powołanie Wspólnej Jednostki Cyberbezpieczeństwa (*Joint Cyber Unit*), powierzając jej zadanie koordynowania współpracy między unijnymi a krajowymi organami i instytucjami odpowiedzialnymi za cyberbezpieczeństwo oraz wzmocnienie funkcjonowania tzw. *Diplomacy Toolbox* – unijnego zestawu narzędzi i metod cyberdyplomacji. Unijna cyberobrona zostałaby skierowana na zapobieganie i reagowanie oraz rozwijanie nowoczesnych zdolności odpowiedzi na cyberataki (w ramach prac Europejskiej Agencji Obrony i możliwości Europejskiego Funduszu Obrony). Do pozostałych inicjatyw z zakresu cyberobronności, zapisanych w unijnej cyberstrategii, należy zaliczyć m.in.: wzbogacenie europejskich ram zarządzania kryzysowego o dziedzinę cyberbezpieczeństwa, realizację programu walki z cyberprzestępczością, wzmocnienie Centrum Analiz Wywiadowczych UE poprzez zachęcenie państw członkowskich do wymiany danych i informacji, działania na rzecz wzmocnienia pozycji UE w celu efektywnej realizacji strategii zniechęcania, odstraszania i reagowania na cyberzagrożenia, przegląd ram unijnej polityki cyberbezpieczeństwa, stworzenie unijnej strategii wojskowej w ramach

cyberbezpieczeństwa, budowę powiązań między przemysłem cywilnym, obronnym i kosmicznym oraz umacnianie bezpieczeństwa infrastruktury krytycznej w przestrzeni kosmicznej (Komisja Europejska, 2020a).

Całości dopełnia, zapisana w unijnej cyberstrategii, w postaci trzeciego obszaru działań i inicjatyw, konieczność zacieśnienia współpracy międzynarodowej na rzecz otwartej i bezpiecznej cyberprzestrzeni w zakresie promowania wartości, na których Unia powstała. Stąd postulaty współpracy m.in. z ONZ, Radą Europy oraz podmiotami trzecimi, dotyczące stosowania podstawowych wolności i praw człowieka w sieci, czy też ochrona dzieci przed wykorzystywaniem seksualnym i niegodziwym traktowaniem w cyberprzestrzeni (Komisja Europejska, 2020a).

Dużej wagi, jaką Unia zaczęła przywiązywać do cyberbezpieczeństwa, dowodzi analiza kilku innych dokumentów o znaczeniu strategicznym, które zostały przyjęte w ciągu ostatnich lat – programu „Horyzont Europa" (Komisja Europejska, 2020e, 2021b), czy też Planu Odbudowy dla Europy (Komisja Europejska, 2021c). „Horyzont Europa" – unijny program finansowania badań i innowacji na lata 2021–2027, zastępujący wcześniejszy „Horyzont 2020" – zakłada przeznaczenie 49 mln EUR na badania nad innowacjami w systemach cyberbezpieczeństwa, tak aby zwiększyć ochronę przed zaawansowanymi cyberzagrożeniami. Przyjęcie przez unijnych przywódców w lipcu 2020 roku nadzwyczajnego instrumentu odbudowy *Next Generation EU* oraz wieloletnich ram finansowych oznaczało przeznaczenie łącznie ponad 1,8 mld EUR na zniwelowanie społeczno-gospodarczych skutków pandemii COVID-19, w tym cyberataków, których liczba i siła wzrosła w okresie tzw. „lockdawnów". Cel ten został połączony ze wcześniejszymi, „przedpandemicznymi" założeniami cyfrowej transformacji UE oraz realizacją założeń europejskiego zielonego ładu.

Unijne akty prawa wtórnego, tworzone w ramach przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz wspólnej polityki zagranicznej i bezpieczeństwa przesiąknięte są rozwiązaniami z dziedziny cyberbezpieczeństwa, czego przyczyn należy upatrywać w samym charakterze unijnych działań, zasadniczo służącym celom wzrostu gospodarczego. Technologie cyfrowe – ich produkcja i użycie są obecnie motorami rozwoju gospodarczego, stąd coraz wyraźniejsze i stanowcze stają się działania Unii w zakresie tworzenia sprzyjającego klimatu wokół procesu cyfryzacji, które zakładają m.in. zapewnienie cyberbezpieczeństwa. Cel ten znajduje uzasadnienie w danych i statystykach, jednoznacznie wskazujących na rosnącą skalę i koszty gospodarcze cyberzagrożeń.

Według prognoz firmy analitycznej Cybersecurity Ventures w 2021 roku straty finansowe, spowodowane cyberprzestępczością na świecie wzrosną dwukrotnie w okresie pięcioletnim (z 3 w 2015 roku do 6 bln dolarów) (Morgan, 2020). Wzrost w granicach 15% w ciągu kolejnych 5 lat oznacza straty finansowe rzędu 10,5 bln dolarów w 2025 roku, co przekracza wartość szkód wyrządzonych przez klęski żywiołowe rocznie oraz zyski osiągane z handlu wszystkimi nielegalnymi narkotykami na świecie (Morgan, 2019a). Cyfryzacja, która jest jednym z priorytetów UE na najbliższe lata, ma zatem swoje koszty, generowane przez uszkodzenie i zniszczenie danych, kradzież środków finansowych w sieci, zmniejszenie lub utratę produktywności, kradzież własności intelektualnej, kradzież danych osobowych i finansowych, oszustwa, przywracanie zhakowanych danych, okupy czy straty wizerunkowe. Zjawiska te będą przybierały na sile, biorąc pod uwagę szacunkowe dane, które mówią o 6 miliardach ludzi podłączonych do internetu w 2022 roku i 7,5 miliardach do końca 2030 roku (Morgan, 2019b) oraz o trzykrotnym wzroście liczby urządzeń podłączonych do sieci do 2030 roku (CISCO, 2020) Pandemia Covid-19 wzmocniła niepokojący trend rosnącej skali cyberprzestępstw – na terenie UE zanotowano liczne przypadki cyberataków na infrastrukturę do pracy zdalnej, nielegalnych domen, infekcji wirusami, fałszywych internetowych ofert sprzedaży maseczek, leków i antycovidowych terapii, dezinformacji i fake newsów, phishingu mailowego i smsowego, fałszywych aplikacji diagnostycznych, czy też cyberataków na organizacje ds. zdrowia (ENISA, 2020). Szczególnie narażone są wysokorozwinięte państwa UE, wyróżniające się swoją siłą gospodarczą i innowacyjną, np. Niemcy. Tamtejszy Federalny Urząd Policji Kryminalnej (BKA) zarejestrował w 2019 r. ponad 100 tysięcy cyberprzestępstw. W roku 2020 liczba ta wzrosła o ponad 8%. Skala incydentów niezgłoszonych i niezarejestrowanych jest prawdopodobnie wielokrotnie większa (Fürstenau, 2021). Z szacunków hiszpańskiej policji wynika, że w tym kraju w 2020 roku popełniono 260 tysięcy cyberprzestępstw. Największy wzrost zanotowały hiszpańskie placówki służby zdrowia (5-krotny wzrost liczby cyberataków) (Forsal.pl, 2021). Działania unijne w zakresie zwiększania cyberbezpieczeństwa są zatem zrozumiałe i konieczne, biorąc pod uwagę liczbę 756 poważnych cyberataków w 2020 roku, których część dotknęła administrację państwową (wzrost o 75% w porównaniu z rokiem 2019). Pod wpływem technologii cyfrowych zmienia się także oblicze przestępczości zorganizowanej w UE, która wykorzystuje klasyczne przestrzenie cyfrowe oraz *dark web* do m.in.

handlu narkotykami, czy transnarodowych przestępstw finansowych (Europol, 2021). Część cyberincydentów powiązana jest z działalnością państwową i można wpisać je w schemat tzw. *state-sponsored cyber operations*, których celem jest m.in. podkopanie zaufania do administracji państwowej i rządów państw UE (np. cyberataki na Europejską Agencję Leków, wskutek których do sieci wyciekły dane o szczepionkach przeciwko Covid-19) (Kiwnik-Pargana, 2021). Takie „wizerunkowe" działanie może w dłuższym okresie prowadzić do wzmacniania kryzysu demokracji liberalnej w krajach UE, co realizowane jest przede wszystkim przez ingerencję w proces wyborczy.

Polityka cyberobrony Unii Europejskiej

Proces integracji europejskiej, od momentu powstania Wspólnot Europejskich w latach 50. XX wieku, jest niczym innym jak rozciągniętym w czasie zwiększaniem kompetencji unijnych instytucji w obszarach zainteresowania UE. Możliwości kształtowania przez Unię systemów politycznych i prawnych rosną wskutek decyzji państw członkowskich, których odzwierciedleniem są zapisy traktatowe, bądź wskutek reakcji tej organizacji na bieżącą sytuację (głównie) gospodarczą – przykład wspólnego długu, który UE zaciągnęła dla realizacji założeń Planu Odbudowy dla Europy. Bezpieczeństwo, w tym cyberbezpieczeństwo, jest również obszarem, który podlega ciągłym zmianom w kierunku zacieśniania współpracy w dziedzinie obrony między państwami członkowskimi. Unia, co najmniej od 2016 roku podejmuje działania, wskazujące na realizację strategii rozszerzania ram wspólnej polityki bezpieczeństwa i obrony o aspekty cyberobrony w postaci zintegrowanego reagowania na cyberataki na unijną infrastrukturę krytyczną oraz na operacje dezinformacyjne w cyberprzestrzeni, które podkopują unijne wartości (przede wszystkim zasady funkcjonowania państwa prawa i modelu liberalnej demokracji).

Jednym z elementów unijnej polityki cyberobrony jest tzw. cyberdyplomacja (dyplomacja cyfrowa). Ta forma kształtowania stosunków dwustronnych Unii z podmiotami trzecimi oraz reagowania na wydarzenia w środowisku międzynarodowym doskonale wpisuje się w praktykę zacieśniania współpracy w ramach wspólnej polityki bezpieczeństwa i obrony. W tym kontekście należy mieć na uwadze fakt, że obszar bezpieczeństwa należy do kompetencji krajowych, Unia zaś pełni rolę pomocniczą w tym zakresie. Współpraca utrudniona jest również z powodu wymaganej jednomyślności dla decyzji dotyczących

obronności. Cyberdyplomacja jawi się zatem jako jeden ze skuteczniejszych (i przede wszystkich możliwych do realizacji w ramach współpracy 27 państw) mechanizmów reagowania na cyberataki. Unia wypracowała w 2017 roku zestaw narzędzi dla dyplomacji cyfrowej (tzw. diplomacy toolbox) (Rada Unii Europejskiej, 2017), którego głównymi składnikami są: współpraca dyplomatyczna i dialog, środki zapobiegawcze przeciwko cyberatakom oraz sankcje. Narzędzia te przeznaczone są do unijnej reakcji na agresywne oraz szkodliwe działania w cyberprzestrzeni i stosowane proporcjonalnie do zakresu, skali, czasu trwania cyberataku, jego intensywności, złożoności, zaawansowania i następstw. Przyjęcie zestawu narzędzi dla dyplomacji cyfrowej oznacza, że UE i państwa członkowskie mają możliwość korzystania ze wszystkich środków, dostępnych w ramach wspólnej polityki zagranicznej i bezpieczeństwa w reakcji na cyberataki, które zagrażają integralności i bezpieczeństwu. Po uchwaleniu *diplomacy toolbox* Unia poszła o krok dalej, przyjmując w maju 2019 roku przepisy umożliwiające jej nakładanie sankcji na osoby indywidualne i/lub podmioty, odpowiedzialne za cyberataki, stanowiące zagrożenie dla UE i jej państw członkowskich (lub wymierzone w państwa trzecie oraz organizacje międzynarodowe, jeśli wiąże się to z realizacją celów wspólnej polityki zagranicznej i bezpieczeństwa) (Decyzja Rady 797, 2019). Pierwsze sankcje za cyberataki „WannaCry", „NotPetya" oraz „Operation Cloud Hopper" zostały nałożone 30 lipca 2020 r. (i przedłużone do 18 maja 2022 r.) na 6 osób i 3 podmioty w postaci zamrożenia aktywów oraz zakazu podróżowania oraz zakazu udostępniania osobom i podmiotom z UE funduszy osobom i podmiotom objętym sankcjami (Decyzja Rady 1127, 2020).

Próba zacieśnienia współpracy w ramach obronności, którą Unia podjęła w połowie drugiej dekady XXI wieku w naturalny sposób dotknęła również cyberprzestrzeń. Za innymi, wiodącymi organizacjami międzynarodowymi (m.in. NATO) oraz mocarstwami (w szczególności USA) Unia uznała cyberprzestrzeń za piątą sferę działań wojennych, obejmującą sieci informacyjno-telekomunikacyjne, infrastruktury i dane przez nie obsługiwane oraz systemy komputerowe, procesory oraz wszelkiego rodzaju urządzenia do sterowania. W obszarze cyberobrony (jak i obrony szerzej) unijne instytucje pełnią zasadniczo rolę pomocniczą, co wynika zarówno z charakteru samej UE, genezy procesu integracji europejskiej oraz (w głównej mierze) z zakresu kompetencji oraz podmiotów tworzących i regulujących systemy bezpieczeństwa i obronności lokalnie i globalnie (państwa narodowe oraz organizacje międzynarodowe o strukturze sojuszów obronnych).

Nie zmienia to jednak faktu, że Unia aspiruje do grona strategicznych graczy w obszarze cyberobrony, próbując zagospodarować te pola, w których możliwe będzie uzyskanie przewagi m.in. nowoczesne technologie cyberobrony, wypracowywane we współpracy państw członkowskich z Europejską Agencją Obrony (EDA), Agencją UE ds. Cyberbezpieczeństwa, Europejskim Funduszem Obrony i Europolem.

Zmianę w unijnym podejściu do cyberobrony zauważa się w nowej cyberstrategii, w której Komisja Europejska zapowiedziała nie tylko koordynację, ale i budowę unijnych zdolności cyberobronnych. Powołanie unijnej jednostki ds. cyberprzestrzeni (*Joint Cyber Unit*) w połowie roku 2021 przybrało realną formę po przedstawieniu przez Komisję Europejską dokładniejszego planu jej utworzenia (Kiwnik-Pargana, 2021). Wypowiedziane wówczas słowa wiceprzewodniczącego KE Margaritisa Schinasa (Komisja Europejska, 2021d), dotyczące przeniesienia cyberbezpieczeństwa ze sfery przemysłowej na sferę bezpieczeństwa narodowego, świadczą o zmianie postrzegania cyberzagrożeń i próbie zacieśnienia współpracy w domenie zarezerwowanej dotychczas dla państw. Proces „przechwytywania" przez Unię kompetencji w zakresie cyberobrony, mimo szumnych zapowiedzi, nie będzie całkowity, biorąc pod uwagę, że instytucje mają kompetencji tyle, ile przekazały im państwa członkowskie w traktatach. Widoczne jest to w samym charakterze planowanej *Joint Cyber Unit*, która mimo, że wykracza poza dotychczasowe ramy współpracy w dziedzinie cyberobrony, nadal jest organem pomocniczym i w pełni uzależnionym od woli państw członkowskich. Jednostka będzie pełniła rolę koordynującą, oferując państwom członkowskim pomoc w reagowaniu i usuwaniu następstw poważnych cyberataków. Oznacza to możliwość powoływania mobilnych zespołów reagowania, które incydent „obsłużą" w czasie realnym oraz korzystania przez państwa unijne z platformy wymiany informacji (wirtualnej i fizycznej), dotyczącej bieżących cyberzagrożeń. Wspólna jednostka ds. cyberprzestrzeni wyposażona zostanie w zdolności techniczne i operacyjne (głównie sprzęt oraz eksperci), z których korzystać będą mogły państwa członkowskie. Komisja Europejska w dokumencie, poświęconym utworzeniu wspólnej jednostki ds. cyberprzestrzeni (Zalecenie Komisji 1086, 2021) zdefiniowała kategorię podmiotów operacyjnych (ENISA, Europol, zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE „CERT-UE", Komisja, Europejska Służba Działań Zewnętrznych – w tym INTCEN, sieć CSIRT i EU-CyCLONe) oraz wspierających (Europejska Agencja Obrony EDA,

przewodniczący grupy współpracy NIS, przewodniczący Horyzontalnej Grupy Roboczej Rady ds. Cyberprzestrzeni oraz jeden przedstawiciel odpowiednich projektów PESCO), określając tym samym ramy współpracy między społecznością cywilną, organami ścigania, dyplomacją i organami odpowiedzialnymi za obronę (Zalecenie Komisji 1086, 2021).

Działania *Joint Cyber Unit* mają w dłuższej perspektywie służyć powstrzymywaniu cyberataków poprzez budowę systemu wczesnego ostrzegania, przygotowanie unijnego planu reagowania na cyberincydenty oraz powoływanie i mobilizowanie zespołów szybkiego reagowania. Cały proces odbywać będzie się w czterech krokach – do końca 2021 roku planowane są ocena aspektów organizacyjnych oraz określenie cyberzdolności operacyjnych UE; do końca czerwca 2022 roku państwa członkowskie są zobowiązane do przygotowania krajowych planów reagowania na incydenty oraz wdrożenie katalogu jednolitych działań naprawczych; do końca 2022 roku nastąpi operacjonalizacja Jednostki dzięki mobilizacji unijnych zespołów szybkiego reagowania; pełną funkcjonalność Jednostka uzyska do końca czerwca 2023 roku, po włączeniu sektora prywatnego, użytkowników oraz dostawców cyberrozwiązań i usług do procesu wymiany informacji (Komisja Europejska, 2021e, 2021f).

Nacisk na rozwój współpracy operacyjnej w dziedzinie cyberbezpieczeństwa jest wyrazem nie tylko reakcji Unii na zmieniający się charakter zagrożeń, szczególnie w krajach rozwiniętych, ale również przejawem realizacji szerszego planu, w którym UE pełni rolę strategicznego i autonomicznego podmiotu, kształtującego system bezpieczeństwa europejskiego i globalnego.

Podsumowanie

Odpowiedzi na pytanie o przyczyny zaangażowania Unii Europejskiej w kształtowanie bezpiecznej cyberprzestrzeni, zarówno w obszarze gospodarczym, jak i obronnym, należy szukać w procesie ewolucji tej organizacji w stronę autonomicznego podmiotu regulującego kwestie bezpieczeństwa w ogóle. Cyberbezpieczeństwo jest w tym kontekście jedną z dróg, umożliwiających Unii realizację strategicznych założeń, w których Wspólnota wyrasta na silnego gracza w stosunkach międzynarodowych, obejmującego swoimi działaniami już nie tylko płaszczyznę gospodarczą, ale również obronną. Scenariusz ten niezwykle trudno urzeczywistnić z powodów instytucjonalnych i prawnych – polityka zagraniczna, bezpieczeństwa, a tym bardziej obronna leżą w kompetencjach państw

członkowskich, instytucje unijne zaś pełnią w tym zakresie rolę pomocniczą. Unia nie jest także organizacją o charakterze sojuszu obronnego, funkcję tę spełnia NATO. Wobec powyższego możliwości wpływania przez Wspólnotę na kształt globalnego (i regionalnego) systemu bezpieczeństwa są ograniczone. Niemniej, od drugiej połowy drugiej dekady XXI wieku Unia podejmuje kroki w celu zacieśnienia współpracy w obszarze bezpieczeństwa, w tym również cyberbezpieczeństwa.

Podyktowane jest to, oprócz przyczyn, wynikających z ewolucji procesu integracji, czynnikami instytucjonalno-prawnymi oraz gospodarczo-klimatycznymi. W pierwszym przypadku regulacje w zakresie cyberbezpieczeństwa odbywają się głównie w ramach polityki przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Dotyczą przede wszystkim zapobiegania i niwelowania skutkom cyberprzestępczości, a sposób podejmowania decyzji przez unijne instytucje w zwykłej procedurze prawodawczej (tzw. system większości kwalifikowanej) pozwala na tworzenie większej liczby bardziej szczegółowych przepisów, chroniących cyberprzestrzeń. Czynniki gospodarczo-klimatyczne, należą do najbardziej pierwotnych przyczyn zainteresowania Unii problematyką cyberbezpieczeństwa. Fundamentem funkcjonowania całej Wspólnoty jest wzrost gospodarczy i bogacenie się gospodarek państw członkowskich. Istotną cegiełką w tym procesie, w warunkach powszechnej w Europie cyfryzacji i rosnącego wykorzystania nowoczesnych technologii, jest zapewnienie bezpieczeństwa w cyberprzestrzeni i zapobieganie stratom finansowym w wyniku cyberprzestępstw.

UE w swoich działaniach posuwa się dalej, wkraczając w sferę obronności, mimo, że kompetencje te zasadniczo zarezerwowane są dla państw członkowskich i sojuszy o charakterze obronnym. Unijna polityka cyberbezpieczeństwa zaczęła wykraczać poza „standardowy", pomocniczy charakter, oferując swoim członkom coraz bardziej zaawansowane formy współpracy. W aktualnych warunkach (instytucjonalno-prawnych, ale także międzynarodowych) autonomiczny, obejmujący aspekty cyberprzestępczości i cyberobrony, w pełni operacyjny unijny system cyberbezpieczeństwa nie powstanie. Niemniej, wysiłki UE służące jej celom gospodarczym, klimatycznym i politycznym, realizowane poprzez przejrzystą politykę cyberbezpieczeństwa wymagają odnotowania i analizy. Mogą bowiem stanowić zalążek większego „projektu" w dziedzinie cyberbezpieczeństwa o zasięgu europejskim.

Bibliografia

CISCO. (2020, February 18). *New Cisco Annual Internet Report Forecasts 5G to Support More Than 10% of Global Mobile Connections by 2023*. https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=2055169 [15.09.2021].

Decyzja Rady 1127. (2020). Decyzja Rady (WPZiB) 2020/1127 z dnia 30 lipca 2020 r. zmieniająca decyzję (WPZiB) 2019/797 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim. *Dziennik Urzędowy Unii Europejskiej* L 246 z 30.7.2020. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32020D1127 [15.09.2021].

Decyzja Rady 797. (2019). Decyzja Rady (WPZiB) 2019/797 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim. *Dziennik Urzędowy Unii Europejskiej* L 129I z 17.5.2019. https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32019D0797 [13.09.2021].

Dyrektywa 1148. (2016). Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. *Dziennik Urzędowy Unii Europejskiej* L 194 z 19.07.2016. https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32016L1148 [13.09.2021].

ENISA. (2020). *Przegląd roczny. Od stycznia 2019 r. do kwietnia 2020 r. Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)*. https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-a-year-in-review-ebook-en-pl.pdf [10.09.2021].

Europol. (2021). *European Union serious and organised crime threat assessment. A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime*. Publications Office of the European Union. https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment [11.09.2021].

Forsal.pl (2021, 30 czerwca). Ponad ćwierć miliona cyberprzestępstw w Hiszpanii w czasie pandemii. *Forsal.pl*. https://forsal.pl/lifestyle/technologie/artykuly/8200885,cyberprzestepstwa-w-hiszpanii-w-czasie-pande-mii.html [10.09.201].

Fürstenau, M. (2021, 11 maja). Cyberprzestępczość kwitnie. Dzięki pandemii koronawirusa. *Deutsche Welle*. https://www.dw.com/pl/cyberprzest%C4%99pczo%C5%9B%C4%87-kwitnie-dzi%C4%99ki-pandemii-koronawirusa/a-57497463 [10.09.2021].

Hall, P. A., & Taylor, R. C. R. (1996). Political Science and the Three New Institutionalism. *Political Studies, 44*(5), 936–957. https://doi.org/10.1111/j.1467-9248.1996.tb00343.x

Janusz, G. (2011). Procedury legislacyjne w Unii Europejskiej po traktacie z Lizbony. *Polityka i Społeczeństwo, 8*, 125–135.

Kiwnik-Pargana, J. (2021, 6 czerwca). UE szykuje się do walki z hakerami. *Deutsche Welle*. https://www.dw.com/pl/ue-szykuje-si%C4%99-do-walki-z-hakerami/a-58018182 [13.09.2021].

Komisja Europejska. (2010). EUROPA 2020. Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu (COM (2010)/2020 końcowy). https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52010DC2020 [05.09.2021].

Komisja Europejska. (2020a). Wspólny komunikat do Parlamentu Europejskiego i Rady. Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę (JOIN (2020) 18 final). https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020JC0018 [06.09.2021].

Komisja Europejska. (2020b). Wniosek. Rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) i zmieniające dyrektywę 2000/31/WE (COM (2020) 825 final). https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020PC0825 [10.09.2021].

Komisja Europejska. (2020c). Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Europejska strategia w zakresie danych (COM (2020) 66 final). https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020DC0066 [10.09.2021].

Komisja Europejska. (2020d). Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie strategii UE w zakresie unii bezpieczeństwa (COM (2020) 605 final). https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020DC0605 [09.09.2021].

Komisja Europejska. (2020e). *Implementation Strategy for Horizon Europe*. https://ec.europa.eu/info/sites/default/files/research_and_innovation/strategy_on_research_and_innovation/documents/ec_rtd_implementation-strategy_he.pdf [08.09.2021].

Komisja Europejska. (2021a). Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie (COM (2021) 118 final). https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021DC0118 [09.09.2021].

Komisja Europejska. (2021b). *Horizon Europe Strategic Plan (2021–2024)*. https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/3c6ffd74-8ac3-11eb-b85c-01aa75ed71a1 [10.09.2021].

Komisja Europejska. (2021c). *Plan odbudowy dla Europy*. https://ec.europa.eu/info/strategy/recovery-plan-europe_en [05.09.2021].

Komisja Europejska. (2021d). *Remarks by Vice-President Schinas at the press conference on the Recommendation on building a Joint Cyber Unit* (Speech/21/3172). https://ec.europa.eu/commission/presscorner/detail/pl/speech_21_3172 [05.09.2021].

Komisja Europejska. (2021e, 23 czerwca). *Joint Cyber Unit*. https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit [31.08.2021].

Komisja Europejska. (2021f, 23 czerwca). *EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents*. Directorate-General for Communication. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088 [31.08.2021].

Kuś, A. (2014). Rodzaje kompetencji Unii Europejskiej a unijna polityka podatkowa. *Studia z Polityki Publicznej, 2*(2), 79–95. https://doi.org/10.33119/KSzPP.2014.2.4

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review, 35*(6), 105336. https://doi.org/10.1016/j.clsr.2019.06.007

Morgan, S. (2019a, 6 lutego). 2019/2020 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. *Cibercrime Magazine*. https://cybersecurityventures.com/cybersecurity-almanac-2019/ [05.09.2021].

Morgan, S. (2019b, 18 lipca). Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion. *Cibercrime Magazine*. https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/ [04.09.2021].

Morgan, S. (2020, 13 listopada). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cibercrime Magazine*. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ [31.08.2021].

NIS Cooperation Group. (2020*). Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures [04.09.2021].

Protokół nr 2. (2008). Protokół (nr 2) w sprawie stosowania zasad pomocniczości i proporcjonalności. *Dziennik Urzędowy Unii Europejskiej* C 115 z 9.05.2008. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:12008E/PRO/02 [10.09.2021].

Rada Unii Europejskiej. (2017). Konkluzje Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej"), nr 10474/17 z 19.06.2017. https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/pl/pdf [08.09.2021].

Rada Unii Europejskiej. (2018). Ramy polityki UE w zakresie cyberobrony (nr 14413/18). https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf [09.09.2021].

Rada Unii Europejskiej. (2020a). Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021–2027 - Analysis of the final compromise text with a view to agreement (nr 13835/20). https://data.consilium.europa.eu/doc/document/ST-13835-2020-INIT/en/pdf [10.09.2021].

Rada Unii Europejskiej. (2020b). Konkluzje prezydencji – Karta praw podstawowych w kontekście sztucznej inteligencji i przemian cyfrowych (nr 11481/20). https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/pl/pdf [08.09.2021].

Rada Unii Europejskiej. (2020c). Kształtowanie cyfrowej przyszłości Europy – Konkluzje Rady z 9 czerwca 2020 r. (nr 8711/20). https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/pl/pdf [10.09.2021].

Rada Unii Europejskiej. (2020d). Konkluzje Rady pt. „Dostęp do wymiaru sprawiedliwości – wykorzystanie możliwości wynikających z cyfryzacji" – tekst uzgodniony przez Coreper (nr 11599/20). https://data.consilium.europa.eu/doc/document/ST-11599-2020-INIT/pl/pdf [08.09.2021].

Rada Unii Europejskiej. (2021). Stanowisko Rady w pierwszym czytaniu w sprawie przyjęcia Rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego program „Cyfrowa Europa" oraz uchylającego decyzję (UE) 2015/2240 - Przyjęte przez Radę w dniu 16 marca 2021 r. (nr 6789/1/20). https://data.consilium.europa.eu/doc/document/ST-6789-2020-REV-1/pl/pdf [10.09.2021].

Reynolds, H. T., & Johnson, J. B. (2011). *Political Science Research Methods*. CQ Press.

Robles-Carrillo, M. (2021). European Union policy on 5G: Context, scope and limits. *Telecommunications Policy, 45*(8), 102216. https://doi.org/10.1016/j.telpol.2021.102216

Rozporządzenie 679. (2016). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). *Dziennik Urzędowy Unii Europejskiej* L 119 z 4.5.2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj [05.09.2021].

Rozporządzenie 881. (2019). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie). *Dziennik Urzędowy Unii Europejskiej* L 151 z 7.6.2019. https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32019R0881 [08.09.2021].

Skolimowska, A. (2015). *Normatywna potęga Unii Europejskiej w obliczu umiędzynarodowionych konfliktów wewnętrznych*. Dom Wydawniczy Elipsa.

Traktat o funkcjonowaniu Unii Europejskiej. (2016). Wersja skonsolidowana Traktatu o funkcjonowaniu Unii Europejskiej. *Dziennik Urzędowy Unii Europejskiej* C 202 z 7.6.2016. https://eur-lex.europa.eu/collection/eu-law/treaties/treaties-force.html#new-2-52 [10.09.2021].

Traktat o Unii Europejskiej. (2016). Wersja skonsolidowana Traktatu o Unii Europejskiej. *Dziennik Urzędowy Unii Europejskiej* C 202 z 7.6.2016. https://eur-lex.europa.eu/collection/eu-law/treaties/treaties-force.html#new-2-52 [10.09.2021].

von der Leyen, U. (2019). *A Union that strives for more. My agenda for Europe, political guidelines for the next European Commission 2019–2024*. https://ec.europa.eu/info/sites/info/files/political-guidelines-next-commission_en_0.pdf [06.09.2021].

Wojtaszczyk, K. A., Wiśniewska-Grzelak, J., Stawarz, P., & Biernacka-Rygiel, A. (red.). (2015). *Problemy instytucjonalne Unii Europejskiej – wymiar teoretyczno-metodologiczny*. Aspra.

Zalecenie Komisji 1086. (2021). Zalecenie Komisji (UE) 2021/1086 z dnia 23 czerwca 2021 r. w sprawie utworzenia wspólnej jednostki ds. cyberprzestrzeni. *Dziennik Urzędowy Unii Europejskiej* L 237 z 5.7.2021. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32021H1086 [08.09.2021].

Zalecenie Komisji 534. (2019). Zalecenie Komisji (UE) 2019/534 z dnia 26 marca 2019 r. Cyberbezpieczeństwo sieci 5G. *Dziennik Urzędowy Unii Europejskiej* 88 z 29.03.2019. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32019H0534 [10.09.2021].