Teka of Political Science and International Relations – UMCS, 2020, 15/2, 7–23

DOI: 10.17951/teka.2020.15.2.7-23

REFORMA POLITYKI CYBERBEZPIECZŃSTWA UNII EUROPEJSKIEJ

Izabela Oleksiewicz

Politechnika Rzeszowska
Zakład Prawa i Administracji
ORCID: https://orcid.org/0000-0002-1622-7467
e-mail: oleiza@prz.edu.pl

Streszczenie: Globalna strategia UE na rzecz polityki zagranicznej i bezpieczeństwa została przyjęta przez Radę Europejską 28 czerwca 2016 r.[1] Określa wspólne interesy UE i państw członkowskich. Opiera się na następujących celach: bezpieczeństwie obywateli i terytorium, dobrobycie, demokracji, ładzie światowym, które mają doprowadzić do stworzenia wiarygodnej, reaktywnej i spójnej Unii Europejskiej. Zasady, którymi zaczęła kierować się Unia Europejska, to jedność, współdziałanie z innymi, odpowiedzialność, pogłębianie partnerstw zewnętrznych.
Warto zauważyć, że cyberbezpieczeństwo w Unii Europejskiej jest prerogatywą państw członkowskich w przeciwieństwie do cyberterroryzmu, który należy do kompetencji dzielonych. Mimo to UE ma do odegrania kluczową rolę w tworzeniu warunków dla zdolności państw członkowskich, aby ulepszać, współpracować i budować zaufanie.
W niniejszym artykule zostanie podjęta próba wykazania, że na skuteczność działań podejmowanych przez organy Unii Europejskiej w zakresie polityki cyberterrorystycznej zależy od rodzaju instrumentów będących w dyspozycji UE i państw członkowskich oraz podstawy prawnej odpowiednich regulacji. Problemem pozostają nieścisłości prawne i rozbieżności interpretacyjne w zapisie regulacji prawnych na poziomie unijnym w zakresie podziału kompetencji dotyczących ochrony cyberprzestrzeni, które w rzeczywistości prowadzą do opóźnienia powstania wzajemnej współpracy między Unią a państwami członkowskimi.

Słowa kluczowe: cyberbezpieczeństwo, Unia Europejska, dyrektywa NIS, strategia, harmonizacja

1. WPROWADZENIE

Cyberprzestrzeń oraz szybkość przeprowadzania ataków sprawiają, że prowadzenie działań obronnych jest utrudnione, a akcje ofensywne są relatywnie tanie i łatwe do przeprowadzenia. Wirtualność, jako cecha cyberprzestrzeni, jest

[1] https://eeas.europa.eu/top_stories/pdf/eugs_pl_.pdf (dostęp: 3.02.2021 r.).

tym wyraźniejsza, im większe jest uzależnienie społeczeństw od jej wykorzystania. Można tu bowiem zauważyć pewien paradoks, z jednej strony wykorzystanie technologii ICT we wszystkich sferach życia ludzkiego wiąże się z wieloma korzyściami, np. natury organizacyjnej, komunikacyjnej czy finansowej, z drugiej – zaawansowany technologicznie podmiot jest zdecydowanie bardziej wrażliwy na ataki teleinformatyczne.

Ponadto, jak zauważył Fred Schreier[2], przestrzeń teleinformatyczna przez wielu jest postrzegana jako część wspólnego dziedzictwa ludzkości. Czynnikiem zewnętrznym, który wywiera większy wpływ na środowisko bezpieczeństwa niż podziały w społeczności międzynarodowej, są procesy globalizacyjne. Globalizacja wydaje się już tak zaawansowana, że sieć różnych powiązań między państwami i społeczeństwami na świecie ma zbyt dużą gęstość, aby ulec dezintegracji czy znacznej redukcji. Nieuniknioną konsekwencją globalizacji jest erozja suwerenności państw, która dotyka każdego kraju, choć w zróżnicowanym stopniu. Wynika to z „odterytorialnienia" procesów społecznych oraz pogłębiania się rozmaitych współzależności w skali globalnej lub międzynarodowej, w każdej dziedzinie życia społecznego. Proces ten dokonuje się stopniowo, jest jednak równie trwały jak globalizacja, wpływając w ten sposób na porządek i środowisko międzynarodowe[3]. Procesy globalizacji, zwłaszcza oddziałujące na sferę społeczno-ekonomiczną, tworzą nowe zagrożenia bezpieczeństwa. Ma również znaczenie fakt, że część zjawisk kryzysogennych toczy się poza jej terytorium. Wprost oddziałują one na wewnętrzną sytuację państw europejskich oraz społeczność europejską. W opinii znacznych części społeczeństw utrzymanie gwarancji zatrudnienia i adekwatnej liczby miejsc pracy, odpowiedniego poziomu bezpieczeństwa socjalnego czy tożsamości kulturowej powinno stać się priorytetem państwa.

Ponieważ zjawisko cyberterroryzmu ma charakter transgraniczny, polityka ochrony cyberprzestrzeni powinna nie tylko zwalczać zagrożenia cyberbezpieczeństwa, ale opierać się na współpracy międzypaństwowej i koordynacji działań, które stanowią nieodzowny element skutecznej odpowiedzi na zagrożenie, jakim jest cyberterroryzm. Złożoność natury tego zjawiska powoduje jednak, że państwa muszą być elastyczne w reakcji na to zjawisko i zdolne do adaptacji zmieniających się warunków. Podjęto próbę wykazania, że pierwszoplanową rolę w skuteczności zwalczania zjawiska cyberterroryzmu odgrywa współpraca na poziomie zarówno państw członkowskich, jak i międzyinstytucjonalnym w poszczególnych państwach. Zostało to udowodnione, ponieważ w analizowanych strategiach państw największy nacisk położono właśnie na współpracę i tworzenie partnerstw publiczno-prywatnych (PPP) oraz reguł usprawniających współpracę międzypaństwową. W ten sposób zostaje potwierdzona teza, że im większy po-

[2] Schreier F., 2015: *On cyberwarfare,* DCAF Horizon, working paper, s. 7–10.

[3] Por.: Oleksiewicz I., 2016: *Polskie prawo karne w zakresie walki z cyberprzestępczością na tle standardów prawa UE*, w: Pietraś M., Chałupczak H., Misiągiewicz J. (red.), 2016: *Europa Środkowo-Wschodnia w procesie transformacji i integracji. Wymiar bezpieczeństwa,* Zamość, s. 530 i n.

ziom wzmacniania współpracy między państwami i mechanizmów implementacji wewnątrzunijnych w obliczu zjawiska cyberprzestepczości, tym większe prawdopodobieństwo stabilności i bezpieczeństwa w UE i poszczególnych państwach.

To z kolei może prowadzić do zjawiska „nadregulacji", ponieważ art. 73 TFUE wyraźnie dopuszcza możliwość stanowienia norm prawnych za zgodą państw na szczeblu unijnym. Jednocześnie zgodnie z art. 75 TFUE to zwalczanie terroryzmu i cyberterroryzmu znalazło się w obszarze kompetencji dzielonych UE i państw członkowskich, obszar cyberobrony jest natomiast podstawowym zadaniem i kompetencją państwa w polityce wewnętrznej państwa członkowskiego, co wynika z art. 4 wzw. 72 TFUE. Unii przyznano prawo do stanowienia strategii bezpieczeństwa w myśl art. 68 TFUE. W tej sytuacji prawnej państwa mogą, ale nie muszą uregulować kwestie związane z polityką cyberobrony. Na szczeblu unijnym może dojść do zjawiska nadregulacji i kolizji przepisów prawnych, co będzie negatywnie wpływało na proces usprawniania współpracy między państwami.

Artykuł 83 TFUE umożliwia współpracę wymiarów sprawiedliwości w sprawach karnych oraz ustanowienie minimalnych zasad dotyczących definicji przestępstwa i sankcji w obszarach poważnych przestępstw o wymiarze transgranicznym, w tym przestępstw komputerowych. W związku z tym istnieje możliwość opracowania kolejnej ogólnej dyrektywy dotyczącej przemocy w cyberprzestrzeni, zawierającej definicje różnych rodzajów przemocy. Powinien nastąpić przegląd dyrektyw w sprawie praw ofiar przestępstw uwzględniający specyficzny charakter przemocy uwarunkowanej płcią i małoletniością oraz zawierać stosowne odniesienia do rozwiązań prawnych, które należałoby wprowadzić.

2. ISTOTA REFORMY POLITYKI CYBERBEZPIECZEŃSTWA UE

Podstawą reformy miały być działania przewidziane w strategii cyberbezpieczeństwa oraz główny filar strategii – dyrektywa o bezpieczeństwie sieci i informacji (dyrektywa NIS). Szybki rozwój usług komunikacyjnych związany z przesyłaniem olbrzymiej ilości danych stawia wiele wyzwań przed podmiotami odpowiedzialnymi za ich przesyłanie, przechowywanie i przetwarzanie. Dodatkowo automatyzacja sieci energetycznych i budowa tzw. sieci inteligentnych powoduje również zwiększenie ilości gromadzonych danych. Ta szeroko rozumiana informatyzacja działalności związanej z dostarczaniem energii elektrycznej sprawia, że jest ona narażona na cyberataki. Konieczne jest zatem rozwijanie narzędzi, które pozwolą w maksymalnie zabezpieczyć prowadzenie działalności dystrybucyjnej oraz odbiorców energii.

Według niektórych uczonych do połowy tego wieku sztuczna inteligencja będzie poza ludzkim zrozumieniem i kontrolą[4]. Jeśli tak się stanie, ludzkość napotka

[4] Barfield W., 2015: *Cyber-Humans. Our Future with Machines*, New York, s. 19–21.

bezprecedensowe problemy prawne, a antropocentryczny punkt widzenia dzisiejszych systemów prawnych nie pozwala ludzkości rozwiązać tych problemów[5].

Chociaż w 2005 r. Rada UE przyjęła strategię w dziedzinie walki z terroryzmem (w tym także z cyberterroryzmem), aby globalnie zwalczać terroryzm i zapewnić Europie bezpieczeństwo przy jednoczesnym poszanowaniu praw człowieka i umożliwieniu obywatelom UE życia w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, to strategia walki ze zjawiskiem cyberterroryzmu została przyjęta w UE w 2013 r. Ważny był również *Program sztokholmski*, który wyznał w dziedzinie sprawiedliwości i spraw wewnętrznych cele strategiczne na lata 2010−2014[6].

Następnie UE przyjęła *Strategię globalną UE* w 2016 r., co wyraźnie ożywiło działania dotyczące polityki bezpieczeństwa związane z polityką antyterrorystyczną (w tym cyberterrorystyczną). Obecna *Strategia UE* z 2016 r. identyfikuje pięć priorytetów, którymi są:

- bezpieczeństwo Unii, które ma polegać na intensyfikacji działań w zakresie obronności, bezpieczeństwa cybernetycznego, zwalczania terroryzmu oraz energii i strategicznej komunikacji;
- sąsiedztwo i odporność, którą zdefiniowano jako zdolność państw i społeczeństw do reformowania się, a tym samym do zwalczania różnych kryzysów, dzięki czemu będzie można inwestować w odporność państw i społeczeństw leżących na wschód i południe od UE;
- zintegrowane podejście do sytuacji konfliktowych (wojna i kryzys), które będzie polegać na bezzwłocznym reagowaniu, działaniu, zapobieganiu oraz inwestowaniu w stabilizację;
- wspieranie stabilnych porządków regionalnych opartych na współpracy na całym świecie (regiony jako kluczowa przestrzeń ładu);
- skuteczne globalne rządzenie w XXI w., czyli działania na rzecz światowego ładu opartego na prawie międzynarodowym, zapewniające poszanowanie praw człowieka, zrównoważony rozwój oraz trwały dostęp do globalnych wspólnych dóbr[7].

Międzynarodowa współpraca w cyberprzestrzeni podkreśla zaangażowanie UE we wspieranie rozwoju budowania zaufania w cyberbezpieczeństwie, aby zwiększyć przejrzystość i zmniejszyć ryzyko nieporozumień, w zachowanie państwa polegające na promowaniu ustanawiania międzynarodowych norm w tej dziedzinie i wzywaniu Komisji oraz wysokiego przedstawiciela, zgodnie z odpowiednimi procedurami do promowania:

---

[5] Pagallo U., 2013: *The laws of robots: crimes, contracts, and torts*, New York, s. 47–66.

[6] *Program sztokholmski – otwarta i bezpieczna Europa dla dobra i ochrony obywateli*, Bruksela, 2 grudnia 2009 r. (17024/09); Przestrzeń wolności, bezpieczeństwa i sprawiedliwości: Plan działań służący realizacji programu sztokholmskiego (COM(2010) 171).

[7] Por.: Wróblewska-Łysik M., 2016: *Europejska Strategia Globalna a możliwości współpracy Unii Europejskiej z NATO po szczycie w Warszawie*, Bezpieczeństwo Narodowe, nr I–IV, s. 67–70.

- konwencji budapeszteńskiej jako wzoru do opracowywania krajowej cyberprzestępczości,
- ustawodawstwa i podstawy międzynarodowej współpracy w tej dziedzinie,
- szacunku podstawowych praw w cyberprzestrzeni,
- pełnego wykorzystania wszystkich dostępnych międzynarodowych narzędzi współpracy służących rozwojowi walki z cyberprzestępczością, powiązanych ze współpracą policyjną i sądową w krajach trzecich, w których dochodzi do cyberprzestępczości,
- poszukiwania wiedzy specjalistycznej państw członkowskich w dziedzinie cyberprzestrzeni i ich doświadczeń w ramach stosunków dwustronnych[8].

We wrześniu 2017 r. Komisja Europejska rozpoczęła przegląd europejskiej strategii bezpieczeństwa cybernetycznego z 2013 r., wydając dokument roboczy przedstawiający jej ocenę[9]. Zgodnie z nim strategia ta była tylko częściowo skuteczna z powodu niewystarczających zasobów i ograniczonego zaangażowania kluczowych podmiotów. Ponadto od tamtej pory możliwości i zagrożenia w cyberprzestrzeni znacznie się rozwinęły. Czynniki te uzasadniły więc podjęcie ważnego kroku, tj. odnowienie strategii cyberbezpieczeństwa[10]. Kolejnym ważnym krokiem w jej wdrażaniu jest z pewnością ustanowienie i uruchomienie pod koniec 2017 r. projektu Stałej Współpracy Strukturalnej, czyli PESCO[11]. *Strategia globalna UE* wdrażana jest na trzech polach: politycznym, ekonomicznym i międzynarodowym. Pole polityczne to implementacja w dziedzinie bezpieczeństwa i obrony koordynowana przez Wysoką Przedstawiciel ds. WPBiO. Pole ekonomiczne stanowi europejski plan działań na rzecz obronności realizowany przez Komisję Europejską. Trzecie pole międzynarodowe to realizacja przez wszystkie podmioty UE porozumienia o współpracy z NATO. Najważniejszym dokumentem wdrożeniowym wobec strategii jest *Plan implementacji w dziedzinie bezpieczeństwa i obronności*[12]. W jego ramach ustanowiono nowy poziom UE dotyczący bezpieczeństwa i obronności w odniesieniu do trzech podstawowych zadań: re-

[8] Biscop S., 2019: *The EU Global Strategy 2020*, Security Policy Brief, nr 108, s. 1–3.

[9] *Commission Staff Working Document Assessment of the EU 2013 Cybersecurity Strategy*, 2017, źródło: https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF (dostęp: 18.01.2021 r.).

[10] Ibidem.

[11] Obejmuje również: ochronę sieci i infrastruktury krytycznej, bezpieczeństwo granic zewnętrznych z budowaniem takich zdolności u swoich partnerów włącznie, ochronę cywilną i reagowanie na katastrofy, zapewnienie stabilnego dostępu i korzystania z przestrzeni globalnych (cyberprzestrzeń, przeciwdziałanie zagrożeniom hybrydowym, cyberbezpieczeństwo, zapobieganie i przeciwdziałanie terroryzmowi zwalczanie przemytu, nielegalnej migracji oraz nielegalnego handlu bronią i zorganizowanej przestępczości). W ramach politycznej implementacji *Strategii globalnej* na szczególną uwagę zasługuje konsekwentne zmierzanie do uruchomienia PESCO, przewidzianej w art. 42.6 i 46 Traktatu o Unii Europejskiej i Protokole 10.

[12] COM(2016) 950 final, 30.11.2016.

agowania na zewnętrzne konflikty i kryzysy, budowania zdolności partnerów, ochrony UE i jej obywateli. Przy każdym z tych założeń strategia podkreśla wagę współpracy z państwami trzecimi i instytucjami międzynarodowymi.

Sytuacja ta zmieniła się za sprawą wprowadzenia dyrektywy NIS. Akt ten formalnie stworzył sieć zespołów reagowania państw członkowskich na incydenty komputerowe (CSIRT), a sekretariat tej sieci zapewnia ENISA. Głównym celem agencji jest wspieranie państw członkowskich we wdrażaniu dyrektywy NIS. Agencja otrzymała nowe zadania i zasoby w takich dziedzinach, jak współpraca operacyjna i certyfikacja bezpieczeństwa technologii informacyjno-komunikacyjnych (ICT) w celu podejmowania działań, które będą odzwierciedlać nowe potrzeby w zakresie bezpieczeństwa cybernetycznego. ENISA odgrywa zatem ważną rolę w dziedzinie unijnej polityki certyfikacji bezpieczeństwa cybernetycznego dzięki przygotowaniu we współpracy z organami certyfikującymi państw członkowskich systemów certyfikacji bezpieczeństwa cybernetycznego[13].

Jednym z zadań polityki UE w zakresie cyberbezpieczeństwa jest wzmocnienie zdolności i współpracy w obszarze bezpieczeństwa cybernetycznego w celu zapewnienia takiego samego poziomu rozwoju we wszystkich państwach członkowskich na ataki cybernetyczne pochodzące zarówno z zewnątrz, jak i wewnątrz.

Celem dyrektywy NIS jest stworzenie równych szans wśród państw członkowskich UE, ustanawiając wymóg posiadania właściwego organu ds. cyberbezpieczeństwa, jak również zdolność do reagowania na incydenty techniczne na poziomie krajowym. W dokumencie zachęca się do współpracy między państwami członkowskimi w celu ułatwienia wymiany informacji i współpracy operacyjnej w razie incydentów. Dyrektywa zatem koncentruje się na zwiększeniu szybkości, regularności i centralizacji wymiany informacji między sektorami publicznym a prywatnym[14]. Dokument nie tworzy jednak centralnego europejskiego wykazu infrastruktury krytycznej ani nie wymaga wspólnych norm. Rządy poszczególnych państw są zobowiązane do współpracy i dzielenia się niektórymi informacjami, ale akt ten nie wprowadza wymogów obowiązkowej ogólnoeuropejskiej współpracy i mechanizmów wymiany informacji, które pierwotnie przewidywano.

Drugim ważnym aktem prawnym jest – wspomniane wcześniej – rozporządzenie w sprawie ochrony danych osobowych (RODO, inaczej GDPR)[15]. Nowe przepisy tworzy spójny, jednolity zbiór regulacji dla wszystkich przedsiębiorstw działających w UE, które przetwarzają dane osobowe obywateli UE. Celem tego rozporządzenia jest ochrona praw jednostki w związku z przetwarzaniem danych osobowych. Określa ono prawo dostępu do informacji, reguluje gromadzenie

[13] Komunikat Komisji, 2017: *State of the Union 2017: The Commission scales up its response to cyberattacks,* źródło: europa.eu/rapid/press-release_MEMO-17-3194_en.pdf (dostęp: 19.01.2021 r.).

[14] Por.: Kowalkowski S. (red.), 2011: *Niemilitarne zagrożenia bezpieczeństwa publicznego*, Warszawa, s. 55.

[15] Ilves L.K. et al., 2016: *European Union and NATO global cybersecurity challenges. A way Forward,* PRISM, vol. 6, nr 2, s. 133.

informacji, przetwarzanie i przekazywanie danych między podmiotami publicznymi oraz daje obywatelom prawo do „bycia zapomnianym", co wymaga od przedsiębiorstw usunięcia pewnych danych osobowych na wniosek obywatela.

Często porównuje się rozporządzenie GDPR i dyrektywę NIS. Należy jednak zwrócić uwagę na różnice z punktu widzenia polityki cyberbezpieczeństwa. Dyrektywa w sprawie bezpieczeństwa sieci i informacji kładzie większy nacisk na sprawne funkcjonowanie gospodarki. Jej jednym z podstawowych zadań jest pomoc przedsiębiorstwom skuteczniej zapobiegać atakom na infrastrukturę cyfrową, której sieć obejmuje wiele państw UE.

Podstawą reformy były działania przewidziane w strategii cyberbezpieczeństwa oraz główny filar strategii – dyrektywa o bezpieczeństwie sieci i informacji (dyrektywa NIS)[16]. Poza tym przewiduje się:

- utworzenie Europejskiego Centrum Badań Naukowych i Kompetencji w dziedzinie Bezpieczeństwa Cybernetycznego (projekt pilotażowy został zrealizowany w 2018 r.). Współpracując z państwami członkowskimi, pomoże ono w opracowywaniu i wdrażaniu narzędzi oraz technologii koniecznych, aby sprostać stale zmieniającym się zagrożeniom, i zagwarantuje, że obrona będzie tak nowoczesna, jak broń, którą posługują się cyberprzestępcy. Centrum będzie uzupełniać działania na rzecz budowy potencjału w tej dziedzinie na poziomach unijnym i krajowym[17];
- opracowanie planu szybkiego reagowania państw członkowskich umożliwiającego natychmiastową, skuteczną i skoordynowaną reakcję w przypadkach wystąpienia ataków cybernetycznych na dużą skalę. Ponadto wzywa się państwa członkowskie i instytucje UE do ustanowienia ram reagowania w sytuacji kryzysu cybernetycznego tak, aby można było ten[18] plan wprowadzić w życie. Będzie on poddawany regularnym testom w ramach ćwiczeń dotyczących zarządzania w sytuacji kryzysu cybernetycznego lub innej sytuacji kryzysowej;
- większą solidarność – w przyszłości można rozważyć możliwość utworzenia nowego funduszu pomocy w cybernetycznych sytuacjach kryzysowych dla tych państw członkowskich, które odpowiedzialnie wdrożą wszystkie środki cyberbezpieczeństwa wymagane na podstawie prawa UE. Fundusz mógłby służyć zapewnianiu wsparcia państwom członkowskim w sytuacjach nadzwyczajnych, podobnie jak Unijny Mechanizm Ochrony Ludności jest wykorzystywany do pomocy w przypadku pożarów lub klęsk żywiołowych;

[16] Dyrektywa Parlamentu Europejskiego i Rady 2016/1148/UE z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE UE L 194 z 19.07.2016 r.).

[17] Szerzej: http://www.consilium.europa.eu/pl/policies/cyber-security/ (dostęp: 3.02.2021 r.).

[18] https://ec.europa.eu/digital-single-market/en/cyber-security (dostęp: 3.02.2021 r.).

- wzmocnienie zdolności w zakresie obrony cybernetycznej – państwa członkowskie zachęca się do włączenia cyberobrony w ramy stałej współpracy strukturalnej (PESCO) i Europejskiego Funduszu Obrony, aby wspierać projekty dotyczące cyberobrony. Można też poszerzyć cyberobronę o zakres działania Europejskiego Centrum Badań Naukowych i Kompetencji w dziedzinie Bezpieczeństwa Cybernetycznego. Aby rozwiązać problem niedoboru wykwalifikowanej kadry w tym zakresie, w 2018 r. UE stworzyła platformę szkoleń i edukacji w dziedzinie cyberobrony. UE i NATO wspierają współpracę na rzecz badań naukowych i innowacji w dziedzinie obrony cybernetycznej. Współpraca z NATO zostanie zacieśniona przez udział w równoległych i skoordynowanych ćwiczeniach;
- pogłębienie współpracy międzynarodowej – UE wzmocni swoją zdolność reagowania na cyberataki, wprowadzając ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne wspierające strategiczne ramy zapobiegania konfliktom i stabilizacji w cyberprzestrzeni. Zostanie to połączone z wysiłkami na rzecz budowania nowych zdolności służących wspieraniu państw trzecich w walce z zagrożeniami cybernetycznymi[19].

9 kwietnia 2019 r. Rada przyjęła rozporządzenie zwane aktem o cyberbezpieczeństwie[20], które ustanowiło system certyfikacji na poziomie unijnym oraz zmodernizowaną agencję UE ds. cyberbezpieczeństwa zastępującą ENISA. Ustanowiła też przepisy, które pozwalają nakładać unijne ukierunkowane środki ograniczające, by zapobiegać cyberatakom stanowiącym zewnętrzne zagrożenie Unii lub jej państw członkowskich i reagować na nie. Dzięki tej decyzji UE po raz pierwszy będzie mogła nakładać sankcje na osoby lub podmioty, które:

- odpowiadają za dokonanie lub próby dokonania cyberataków,
- zapewniają w tym celu wsparcie finansowe, techniczne lub materialne,
- angażują się w te działania w inny sposób.

W ramach tej samej reformy UE wprowadziła także przepisy, na których mocy powstało Europejskie Centrum Badań Naukowych i Kompetencji w dziedzinie Cyberbezpieczeństwa wspierane przez sieć krajowych ośrodków koordynacyjnych. Struktury te pomogą zabezpieczyć jednolity rynek cyfrowy (art. 114 TFUE) i zwiększyć autonomię UE w dziedzinie cyberbezpieczeństwa. Ponadto UE może wymierzać sankcje wobec osób lub podmiotów unijnych, a także przeciwko państwom spoza UE lub organizacjom międzynarodowym, jeżeli uzna to za konieczne do osiągnięcia celów wspólnej polityki zagranicznej i bezpieczeństwa.

[19] Ibidem.

[20] Regulation of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (EU) no 526/2013 (CYBERSECURITY ACT), Dok. PE-CONS 86/1/18 REV 1(2017/0225 (COD) LEX 1899).

Jednocześnie UE pracuje nad środkami międzysektorowymi, które pomogą eliminować cyberzagrożenia w kilku obszarach naraz. Przykładem są:

- walka z przestępczością zorganizowaną, w tym obszarze cyberprzestępczość została uznana za jeden z 10 priorytetów na lata 2018–2021,
- wspólna polityka zagraniczna i bezpieczeństwa, realizacja jej celów zależy również od udanego zapobiegania cyberatakom,
- cyberobrona − UE zaktualizowała przepisy cyberobronne, uwzględniając ewoluujące wyzwania w zakresie bezpieczeństwa[21].

Najnowszym posunięciem w polityce cyberbezpieczeństwa jest wydanie *Białej Księgi* z 2020 r. dotyczącej sztucznej inteligencji (AI) i cyfryzacji, która ma stanowić klucz do zwalczenia cyberterroryzmu i osiągnięcia ładu klimatycznego przez doskonalenie AI[22]. To element konieczny pozwalający na utrzymanie jednolitego rynku UE przez badania naukowe, innowacje i wdrożenie do grudnia 2020 r. skoordynowanego planu działań w ramach programów *Cyfrowa Europa* oraz *Horyzont Europa* na lata 2021−2027[23].

Opracowanie planu szybkiego reagowania państw członkowskich umożliwi natychmiastową, skuteczną i skoordynowaną reakcję w przypadkach wystąpienia ataków cybernetycznych na dużą skalę. Pogłębienie współpracy międzynarodowej UE ma celu wzmocnienie zdolności reagowania na cyberataki, wprowadzając ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne wspierające strategiczne ramy zapobiegania konfliktom i stabilizacji w cyberprzestrzeni. Zostanie to połączone z wysiłkami na rzecz budowania nowych zdolności służących wspieraniu państw trzecich w walce z zagrożeniami cybernetycznymi[24].

3. DYREKTYWA NIS W PRAWIE POLSKIM

Polityka i strategia zawsze określają byt i rozwój państwa, co pozwala na spostrzeżenie, że dzieje się to w związku z umiejętnością jego zapewnienia w stosunku do wartości, potrzeb, interesów, celów, które warunkują realizację polityki i strategii państwa w perspektywie krótko-, średnio- i długoterminowej. Dzięki tym umiejętnościom lub ich brakowi państwo generuje w czasie i przestrzeni swoją siłę, potęgę, wpływ, który wywiera na pozostałe podmioty państwa i ich organizacje, społeczności i społeczeństwo, naród. Polityka i strategia są przy tym uwarunkowane przez wyzwania, zagrożenia, szanse dla bytu i rozwoju podmiotu, czyli jego wizji, misji i celów, które podejmuje bądź realizuje.

[21] https://www.consilium.europa.eu/ (dostęp: 18.01.2021 r.).

[22] *Biała Księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania* [COM(2020) 65 final].

[23] https://europa.eu (dostęp: 18.01.2021 r.).

[24] https://ec.europa.eu/digital-single-market/en/cyber-security (dostęp: 13.06.2020 r.).

Trychotomia zjawiska cyberprzestępstwa polega na połączeniu trzech czynników zapobiegania zjawisku cyberprzestępczości, ścigania sprawców przestępstw i egzekwowania skuteczności prawa. Jak łatwo zauważyć przewagą cyberprzestępców są ich umiejętności, znajomość technologii i innowacyjnych rozwiązań cyberprzestrzeni. Z kolei słabością ofiar przestępstw terrorystycznych jest ich niewiedza i chęć posiadania ochrony (zabezpieczeń) internetowych. Cyberprzestępcy tak długo będą działać, jak długo poczynione nakłady (koszty) będą niższe od uzyskanych przychodów.

Jak słusznie zauważa Marek Górka[25] nie każdy incydent może zostać zaklasyfikowany jako ten, który ma istotne znaczenie społeczno-polityczne. Zadaniem badawczym jest więc odróżnienie tych incydentów cybernetycznych o charakterze politycznym od pozostałych ataków, które mają charakter ekonomiczny bądź społeczny. Uwzględniony zostaje w tym miejscu zestaw danych w oparciu jako perspektywę intensywności działań cyfrowych, postrzeganych w tym przypadku o pięć wskaźników pozwalających przyporządkować zaistniałe cyberincydenty do zbioru działań o charakterze politycznym. Uwzględnienie tych czynników w kontekście prowadzonych ataków przez państwo lub podmioty prywatne, wypełnia zarówno dotychczasową lukę empiryczną, jak i pozwala na bardziej wszechstronną analizę zjawisk zachodzących w zakresie polityki bezpieczeństwa cybernetycznego.

Pierwszym, pomocnym wskaźnikiem w zaproponowanej selekcji jest informacja na temat źródła pochodzenia cyberataku. Identyfikując cyberatak o charakterze politycznym warto pamiętać, że jest on elementem składowym interakcji, która zachodzi między określonymi podmiotami będącymi w stanie konfliktu. Ta forma rywalizacji bywa więc przedłużeniem oraz odzwierciedleniem rywalizacji pomiędzy podmiotami politycznymi.

We wszystkich państwach UE 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 z dnia 6 lipca 2016 r.[26], zwana dalej dyrektywą NIS, jest wprowadzona szerzej, niż wynika to z jej zapisu. W przypadku Polski uwzględniono dodatkowe sektory takie, jak energetyczny i węglowy, a także związane ze zdrowiem i bakowością. Zgodnie z art. 1 ustawy i art. 1 dyrektywy 2016/1148 nie ma ona zastosowania wobec przedsiębiorców telekomunikacyjnych i dostawców usług zaufania, którzy zostali już objęci europejskimi i krajowymi wymaganiami sektorowymi z zakresu cyberbezpieczeństwa[27].

[25] Górka M., 2019: *Istota bezpieczeństwa cybernetycznego w polityce państw Grupy Wyszehradzkiej w latach 2013–2017*, Toruń, s. 154.

[26] Dz.Urz. UE L 194, s. 1.

[27] Postanowienie NSA z dnia 23.04.2020 r. w sprawie II GZ 97/20; wyrok WSA z 11.12.2019 r. w sprawie VI SA/Wa 1436/19.

W przepisach ogólnych, szczególnie art. 2. ustawy określono zakres regulacji, słowniczek pojęć ustawowych, katalog podmiotów tworzących krajowy system cyberbezpieczeństwa oraz cele projektowanej ustawy. Ustawa określa organizację polskiego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy, zakres oraz tryb stanowienia *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej*[28].

Należy również zauważyć, że zgodnie z art. 288 TL[29] transpozycja przepisów wprost co do dyrektywy do prawa krajowego nie jest rozwiązaniem przyjętym przez ustawodawcę unijnego. Priorytetem jest spójność krajowego systemu prawa z prawem unijnym.

Definicja bezpieczeństwa informacji w dyrektywie NIS rozszerzyła trzy podstawowe atrybuty: poufność, integralność i dostępność o czwarty atrybut – autentyczność, która polega na tym, że podmiot jest tym, za kogo się podaje[30].

Ustawa wprowadza pojęcie sektorowego zespołu cyberbezpieczeństwa[31], czyli zespołu ustanowionego przez organ właściwy dla danego sektora lub podsektora wymienionego w załączniku do ustawy, odpowiedzialnego za obsługę lub wsparcie obsługi incydentów w danym sektorze lub podsektorze.

Polski ustawodawca zdefiniował cyberbezpieczeństwo w art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa jako odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Dyrektywa NIS przyjęła nową definicję systemów i sieci teleinformatycznych obejmującą:

- sieci łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE;
- wszelkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych lub dane cyfrowe przechowywane, przetwarzane, odzyskiwane lub przekazywane w celu ich eksploatacji, użycia, ochrony i utrzymania[32].

[28] Szczegóły: rozdział 13 ustawy z dnia 5.07. 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2020 poz. 1369)

[29] Dawny art. 249 TUE dotyczący hierarchii źródeł prawa wtórnego.

[30] Por.: art. 4 pkt 2 dyrektywy NIS i art. 2 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa.

[31] Zob.: art. 9 ust. 1 pkt 3. Sektorowe zespoły zostały uregulowane w art. 44 ustawy o krajowym systemie cyberbezpieczeństwa.

[32] Istniejąca w ustawie o świadczeniu usług elektronicznych definicja systemu teleinformatycznego zawierała pierwszy i drugi element definicji, nie objęła jednak danych cyfrowych. W tym celu należało opracować definicję obejmującą również dane cyfrowe (por.: art. 2 pkt 14 ustawy).

Należy też wskazać na definicje związane z szacowaniem ryzyka i zagrożeniami. Ustawa definiuje ryzyko[33], szacowanie ryzyka[34], zarządzanie ryzykiem[35], zagrożenie cyberbezpieczeństwa[36] i podatność[37].

W rozumieniu ustawy i dyrektywy NIS istnieją trzy usługi cyfrowe:

- internetowa platforma handlowa,
- przetwarzanie w chmurze,
- wyszukiwarka internetowa[38].

[33] Art. 2 pkt 12 ustawy. Treść definicji ryzyka przyjętej na gruncie polskiej ustawy różni się od sposobu interpretacji tego pojęcia zawartego w art. 4 pkt 9 dyrektywy NIS. Zgodnie ze sformułowaną w art. 4 pkt 9 dyrektywy NIS definicją „ryzyko" oznacza „każdą dającą się racjonalnie określić okoliczność lub zdarzenie, które ma potencjalny niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych". Ustawodawca unijny powiązał zatem definicję ryzyka z pojęciem zagrożenia, a nawet dokonał utożsamienia tych pojęć.

[34] Art. 2 pkt 13 ustawy. Proces szacowania ryzyka polega na określeniu możliwości wystąpienia zagrożeń oraz potencjalnych strat. W związku z tym takie oszacowanie uwzględnia dwa kluczowe parametry: możliwość lub prawdopodobieństwo realizacji zagrożenia i jego skutki finansowe. Przy wyborze metody do tego służącej istnieją w zasadzie dwie możliwości:

- metoda ilościowej analizy ryzyka, w której operuje się miarą zdarzenia losowego – prawdopodobieństwem wyrażonym liczbą z przedziału [0,1],
- metoda jakościowa analizy ryzyka, gdzie operuje się opisowymi, arbitralnie dobieranymi miarami wyrażającymi możliwość zajścia zdarzenia. Szerzej: K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008, s. 83 i n.

[35] Art. 2 pkt 19 ustawy. Zarządzanie ryzykiem jest procesem permanentnym, ponieważ ryzyko ma charakter dynamiczny. Należy się liczyć z tym, że zachodzą różne zdarzenia mogące mieć wpływ na jego poziom i rodzaj. Por.: Berlin A., Brotherson L., 2018: *Bezpieczeństwo defensywne. Podstawy i najlepsze praktyki*, Gliwice, s. 22; Cygan M., Geilke M., 2015: *Tworzenie systemu zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001:2014*, Wrocław, s. 17.

[36] Art. 2 pkt 17 ustawy.

[37] Art. 2 pkt 11 ustawy. Na gruncie dyrektywy NIS występowanie zagrożenia jest tożsame z istnieniem ryzyka, podczas gdy ryzyko w ujęciu ustawodawcy polskiego oznacza wypadkową występującego potencjalnie zagrożenia i konsekwencji (szkody, krzywdy), jakie może ono wywołać. Ustawodawca polski wymaga zatem, by ustalenie istnienia ryzyka było wynikiem permanentnie realizowanego procesu polegającego na filtrowaniu cyberprzestrzeni w poszukiwaniu zdarzeń, a następnie dokonywaniu ich selekcji i oceny pod kątem skutków, jakie zdarzenia te mogą wywołać dla realizacji celów instytucji. Polski ustawodawca – jak należy sądzić – stoi na stanowisku, że zdarzenie samo w sobie nie stanowi ryzyka, ryzyko może bowiem powstawać dopiero wówczas, gdy przewidywalne konsekwencje zdarzeń będą stanowić naruszenie wartości istotnych dla instytucji.

[38] Do ustalenia zakresu pojęcia „usługi cyfrowe" niezbędne staje się uwzględnienie zarówno postanowień dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz. Urz. UE L 178, s. 1), a także dyrektywy 98/34/WE Parlamentu Europejskiego i Rady z 22 czerwca 1998 r. ustanawiającej procedurę udzielania informacji w zakresie norm i przepisów technicznych (Dz.Urz. UE L 204, s. 37 ze zm.). Do celów zawartej w tej dyrektywie definicji wskazano, że użyte w niej sformułowanie „na odległość" oznacza usługę świadczoną bez równoczesnej obecności stron, natomiast wyrażenie „drogą elektroniczną" oznacza, że usługa jest przesyłana pierwotnie i otrzymywana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (włącznie z kompresją cyfrową) oraz przechowywania danych, i która jest całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, odbiornika radiowego, środków optycznych lub innych środków

Definicja usługi przetwarzania w chmurze została skonstruowana na podstawie terminów technologicznych, a nie prawnych, dlatego należy odczytywać ją razem z motywami dyrektywy NIS i definicją usługi cyfrowej. Usługa przetwarzania w chmurze dotyczy tylko usług świadczonych przez dany podmiot swoim klientom. Wyłączone są zatem przypadki chmury prywatnej, która jest usługą świadczoną wewnątrz organizacji. Z kolei w art. 3 zostały określone cele polskiego systemu cyberbezpieczeństwa, którymi będą niezakłócone świadczenie usług kluczowych i usług cyfrowych, osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.

Artykuł 4 wskazuje podmioty, które obejmuje krajowy system cyberbezpieczeństwa, a więc podmioty zobowiązane, podmioty realizujące techniczne, organizacyjne i administracyjno-regulacyjne zadania w systemie, jednostki sektora finansów publicznych. System będzie zatem obejmować m.in. operatorów usług kluczowych, dostawców usług cyfrowych, zespoły CSIRT, sektorowe zespoły cyberbezpieczeństwa, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe ds. cyberbezpieczeństwa, pojedynczy punkt kontaktowy ds. cyberbezpieczeństwa, pełnomocnika rządu ds. cyberbezpieczeństwa i kolegium ds. cyberbezpieczeństwa, instytuty badawcze, a także jednostki sektora finansów publicznych objęte zakresem ustawy. W przepisach szczegółowych zostały natomiast opisane uprawnienia i obowiązki tych podmiotów, jak również zakres przypisanej im odpowiedzialności[39].

Uwzględniono również konieczność objęcia ustawą niektórych podmiotów wymienionych w art. 9 pkt 14 ustawy o finansach publicznych (tzw. inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych). Należą do nich: Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej. Ustawą zostaną również objęte spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej[40].

---

elektromagnetycznych. Przez świadczenie usługi „na indywidualne żądanie odbiorcy usług" należy natomiast rozumieć, że usługa świadczona jest przez przesyłanie danych na indywidualne żądanie (art. 2 pkt 2 dyrektywy technicznej).

[39] W rozdziale 6. zostały wskazane uprawnienia i wymagane kompetencje CSIRT, pełniące najważniejsze funkcje techniczne w systemie, obejmujące m.in. koordynację i obsługę poważnych, istotnych i krytycznych incydentów. Opisane zostały również sposoby realizacji współpracy z operatorami usług kluczowych, dostawcami usług cyfrowych, podmiotami publicznymi i sektorowymi zespołami cyberbezpieczeństwa. W przepisach szczegółowych zostały opisane także role o charakterze administracyjno-regulacyjnym, role oraz zależności, które powstają między organem właściwym ds. cyberbezpieczeństwa a operatorem usługi kluczowej.

[40] Dz.U. z 2017 r. poz. 827 z późn. zm.

4. WNIOSKI

Częstotliwość oraz rozwój nowych technologii i zagrożeń znacznie przewyższa implementację prawodawstwa UE. Procedury Unii nie zostały zaprojektowane z myślą o erze cyfrowej. Opracowywanie innowacyjnych i elastycznych procedur w celu zapewnienia polityki i ram prawnych, które są odpowiednie do wyznaczonego celu strategicznego, aby lepiej przewidywać i kształtować przyszłość, jest zadaniem kluczowym. Mimo dążenia do większej spójności ramy prawne dotyczące cyberbezpieczeństwa pozostają niekompletne.

Na podstawie przeprowadzonej analizy należy stwierdzić, że skuteczność działań podejmowanych przez organy UE w zakresie polityki cyberterrorystycznej zależy od rodzaju instrumentów będących w dyspozycji UE i państw członkowskich oraz podstawy prawnej odpowiednich regulacji. Na efektywność danego instrumentu wpływa jego prosty mechanizm funkcjonowania, sposób jego uchwalenia, zakres jego obowiązywania wobec państw członkowskich, bezpośredniość skutku bądź jego brak oraz mechanizmy kontroli nad jego przestrzeganiem[41].

Kolejnym problemem jest brak powszechnie stosowanych, znormalizowanych sposobów poziomej oceny bezpieczeństwa oprogramowania, oprócz niektórych metod przeprowadzania testów penetracyjnych lub przeglądu kodu. Sytuacja wygląda gorzej, jeśli weźmiemy pod lupę sposób certyfikacji bezpieczeństwa oprogramowania.

Patrząc z ogólnej perspektywy na realizację polityki cyberbezpieczeństwa i działania podejmowane przez UE, ocena jest raczej negatywna. Najbardziej prawdopodobnym powodem takiego rozpoznania jest to, że europejskie ambicje i oczekiwania w walce z cyberterroryzmem są zbyt wysokie w porównaniu z rzeczywistością. Chociaż przygotowano stosowne przepisy mające służyć przeciwdziałaniu cyberterroryzmowi (NIS czy RODO), problemem jest niechęć do współpracy między państwami członkowskimi a UE, zwłaszcza gdy jest od nich wymagana rezygnacja z kompetencji na szczeblu państwowym w zakresie cyberbezpieczeństwa, oraz nieprecyzyjny podział kompetencji między Unię a państwa członkowskie.

Polityka cyberbezpieczeństwa Unii Europejskiej powinna zatem zmierzać do wskazania nowych przyczyn tego zjawiska oraz stworzenia zintegrowanego systemu obronnego cyberprzestrzeni zarówno na terenie poszczególnych państw, jak i całej UE. Wprawdzie dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[42] w dniu 6 lipca 2016 r. (zwana dalej dyrektywą 2016/1148 lub dyrektywą NIS) zobowiązała wszystkie państwa członkowskie UE do zagwarantowania minimalnego poziomu

[41] Por.: *Challenges to effective EU cybersecurity policy 2019*, https://www.eca.europa.eu/ (dostęp: 30.07.2020 r.).

[42] Dz.Urz. UE L 194 z 19.07.2016 r., s. 1.

zdolności krajowych w dziedzinie cyberbezpieczeństwa przez ustanowienie organów właściwych oraz pojedynczego punktu kontaktowego ds. cyberbezpieczeństwa, powołanie zespołów reagowania na incydenty komputerowe (CSIRT) oraz przyjęcie państwowych strategii w zakresie cyberbezpieczeństwa, jednak w obecnych uwarunkowaniach należałoby się posługiwać zarówno wysoce wyspecjalizowanymi narzędziami informatycznymi, jak i lepszymi instytucjami na szczeblu unijnym. Ponadto zbyt wąskie kompetencje w tej dziedzinie ENISY czy Eurojustu nie dają szansy na szybką współpracę w obszarze zwalczania cyberterroryzmu. Wprowadzenie odpowiednich przepisów prawnych z pewnością zmniejszyłoby ryzyko wystąpienia tego zjawiska, jednak go nie zniweluje. Trudność leży głównie po stronie prawnej.

Należy pamiętać, że nawet najlepsze zabezpieczenia techniczne i regulacje prawne na nic się zdadzą, jeżeli nie będą iść w parze z działaniem odpowiednich instytucji i rozwagą użytkowników. I w tym przypadku potwierdza się reguła, że człowiek stanowi najważniejsze, a zarazem najsłabsze ogniwo w systemie zabezpieczeń. Brak spójnych ram zarządzania cyberbezpieczeństwem osłabia zdolność społeczności międzynarodowej do reagowania na cyberataki i ich ograniczania. Dlatego należy wypracować konsensus w sprawie takich ram zarządzania, które są najlepszym odzwierciedleniem interesów i wartości UE.

Należy również zauważyć, że zgodnie z art. 288 TL[43] transpozycja przepisów wprost z dyrektywy do prawa krajowego nie jest rozwiązaniem przyjętym przez ustawodawcę unijnego. Priorytetem jest spójność krajowego systemu prawa z prawem unijnym. Definicja bezpieczeństwa informacyjnego w dyrektywie NIS natomiast rozszerzyła podstawowe trzy atrybuty, tzn. poufność, integralność i dostępność, o czwarty, którym jest autentyczność, czyli właściwość polegająca na tym, że podmiot jest tym, za kogo się podaje[44]. Warto wspomnieć, że normy prawne są skuteczniej egzekwowane na poziomie prawa unijnego niż międzynarodowego.

Należy stwierdzić, że wprowadzenie mechanizmów współpracy dyrektywy 2016/1148 (NIS) na dwóch poziomach − technicznym i polityczno-strategicznym, co było właściwym i koniecznym posunięciem ze strony UE. Dyrektywa nałożyła także na państwa członkowskie obowiązek przyjęcia narodowej strategii bezpieczeństwa sieci i informacji, w której określone zostały m.in. narodowe cele i priorytety w dziedzinie cyberbezpieczeństwa, role i obowiązki organów administracji publicznej w procesie osiągania wyznaczonych celów, zasady współpracy sektorów publicznego i prywatnego oraz krajowa analiza ryzyka i zadania w zakresie edukacji na rzecz cyberbezpieczeństwa.

Przepisy dyrektywy umożliwiły utworzenie zarówno scentralizowanego systemu na poziomie państwowym, jak i podzielenie kompetencji między różne

[43] Dawny art. 249 TUE dotyczący hierarchii źródeł prawa wtórnego.

[44] Por.: art. 4 pkt 2 dyrektywy NIS i art. 2 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa.

podmioty wymieniające informacje za pomocą wypracowanych mechanizmów współpracy. Dyrektywa zobowiązała także wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu krajowych zdolności w dziedzinie bezpieczeństwa teleinformatycznego. Dała organom publicznym konkretne narzędzie do przeciwdziałania i reakcji na incydenty w cyberprzestrzeni. Było to możliwe m.in. dzięki nałożonym obowiązkom raportowania, przygotowania krajowych strategii, skoordynowania przepływu informacji czy też zinstytucjonalizowania współpracy CSIRT.

Title: Reform of the European Union cybersecurity policy

Abstract: The EU Global Strategy for Foreign and Security Policy was adopted by the European Council on June 28, 2016. It defines the common interests of the EU and its member states. It was based on the following objectives: security of citizens and territory, prosperity, democracy, global order, which are to lead to the creation of a credible, reactive and cohesive European Union. The principles which the European Union began to follow are unity, cooperation with others, responsibility, and deepening external partnerships.
It is worth noting that cybersecurity in the European Union is a prerogative of the Member States unlike cyberterrorism which is a shared competence. Nevertheless, the EU has a key role to play in creating the conditions for the ability of Member States to improve, cooperate and build trust.
This article will attempt to demonstrate that the effectiveness of actions taken by European Union bodies in the field of cyber terrorism depends on the type of instruments at the disposal of the EU and the Member States and the legal basis of the relevant regulations. The problem is that there are legal inaccuracies and interpretation discrepancies in the provisions of legal regulations at the EU level regarding the division of competences regarding cyberspace protection, which in fact lead to a delay in the establishment of mutual cooperation between the EU and the Member States.

Keywords: cybersecurity, European Union, NIS directive, strategy, harmonization

BIBLIOGRAFIA

1. Barfield W., 2015: *Cyber-Humans. Our Future with Machines*, New York.
2. Berlin A., Brotherson L., 2018: *Bezpieczeństwo defensywne*, *Podstawy i najlepsze praktyki*, Gliwice.
3. *Biała Księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania* [COM(2020) 65 final].
4. Biscop S., 2019: *The EU Global Strategy 2020*, Security Policy Brief, nr 108.
5. *Challenges to effective EU cybersecurity policy 2019*, https://www.eca.europa.eu/ (dostęp: 30.07.2020 r.).
6. *Commission Staff Working Document Assessment of the EU 2013 Cybersecurity Strategy, 2017*, źródło: https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF (dostęp: 18.01.2021 r.).
7. Cygan M., Geilke M., 2015: *Tworzenie systemu zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001:2014*, Wrocław.
8. Dyrektywa Parlamentu Europejskiego i Rady 2000/31/WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu

elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.Urz. UE L 178).

9. Dyrektywa Parlamentu Europejskiego i Rady 2016/1148/UE z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE UE L 194 z 19.07.2016 r.).
10. Dyrektywy Parlamentu Europejskiego i Rady 98/34/WE z dnia 22 czerwca 1998 r. ustanawiającej procedurę udzielania informacji w zakresie norm i przepisów technicznych (Dz.Urz. UE L 204, s. 37 ze zm.).
11. Górka M., 2019: *Istota bezpieczeństwa cybernetycznego w polityce państw Grupy Wyszehradzkiej w latach 2013–2017*, Toruń.
12. http://www.consilium.europa.eu/pl/policies/cyber-security/ (dostęp: 3.02.2021 r.).
13. https://ec.europa.eu/digital-single-market/en/cyber-security (dostęp: 3.02.2021 r.).
14. https://eeas.europa.eu/top_stories/pdf/eugs_pl_.pdf. (dostęp: 3.02.2021 r.).
15. Ilves L.K. et al., 2016: *European Union and NATO global cybersecurity challenges. A way Forward,* PRISM, vol. 6, nr 2.
16. Komunikat Komisji, 2017: *State of the Union 2017: The Commission scales up its response to cyberattacks,* źródło: europa.eu/rapid/press-release_MEMO-17-3194_en.pdf (dostęp: 19.01.2021 r.).
17. Kowalkowski S.(red.), 2011: *Niemilitarne zagrożenia bezpieczeństwa publicznego*, Warszawa.
18. Liderman K., 2008: *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa.
19. Oleksiewicz I., 2016: *Polskie prawo karne w zakresie walki z cyberprzestępczością na tle standardów prawa UE*, [w:] Pietraś M., Chałupczak H., Misiągiewicz J. (red.), 2016: *Europa Środkowo-Wschodnia w procesie transformacji i integracji. Wymiar bezpieczeństwa,* Zamość.
20. Pagallo U., 2013: *The laws of robots: crimes, contracts, and torts*, New York.
21. *Plan implementacji w dziedzinie bezpieczeństwa i obronności* [COM(2016) 950 final, 30.11.2016 r.].
22. Postanowienie NSA z dnia 23.04.2020 r. w sprawie II GZ 97/20; wyrok WSA z 11.12.2019 r. w sprawie VI SA/Wa 1436/19.
23. *Program sztokholmski – otwarta i bezpieczna Europa dla dobra i ochrony obywateli,* Bruksela, 2 grudnia 2009 r. (17024/09); *Przestrzeń wolności, bezpieczeństwa i sprawiedliwości: Plan działań służący realizacji programu sztokholmskiego* (COM(2010) 171).
24. Regulation of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (EU) no 526/2013 (CYBERSECURITY ACT), Dok. PE-CONS 86/1/18 REV 1(2017/0225 (COD) LEX 1899).
25. Schreier F., 2015: *On cyberwarfare,* DCAF Horizon, working paper.
26. Ustawa z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz.U. z 2017 r. poz. 827 z późn. zm.).
27. Wróblewska-Łysik M., 2016: *Europejska Strategia Globalna a możliwości współpracy Unii Europejskiej z NATO po szczycie w Warszawie*, Bezpieczeństwo Narodowe, nr I–IV.