Krzysztof Wąsik*

Międzynarodowe regulacje prawne dotyczące cyberprzestrzeni

Streszczenie

Niniejszy artykuł ma na celu przedstawienie odmiennych podejść państw na świecie do regulacji prawnych cyberprzestrzeni. Utworzenie jednolitego systemu prawnego dotyczącego wirtualnej przestrzeni będzie trudnym procesem ze względu na duże konflikty interesów. Międzynarodowe organizacje takie jak Unia Europejska (UE) czy Pakt Północnoatlantycki (NATO), zrzeszające państwa, które mają podobną wizję świata oraz funkcjonowania, przyczyniają się do ujednolicenia norm prawnych regulujących cyberprzestrzeń w poszczególnych krajach. Z drugiej strony, ogólnikowe inicjatywy największej organizacji na świecie – Organizacji Narodów Zjednoczonych (ONZ), a także brak implementacji nowo przyjmowanych regulacji przez wszystkie kraje członkowskie, niestety, spowalniają walkę z cyberterroryzmem oraz cyberprzestępstwami, które mają charakter transgraniczny. Wszystkie kraje na świecie zwiększają nakłady finansowe na poprawę sieci informatycznych, tworzą nowe instytucje zajmujące się zwalczaniem zagrożeń w przestrzeni cyfrowej oraz dostosowują prawo do bardzo szybko zmieniającego się świata.

Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, prawo międzynarodowe, organizacje międzynarodowe

* Krzysztof Wąsik, Katedra Bezpieczeństwa Wewnętrznego, Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej w Warszawie.

W dobie wszechobecnej globalizacji oraz szybko zmieniającego się świata państwa i organizacje międzynarodowe zauważają bardzo duże zagrożenia wynikające z dynamicznie rozwijających się problemów w wirtualnym świecie. Często rządy, parlamenty krajów oraz poszczególne organizacje nie nadążają z tworzeniem aktów normatywnych, żeby uregulować to, co dzieję się w cyberprzestrzeni. Jest to związane z tym, że prawo międzynarodowe, regionalne i krajowe nie zawsze podąża za innowacjami technologicznymi oraz sektorem prywatnym. Niniejszy artykuł ma na celu przedstawienie międzynarodowych aktów prawnych wybranych organizacji międzynarodowych oraz państw jako środków uregulowania sposobów korzystania z cyberprzestrzeni i zapewnienia bezpieczeństwa w danej sferze podmiotom rządowym i prywatnym.

Cyberprzestrzeń została zdefiniowana ustawowo jako przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania) zapewniające przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne[1]. W powstałych dokumentach napisanych przez organizacje międzynarodowe czy poszczególne państwa jest bardzo dużo definicji cyberprzestrzeni. Obecnie nie ma możliwości, żeby zaszeregować prawo cyberprzestrzeni jako samodzielnej gałęzi prawa, mimo wydawanych dokumentów o charakterze międzynarodowym, regionalnym i krajowym. Trzeba pamiętać, że na wyżej wspomnianych poziomach występuje wiele rozbieżnych i często różniących się od siebie definicji. Prawo cyberprzestrzeni jest powiązane ze wszystkimi gałęziami prawa, a w szczególności z prawem cywilnym, karnym, ochroną danych osobowych i prawami człowieka. Bardzo często definicje te się różnią (np. w zakresie części składowych cyberprzestrzeni), lecz łączy je jedno – wirtualny świat, który jest przeniesiony na sferę życiową. Wraz z rozwojem popularności komputerów, cyfryzacji i dostępem do internetu społeczność międzynarodowa dostrzegła brak odpowiednich regulacji prawnych cyberprzestrzeni. Międzynarodowy charakter cyberprzestrzeni spowodował, że korzystanie z tego środka komunikacji może przenieść użytkownika w ciągu kilku sekund do innego kraju. Trzeba pamiętać, że cyberprzestrzeń nie może być miejscem, w którym nie funkcjonuje prawo. Coraz większa liczba użytkowników oraz szybki powszechny dostęp do przestrzeni cyfrowej powoduje również zwiększoną liczbę zagrożeń,

1 Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, t.j., Dz.U. 2022, poz. 2091, art. 2, ust. 1b.

które występują w tej przestrzeni. Wszystkie kraje na świecie oraz organizacje międzynarodowe dążą do uregulowania sfery cyberprzestrzeni. Czynniki, które napędzają poszczególne kraje do ratyfikacji umów międzynarodowych lub tworzenia własnego krajowego porządku prawnego, to rozwój cyberprzestępczości oraz cyberterroryzm. Dynamiczny rozwój nowych technologii, pojawienie się nowych urządzeń (smartwatche, drony, tablety, smartfony), stron internetowych, programów i aplikacji powoduje, że cyberprzestępcy poszukują i wykorzystują nowe, innowacyjne przestępcze metody działania. W ten sposób nierzadko wyprzedzają organy ścigania, posługują się zaawansowanym technologicznie sprzętem i umiejętnościami. Z tego względu wszystkie organizacje międzynarodowe i rządy krajów zaczęły podejmować odpowiednie kroki w celu regulacji nowego, nieznanego wcześniej zjawiska – cyberprzestrzeni[2]. Nowe możliwości spowodowały ustanowienie nowych przepisów, które zaczęły regulować korzystanie z wirtualnego świata. Wydanie poszczególnych dokumentów normatywnych o charakterze międzynarodowym zapoczątkowało utworzenie drogi legislacyjnej dla krajów, które zaczęły implementować nowy porządek prawny w swoich krajowych przepisach[3].

Za pierwszy poważny atak w świecie cyber na funkcjonowanie państwa należy uznać atak hakerski na Estonię. Do paraliżu, ale również pokazania ogromnej słabości w przestrzeni cyber doszło w 2007 roku. Podczas zamieszek po zmianie miejsca pomnika radzieckiego upamiętniającego żołnierzy Armii Czerwonej jednocześnie doszło do ataków hakerskich na strony internetowe najważniejszych instytucji państwowych[4]. Od tego momentu Estonia zaczęła podejmować kroki w celu ochrony swojego kraju, dzięki czemu stała się pionierem cyfrowego państwa w Europie i na świecie. Rozbudowana sieć informatyczna spowodowała, że Estonia stała się krajem najbardziej rozwiniętym informatycznie w Europie. Po atakach w Estonii NATO stworzyło najważniejszą jednostkę odpowiedzialną za cyberobronę całego Sojuszu Północnoatlantyckiego – Centrum Doskonalenia Cyberobrony NATO (NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE). Ponadto należy pamiętać o atakach na Litwę czy Gruzję. Za tymi atakami zawsze stała

2 M. Karpiuk, *Cybersecurity as an element in the planninc activities of public administration*, „Cybersecurity and Law" 2021, nr 1, s. 48.

3 K. Chałubińska-Jentkiewicz, A. Brzostek, *Strategie cyberbezpieczeństwa współczesnego świata*, Warszawa 2021, s. 12.

4 J. Dereń, A. Rabiak, *NATO a aspekty bezpieczeństwa w cyberprzestrzeni* [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Warszawa 2004, s. 210.

Federacja Rosyjska, która chce wywierać wpływ na terenach wcześniej od niej uzależnionych i pokazać, że pamięta o swoich byłych terytoriach. Już od lat 90. wieku XX wrzało na linii Izrael–Syria, Izrael–Iran, a tocząca się od 1952 roku wojna pomiędzy Koreami przeniosła się do wirtualnego świata. Należy wspomnieć, że w roku 2014 po emisji prześmiewczego filmu o przywódcy Korei Północnej Kim Dzong Unie wyciekły dane użytkowników korzystających z różnych aplikacji firmy Sony, która wyprodukowała ten film, oraz doszło do zaatakowania serwerów. Ataki na Colonial Pipeline w Stanach Zjednoczonych Ameryki spowodowały brak dystrybucji paliw do 19 stanów, co fizycznie zatrzymało w niektórych z nich funkcjonowanie. Opisane powyżej poszczególne ataki miały miejsce kilka lat temu, ale ich cele oraz zadania, niestety, są wciąż aktualne.

Rada Europy/Unia Europejska

Pierwszą próbę unormowania wirtualnej przestrzeni w Europie podjęła Rada Europy 23 listopada 2001 roku, kiedy w Budapeszcie została przyjęta konwencja o cyberprzestępczości[5]. Innowacyjność oraz istotna tematyka spowodowały, że do konwencji przystąpiły kraje spoza Rady Europy. Dokument ten zobowiązuje państwa do zaliczenia wirtualnych przestępstw do przestępstw, które muszą się znaleźć w jurysdykcji krajowej. Konwencja kategoryzuje cztery rodzaje przestępstw:

1. Przeciwko poufności, integralności i dostępności danych informatycznych i systemów (art. 2 – nielegalny dostęp, art. 3 – nielegalne przechwytywanie danych, art. 4 – naruszenie integralności danych, art. 5 – naruszenie integralności systemu, art. 6 – niewłaściwe wykorzystywanie urządzeń);

2. Przestępstwa komputerowe (art. 7 – fałszerstwo komputerowe, art. 8 – oszustwo komputerowe);

3. Przestępstwa ze względu na charakter zawartych informacji (art. 9 – przestępstwa związane z pornografią dziecięcą);

4. Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych (art. 10 – przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych).

5 Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., Dz.U. 2015, poz. 728.

W podobny sposób czyny wymierzone w bezpieczeństwo cyberprzestrzeni definiuje prawo Unii Europejskiej, tzw. dyrektywa o atakach na systemy informatyczne[6]. Dyrektywa 2013/40/UE zobowiązuje państwa członkowskie Unii Europejskiej do podjęcia kroków umożliwiających karanie za poszczególne czyny we wszystkich krajach UE.

Pod koniec grudnia 2020 roku Komisja Europejska przedstawiła nową strategię cyberbezpieczeństwa UE (Joint communication to The European Parliament and The Council. The EU's Cybersecurity Strategy for the Digital Decade) i uchyliła dyrektywę 2016/1148 [Directive onmeasures for high common level of cybersecurity across the Union, repealing Directive (UE) 2016/1148][7]. Komisja Europejska w swojej strategii cyberbezpieczeństwa proponuje konkretny zestaw rozwiązań regulacyjnych, inwestycyjnych i politycznych w trzech następujących obszarach:

– odporność, technologiczna suwerenność i przywództwo;

– budowanie zdolności operacyjnych do zapobiegania, odstraszania i reagowania na incydenty w cyberprzestrzeni;

– rozwój globalnej i otwartej cyberprzestrzeni poprzez zacieśnienie współpracy międzynarodowej.

Głównym celem strategii jest wzmocnienie odporności Europy na cyberprzestępstwa oraz pomoc w zapewnieniu dostępu do niezawodnych i wiarygodnych narzędzi cyfrowych wszystkim obywatelom i przedsiębiorstwom. Nowa dyrektywa ma ugruntować pozycję Europy jako lidera w tworzeniu międzynarodowych standardów prawa w obszarze cyberbezpieczeństwa, ochrony dostępu do internetu i budowania globalnego partnerstwa opartego na europejskich wartościach. Motto strategii brzmi: „Zaufanie i bezpieczeństwo w centrum cyfrowej dekady UE"[8]. Najważniejsze zmiany to: utworzenie instytucji odpowiedzialnych za reagowanie na incydenty bezpieczeństwa komputerowego (CSIRT), opracowanie krajowych strategii cyberbezpieczeństwa oraz zapewnienie odpowiedniej współpracy z właściwymi organami CSIRT innych państw członkowskich, wprowadzanie sieci 5G.

6 Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dz. Urz. UE 2013, L 218/8.

7 *Wspólny Komunikat do Parlamentu Europejskiego i Rady. Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę*, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020JC0018&from=EN [dostęp: 20.06.2023].

8 Ibidem.

Nowe przepisy nakładają na kraje UE bardziej szczegółowe zadania w zakresie nadzoru cyberbezpieczeństwa. Poprawiają też egzekwowanie wdrażania nowych praw i obowiązków, w tym poprzez dostosowywanie sankcji, które państwa członkowskie mogą nakładać. Mają również poprawić współpracę między krajami UE, w tym w zakresie incydentów na dużą skalę, pod nadzorem Agencji UE ds. Cyberbezpieczeństwa (ENISA).

Sektor finansowy jest coraz bardziej zależny od oprogramowania, aplikacji i procesów cyfrowych, dlatego UE zdecydowała się na jego ochronę poprzez program DORA[9]. Rozporządzenie weszło w życie i ma zagwarantować odporność bezpieczeństwa sieci i systemów informatycznych firm i instytucji działających w sektorze finansowym, a także kluczowych zewnętrznych dostawców usług związanych z ICT (technologiami informacyjno-komunikacyjnymi) takich jak platformy w chmurze czy usługi analizy danych. Nowo powstałe regulacje mają ochronić i wytrzymać wszelkiego rodzaju zakłócenia i zagrożenia związane z ICT, reagować na nie i przezwyciężać ich skutki. Wymogi zawarte w rozporządzeniu są jednolite we wszystkich państwach członkowskich UE. Głównym celem jest zapobieganie cyberzagrożeniom oraz ich łagodzenie. Pakiet ma wspierać innowacje i upowszechnianie nowych technologii finansowych, a jednocześnie zapewniać właściwą ochronę konsumentom i inwestorom.

Sojusz Północnoatlantycki

Cyberbezpieczeństwo oraz rozwój nowych technologii zostały sklasyfikowane jako najważniejsze obszary działań NATO w najbliższej przyszłości. W najnowszej strategii zaznaczono, że w cyberprzestrzeni toczą się nieustanne walki, są prowadzone ataki na sieci komputerowe, a złośliwe oprogramowania i podmioty dążą do niszczenia infrastruktury krytycznej NATO, zakłócenia pracy służb rządowych, pozyskiwania danych wywiadowczych, kradzieży własności intelektualnej i utrudniania działań wojskowych Sojuszu.

W 1999 roku po przeprowadzonych atakach lotniczych przez koalicję państw członkowskich NATO na Jugosławię serbscy hakerzy dokonali poważnego cyberataku na główny serwer siedziby Sojuszu Północnoatlantyckiego

9 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Tekst mający znaczenie dla EOG), Dz. Urz. UE 1022, L 333/1.

w Brukseli. Dopiero w 2002 roku na szczycie w Pradze kraje członkowskie przyjęły program ochrony cybernetycznej (Cyber Defense Program). Rozwijające się problemy międzynarodowe spowodowały, że w 2006 roku w Rydze utworzono dodatkową ochronę dla systemów informacyjnych i komunikacyjnych. Dopiero cyberataki przeprowadzone w kwietniu i maju 2007 roku na estońskie instytucje publiczne i prywatne pokazały, że NATO musi rozpocząć pracę nad opracowaniem polityki cyberbezpieczeństwa Sojuszu w trybie pilnym. Finałem tego było zatwierdzenie przez państwa członkowskie Sojuszu pierwszej polityki cyberbezpieczeństwa (Cyber Defence Policy) w styczniu 2008 roku w Bukareszcie. Dokument ten zawierał propozycje wspólnej polityki działania państw NATO przeciwko cyberatakom, zapewnił wsparcie w razie ich występowania oraz określił politykę skierowaną na wzmocnienie kluczowych systemów dowodzenia.

Ataki Rosji na Estonię spowodowały, że na szczycie NATO 19–20 listopada 2010 roku w Lizbonie została przyjęta „Koncepcja strategiczna NATO", która miała obowiązywać przez 10 kolejnych lat. Głównym zadaniem Sojuszu było zapobieganie, wykrywanie, obrona przed atakami cybernetycznymi oraz odtwarzanie zdolności po nich. Punkt 12 koncepcji stwierdza, że „Ataki cybernetyczne stają się coraz częstsze, lepiej zorganizowane i bardziej kosztowne, biorąc pod uwagę szkody, jakie wyrządzają administracjom rządowym, biznesowi, gospodarce, a potencjalnie także transportowi, sieciom dostaw i innej infrastrukturze krytycznej i mogą one osiągnąć poziom, którego przekroczenie zagraża narodowemu i euroatlantyckiemu dobrobytowi, bezpieczeństwu i stabilności"[10]. Źródłem takich ataków mogą być obce siły wojskowe i służby wywiadowcze, zorganizowane grupy przestępcze, terrorystyczne i/lub grupy ekstremistyczne. W dobie narastających zagrożeń w cyberprzestrzeni NATO przyjęło na szczycie w Newport w 2014 roku deklarację, w której zapisano, że cyberataki mogą prowadzić do powołania się na art. 5 Traktatu północnoatlantyckiego, mówiący o obronie zbiorowej[11]. Była to przełomowa deklaracja, która potwierdziła, że zagrożenie cyberatakami może zdestabilizować funkcjonowanie państwa. W 2016 roku w trakcie warszawskiego szczytu

10 *Koncepcja strategiczna NATO (Tłumaczenie robocze BBN). „Koncepcja strategiczna obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego, przyjęta przez szefów państw i rządów w Lizbonie 20 listopada 2010 r."*, tłum. A. Juszczak, https://www.bbn.gov.pl/ftp/dok/01/koncepcja_strategiczna_nato_tlumaczenie.pdf [dostęp: 15.05.2023].

11 Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r., Dz.U. 2000, nr 87, poz. 970.

sporządzono deklarację cyberbezpieczeństwa (Cyber Defence Pledge), w której w siedmiu punktach państwa zobowiązały się do wzmocnienia ochrony krajowej infrastruktury teleinformatycznej, przydzielenie odpowiedniej ilości środków finansowych na organizację cyberobrony, wzmocnienia współpracy wewnątrz kraju z podmiotami odpowiedzialnymi za cyberbezpieczeństwo, położenia większego nacisku na edukację w obszarze cyberbezpieczeństwa czy zwiększenie świadomości wśród decydentów zasad korzystania z cyberprzestrzeni. Zwrócono również uwagę na znaczenie współpracy z Unią Europejską w celu wzmocnienia tego region przed atakami. Sojusznicy potwierdzili, że NATO musi równie skutecznie bronić się w cyberprzestrzeni jak na lądzie, w powietrzu czy na morzu. Każdy kraj musi wzmocnić swoją obronę cybernetyczną i rozwijać ją w sposób priorytetowy. W tym celu zostały utworzone zespoły NATO Cyber Rapid Reaction, które są w gotowości 24 godziny na dobę, żeby pomóc sojusznikom, jeżeli zajdzie taka potrzeba.

Po ciągłych atakach na infrastrukturę cybernetyczną poszczególnych członków NATO w 2018 roku Rada Północnoatlantycka zatwierdziła wizję i strategię Komitetu Wojskowego w sprawie cyberprzestrzeni jako domeny działań (Vision and Strategy on Cyberspace as a Domain of Operations). W trakcie szczytu NATO w Madrycie w 2022 roku została przyjęta nowa koncepcja strategiczna NATO. W punktach 24 i 25 zapisano, że zostanie przyspieszona cyfrowa transformacja, a jeżeli będą prowadzone złośliwe działania w cyberprzestrzeni albo w przestrzeni kosmicznej, to Rada Północnoatlantycka może być skłonna to powołania się na art. 5 Traktatu północnoatlantyckiego[12].

Organizacja Narodów Zjednoczonych

Organizacja Narodów Zjednoczonych (ONZ) jest największą organizacją na świecie; zrzesza 193 państwa. W swojej misji kieruje się przede wszystkim utrzymywaniem pokoju i bezpieczeństwa wszystkich państw, które dążą do rozwijania swoich stosunków. Głównymi zadaniami ONZ jest utrzymanie międzynarodowego pokoju i bezpieczeństwa, ochrona praw człowieka, dostarczanie pomocy humanitarnej, wspieranie zrównoważonego rozwoju i działania na rzecz klimatu oraz przestrzeganie prawa międzynarodowego. Pierwszym

12 *NATO 2022 Strategic Concept*, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf [dostęp: 3.06.2023].

dokumentem dotyczącym sfery cyberprzestrzeni określającym przestępstwa komputerowe była rezolucja Zgromadzenia Ogólnego ONZ nr 45/121 z 14 grudnia 1990 roku, która wzywała państwa członkowskie do intensyfikacji wysiłków skierowanych na skuteczne zwalczanie nadużyć komputerowych, w szczególności przez:

1. Wprowadzenie odpowiednich zmian do ustawodawstwa karnego materialnego i procesowego, w celu dostosowania istniejących definicji przestępstw oraz przepisów, dotyczących środków przymusu i dopuszczalności dowodów do ścigania nadużyć komputerowych i pozbawienia ich sprawców nielegalnie uzyskanych korzyści[13];

2. Usprawnienie zabezpieczeń systemów komputerowych, uwzględniając przy tym problemy związane z ochroną prywatności oraz praw i wolności obywatelskich[14].

W kolejnych latach w ONZ podjęto następujące rezolucje: nr 55/63, styczeń 2001 – zwalczanie przestępczego wykorzystywania technologii informacyjnych, nr 56/121, styczeń 2002 – zwalczanie przestępczego wykorzystywania technologii informacyjnych, nr 57/239, styczeń 2003 – stworzenie globalnej kultury cyberbezpieczeństwa, uchwałę nr 58/199, styczeń 2004 – tworzenie globalnej kultury cyberbezpieczeństwa i ochrony krytycznej infrastruktury informatycznej, rezolucję nr 64/211, marzec 2010 – stworzenie globalnej kultury cyberbezpieczeństwa i podsumowanie krajowych wysiłków na rzecz ochrony infrastruktury krytycznej.

W grudniu 2018 roku Zgromadzenie Ogólne ONZ przyjęło dwie ważne rezolucje – nr 73/271 w sprawie rozwoju w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego oraz nr 73/2662 w sprawie rozwijania odpowiedzialnych zachowań państw w cyberprzestrzeni w kontekście bezpieczeństwa międzynarodowego. W grudniu 2019 roku Zgromadzenie Ogólne ONZ przyjęło rezolucję w sprawie przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych do celów przestępczych, a także powołało komitet do opracowania konwencji międzynarodowej dotyczącej cyberbezpieczeństwa oraz cyberprzestępczości. Pierwsze spotkania grupy roboczej miało miejsce na początku 2022 roku, ale ze względu na szeroki zakres traktatu ostateczna jego wersja ma zostać opublikowana na początku 2024 roku. Głównymi zagadnieniami będzie: ustanowienie

13 A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 9-10.

14 Rezolucja Zgromadzenia Ogólnego ONZ nr 45/121 z 14 grudnia 1990 r., https://digitallibrary.un.org/record/105578 [dostęp: 15.05.2023].

jednolitego prawa karnego materialnego dotyczącego cyberprzestępczości, światowy dostęp do organów ścigania za przestępstwa transgraniczne i ochrona praw człowieka w wirtualnym świecie. „Cybersecurity in the United Nations system organizations" to najnowsza pozycja z dotychczasowymi zaleceniami, która wskazuje, elementy przyczyniające się do zwiększenia cyberodporności[15].

Stany Zjednoczone Ameryki

Internet powstał pod koniec lat 60. wieku XX w Stanach Zjednoczonych Ameryki, ale dopiero w 2011 roku została zaprezentowana pierwsza międzynarodowa strategia cyberbezpieczeństwa, którą wydał Biały Dom za prezydentury Baracka Obamy[16]. Została ona podzielona na trzy części: budowanie polityki cyberprzestrzeni, przyszłość cyberprzestrzeni oraz priorytety polityki. Dokument zakładał m.in.: ochronę własnych sieci, wytworzenie międzynarodowych standardów, ochronę infrastruktury krytycznej, minimalizację skutków ataków na serwery, współpracę międzynarodową, walkę z cyberprzestępczością, przygotowanie armii do walki w cyberprzestrzeni[17]. Cztery lata później w 2015 roku została opracowana narodowa strategia bezpieczeństwa, która określiła priorytety kraju w budowaniu amerykańskiej potęgi w sferze cyber. W dokumencie tym podkreślono szczególną rolę Stanów Zjednoczonych na świecie jako najważniejszego gracza, ale także jako największego sojusznika swoich partnerów i organizacji międzynarodowych. Najważniejszym zadaniem Stanów Zjednoczonych oraz ich sojuszników jest bezpieczeństwo, wzrost gospodarczy, szacunek dla krajowych i międzynarodowych wartości uniwersalnych oraz promowanie pokoju i bezpieczeństwa światowego. W strategii ustosunkowano się również do coraz większych wyzwań i zagrożeń związanych z cyberprzestrzenią. Potwierdzono, że rośnie niebezpieczeństwo związane z cyberatakami, w tym przede wszystkim ataki na infrastrukturę krytyczną państwa. Podkreślono w niej, że wprawdzie internet został zaprojektowany

15 *Cybersecurity in the United Nations system organizations 2021*, https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf [dostęp: 21.05.2023].

16 *International Strategy for Cyberspace the White House 2011*, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [dostęp: 12.05.2023].

17 M. Grzelak, *Międzynarodowa strategia USA dla cyberprzestrzeni*, „Bezpieczeństwo Narodowe" 2011, nr 2, s. 140.

jako otwarty system wymiany informacji, lecz obecnie jest konieczne zagwarantowanie bezpieczeństwa cybernetycznego państwa. Zaznaczono, że internet obecnie służy nie tylko do celów państwowych, lecz także prywatnych i swobodnego przepływu informacji czy wiadomości, co może przynieść skutki gospodarcze i polityczne. Strategia Departamentu Obrony podkreślała ważkość prawidłowej koordynacji zadań i wymiany informacji między głównymi agencjami (Departamentem Obrony, Departamentem Bezpieczeństwa Wewnętrznego, FBI) a organizacjami międzynarodowymi. Bardzo ważnym elementem cyberstrategii Departamentu Obrony Stanów Zjednoczonych było potwierdzenie współpracy z firmami prywatnymi w ochronie infrastruktury krytycznej. Dokument ten miał być ukierunkowany na współpracę wszystkich instytucji rządowych i federalnych w obszarze cyberbezpieczeństwa. Potwierdzono, że bardzo ważnym elementem jest współpraca międzynarodowa z partnerami z całego świata zarówno państwowymi, jak i prywatnymi. Za najważniejsze elementy rozwoju uznano: gospodarkę, ochronę sieci, egzekwowanie prawa, partnerstwo z podmiotami cywilnymi i państwowymi, współpracę wojskową, zarządzanie globalną siecią oraz przestrzeganie praw człowieka. W dalszych częściach strategia Stanów Zjednoczonych podkreślała, że państwo zawsze będzie reagowało na wszystkie niebezpieczeństwa, wykorzystując do tego wszelkie niezbędne środki, tj.: dyplomatyczne, informacyjne, militarne i ekonomiczne dozwolone przez prawo międzynarodowe. Zapewniano, że rozwiązania militarne będą ostatecznością, po którą Waszyngton sięgnie dopiero po wyczerpaniu wszystkich innych środków.

Pod koniec 2017 roku prezydent Donald Trump podpisał strategię bezpieczeństwa narodowego, w której wskazano szczególne zagrożenie ze strony Chin, Rosji, Iranu i Korei Północnej[18]. W dokumencie zwrócono uwagę na dominującą rolę Stanów Zjednoczonych w sferze cyber oraz współpracę z międzynarodowymi partnerami. Wskazywano również cztery filary: ochronę Amerykanów, ich ojczyzny i amerykańskiego stylu życia, promowanie amerykańskiego dobrobytu, ochronę pokoju poprzez siłę oraz powiększanie wpływów państwa. Strategia podkreślała globalną hegemonię Stanów Zjednoczonych w cyberprzestrzeni.

Narodowa strategia cybernetyczna wydana w październiku 2018 roku została podzielona na cztery grupy zadań: zapewnienie bezpieczeństwa

18 *National Security Strategy of the United States of America December 2017*, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [dostęp: 17.05.2023].

narodowego, promowanie dobrobytu i amerykańskiego stylu życia, zachowanie pokoju poprzez siłę oraz poszerzanie wpływu Ameryki[19]. W podpisanej przez prezydenta Donalda Trumpa narodowej strategii cybernetycznej Stany Zjednoczone określiły swoją pierwszą w pełni sformułowaną strategię cybernetyczną od 15 lat. Zwrócono w niej uwagę na rozwój gospodarki cyfrowej, stworzenie personelu, który będzie pracował dla cyberbezpieczeństwa, rozbudowę międzynarodowych relacji i ciągłe budowanie potencjału cybernetycznego. Określiła ona następujące zadania organów administracji publicznej:

- „Bronić ojczyzny, chroniąc sieci, systemy, funkcje i dane.
- Promować amerykański dobrobyt, pielęgnując bezpieczną, prosperującą gospodarkę cyfrową i wspierając innowacje krajowe.
- Zachować pokój i bezpieczeństwo poprzez wzmocnienie zdolności Stanów Zjednoczonych — wspólnie z sojusznikami i partnerami, aby odstraszać i, jeśli to konieczne, karać tych, którzy używają narzędzi cybernetycznych w złym celu.
- Zwiększyć wpływy USA za granicą, aby rozszerzyć kluczowe założenia otwartego, interoperacyjnego, niezawodnego i bezpiecznego internetu"[20].

W październiku 2022 roku Agencja ds. Bezpieczeństwa Cybernetycznego i Infrastruktury (CISA) wydała strategiczny plan działania na lata 2023–2025, który stanowi ujednolicone podejście do zapewnienia bezpieczeństwa narodu amerykańskiego, infrastruktury krytycznej oraz cyberprzestrzeni[21]. Należy również wspomnieć o dwóch innych dokumentach wydanych przez Biały Dom oraz Departament Obrony Stanów Zjednoczonych w październiku 2022 roku – strategii bezpieczeństwa narodowego[22] i strategii obrony narodowej[23]. Dokumenty te nie zawierają rozdziałów poświęconych wyłącznie dziedzinie cyberbezpieczeństwa i związanych z nim zagrożeń, ale podkreślono w nich, że takie zagrożenia istnieją.

19 *National Security Strategy of the United States of America September 2017*, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [dostęp: 17.05.2023].

20 Ibidem.

21 *Cybersecurity and infrastructure Security Agency 2023–2025*, https://www.cisa.gov/sites/default/files/publications/StrategicPlan_20220912-V2_508c.pdf [dostęp: 20.05.2023].

22 *National Security Strategy October. The White House*, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf [dostęp: 30.05.2023].

23 *National Defence Strategy of The United States of America*, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF [dostęp: 30.05.2023].

Japonia

Japonia jest jednym z krajów najbardziej rozwiniętych gospodarczo oraz zawansowanych technologiczne. To w Kraju Kwitnącej Wiśni mieszczą się siedziby największych producentów elektroniki na świecie – Sony, Sharp, Toshiba czy Yamaha. Japończycy należą do jednej z nacji najchętniej korzystających z internetu. Z najważniejszych dokumentów dotyczących cyberprzestrzeni warto zwrócić uwagę na wydaną w 2015 roku przez japoński rząd strategię cyberbezpieczeństwa, która w pięciu zagadnieniach przedstawia zasady cyberbezpieczeństwa[24]. Wskazano w niej jak można poprawić dynamiczność społeczno-gospodarczą i zrównoważyć rozwój państwa, a także budować bezpieczną społeczność w sieci dla ludzi, zapewnić pokój i stabilność społeczności międzynarodowej i bezpieczeństwo narodowe oraz zwięźle przedstawiono podejście do cyberbezpieczeństwa[25]. Artykuł 12 pkt 2 strategii określa podstawy cyberbezpieczeństwa:

1. „Podstawowa polityka dotycząca środków bezpieczeństwa cybernetycznego.

2. Sprawy związane z zapewnieniem cyberbezpieczeństwa w agencjach rządowych.

3. Sprawy dotyczące promowania cyberbezpieczeństwa u ważnych operatorów infrastruktury, organizowanych przez nich organizacji oraz samorządów terytorialnych (zwanych dalej »ważnymi operatorami infrastruktury«).

4. Wszechstronne i skuteczne promowanie środków bezpieczeństwa cybernetycznego”[26].

Najnowsza strategia z grudnia 2022 roku jest podstawą japońskiej strategii bezpieczeństwa narodowego na następne 10 lat[27]. Skupia się na poprawie bezpieczeństwa państwa, wyzwaniach przed nią stojących, bezpieczeństwie Indo-Pacyfiku, zagrożeniach ze strony Korei Północnej i Chin, zadaniach, które Japonia musi zrealizować, żeby być krajem bezpiecznym i zaawanasowanym technologicznie. Poza tym strategia reguluje kwestie związane z ochroną infrastruktury, reagowaniem na ataki i ze współpracą międzynarodową, w szczególności z Amerykanami.

24 *Japan Cybersecurity Strategy 2015*, https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf [dostęp: 30.05.2023].

25 Ibidem.

26 http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm [dostęp: 30.05.2023].

27 *National Security Strategy of Japan 2022*, https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf [dostęp: 30.05.2023].

Kanada

W Kanadzie w 2013 roku został przyjęty pierwszy znaczący dokument dotyczący cyberprzestrzeni, w którym przedstawiono dotychczasową pracę na rzecz sfery cyber[28].

W strategii bezpieczeństwa cybernetycznego na lata 2019–2024 określono trzy najważniejsze cele: bezpieczeństwo, wytrzymałość i wydolność systemów kanadyjskich, innowacyjny i adaptacyjny ekosystem cybernetyczny oraz skuteczne przywództwo i współpraca z podmiotami rządowymi oraz prywatnymi[29]. Za najważniejsze zagrożenia w cyberprzestrzeni uznaje się cyberprzestępczość (kradzież tożsamości, pranie brudnych pieniędzy, oszustwa), cyberterroryzm czy wykorzystanie cyberprzestrzeni przez wywiad i służby wojskowe państw obcych.

Australia

W białej księdze obrony został poruszony temat zagrożeń, które coraz częściej dotykają Australię w cyberprzestrzeni i zostały nazwane jako niemilitarne[30]. Australia jest w trakcie opracowywania skutecznych metod przeciwstawiania się takim działaniom jak szpiegostwo czy uzyskiwanie informacji. Kolejnym dokumentem była biała księga obronna z 2009 roku, w której podkreślono pojawiające się cyberataki mogące potencjalnie zagrozić bezpieczeństwu narodowemu oraz uwidoczniono wzrost ataków w cyberprzestrzeni na podmioty rządowe, gospodarcze oraz infrastrukturę sieci informatycznych[31].

W listopadzie 2009 roku opublikowano przyjętą przez australijski rząd strategię bezpieczeństwa cybernetycznego, w które opisano prace legislacyjne nad szybko zmieniającą się sferą cyber oraz powstanie organizacji mających

28 *Action Plan 2010–2015 for Canada's Cyber Security Strategy*, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf [dostęp: 30.05.2023].

29 *Public Safety Canada Horizontal Evaluation of Canada's Cyber Security Strategy Final Report 2017*, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-cnd-scrt-strtg/vltn-cnd-scrt-strtg-en.pdf [dostęp: 30.05.2023]; *National Cyber Security Action Plan 2019–2024*, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf [dostęp: 30.05.2023].

30 *Australia-Defence 2000 Our Future Defence Force*, https://apps.dtic.mil/sti/pdfs/ADA481122.pdf [dostęp: 30.05.2023].

31 *Defending Australia in the Asia Pacific century: force 2030*, https://www.ssri-j.com/MediaReport/Document/AustraliaDefenceWhitePaper2009.pdf [dostęp: 30.05.2023].

walczyć z cyberprzestępstwami, a także podkreślano niebezpieczeństwo związane z cyberzagrożeniami[32].

W strategii cyberbezpieczeństwa z 2016 roku określono zakres współpracy z partnerami zagranicznymi i sektorem prywatnym[33]. Ostatnia wersja kolejnego aktu legislacyjnego pochodzi z 2020 roku[34]. Głównym celem jest zwiększanie zdolności w odparciu cyberataków oraz promowanie cyberbezpieczeństwa jako wspólnej odpowiedzialności wielu podmiotów – od sektora rządowego, poprzez prywatny i przemysłowy, po osoby fizyczne.

W strategii z 2022 roku proponowane rozwiązania powielają poprzednie, a elementy obronne Australii mają odstraszać i reagować na zagrożenia[35]. Standardy eksploatacji sieci wirtualnych powinny nieustannie się podnosić, a partnerstwa wzmacniać.

Niemcy

Rząd niemiecki 23 lutego 2011 roku przyjął strategię cyberbezpieczeństwa, w której określono główne zadania, tj.: sprawne funkcjonowanie organów administracji w komunikacji oraz zwalczaniu zagrożeń, ochrona infrastruktury krytycznej i sieci teleinformatycznych, ciągły rozwój gospodarki i efektywne zwalczanie cyberprzestępczości[36]. Utworzono także Narodowe Centrum Przeciwdziałania Zagrożeniom dla Cyberprzestrzeni (Nationales Cyber-Abwehrzentrum – NCAZ) oraz Narodową Radę Cyberbezpieczeństwa (Nationaler Cyber-Sicherheitsrat). Adresatami tej strategii są zarówno organy państwowe, jak i sektor prywatny z indywidualnymi użytkownikami włącznie.

Najnowsza strategia cyberbezpieczeństwa została przyjęta w 2021 roku przez Federalne Ministerstwo Spraw Wewnętrznych i ma obowiązywać do

32 *Australian Cyber Security Strategy 2009*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AGCyberSecurityStrategyforwebsite.pdf [dostęp: 30.05.2023].

33 *Australia's Cyber Security Strategy 2016*, https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf [dostęp: 30.05.2023].

34 *Australia's Cyber Security Strategy 2020*, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf [dostęp: 30.05.2023].

35 *Australian Defence Cyber Security Strategy 2022*, https://www.defence.gov.au/sites/default/files/2022-08/defence-cyber-security-strategy.pdf [dostęp: 30.05.2023].

36 *CyberSicherheit und Streitkräfte*, https://www.bundestag.de/resource/blob/414822/04afe986fd8aba8fe0c534d95c389309/WD-2-037-11-pdf-data.pdf [dostęp: 25.05.2023].

2026 roku[37]. Wyznaczono w niej takie kierunki działań w sprawie cyberbezpieczeństwa, jak: wzmocnienie cyfrowej suwerenności państwa, gospodarki, nauki i społeczeństwa, bezpieczne i samodzielne działanie w zdigitalizowanym środowisku, wspólny ład państwa i gospodarki, skuteczna i zrównoważona krajowa architektura cyberbezpieczeństwa.

Wielka Brytania

Działania ukierunkowane na regulację wzmożonego funkcjonowania w cyberprzestrzeni zostały odzwierciedlone w dużej liczbie dokumentów poświęconych tej sferze.

Pierwsza strategia cyberbezpieczeństwa Wielkiej Brytanii zakładała trzy cele do zrealizowania do 2015 roku, dlatego że zauważono narastające problemy w wirtualnym świecie.

1. Wielka Brytania będzie walczyć z cyberprzestępczością i stworzy jedną z najbezpieczniejszych platform cyfrowych dla prowadzenia biznesu na świecie.

2. Wielka Brytania zwiększy swoją odporność na cyberataki i będzie lepiej chronić interesy państwowe w cyberprzestrzeni.

3. Wielka Brytania zapewni otwartą, stabilną i tętniącą życiem cyberprzestrzeń, z której będzie mógł korzystać naród brytyjski.

4. Wielka Brytania poszerzy wiedzę, umiejętności i zdolności, które są niezbędne do osiągnięcia celów w zakresie bezpieczeństwa cybernetycznego[38].

Następnie rząd Zjednoczonego Królestwa opracował „National Cyber Strategy 2022 Pioneering a cyber future with the whole of the UK", którą podzielono na pięć bloków: brytyjski ekosystem cybernetyczny, odporność cybernetyczna, przewaga technologiczna, światowe przywództwo i przeciwdziałanie zagrożeniom[39]. W dokumencie tym doprecyzowano zadania, które mają zwiększyć ochronę państwową i sektora prywatnego w sferze cyber

37 *Cyber Security Strategy for Germany 2021*, https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf;jsessionid=32AA015A2C6C40289805C972412BA64B.2_cid322?__blob=publicationFile&v=4 [dostęp: 20.05.2023].

38 *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [dostęp 26.06.2023]

39 *National Cyber Strategy 2022 UK*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf [dostęp: 10.05.2023].

poprzez m.in.: zwiększenie środków przeznaczonych na program cyberbezpieczeństwa, wzmocnienie partnerstwa międzynarodowego (szczególnie z organami administracji Szkocji, Walii i Irlandii Północnej), utworzenie National Cyber Security Centre (NCSC), zwiększenie potencjału i zaangażowania wojskowego, zainwestowanie 1,9 mld funtów na poprawę bezpieczeństwa Wielkiej Brytanii.

W przedmowie do „Government Cyber Security Strategy Building a cyber resilient public sector 2022–2030" Boris Johnoson zapewniał, że „[...] niewiele krajów jest lepiej przygotowanych do poruszania się po cyberprzestrzeni […] Organizacje rządowe mają chronić usługi i funkcje, które utrzymują i promują naszą gospodarkę i społeczeństwo, rząd musi być wzorem dla sektora prywatnego i zapewnić, że Wielka Brytania umacnia swoją reputację jako jeden z krajów z najbezpieczniejszą i najbardziej atrakcyjną gospodarką cyfrową, gdzie można mieszkać, prowadzić działalność gospodarczą oraz inwestować"[40]. Strategia obejmuje takie zagadnienia, jak: zarządzanie ryzykiem w cyberprzestrzeni, ochrona przed cyberatakami, wykrywanie zdarzeń cybernetycznych, minimalizowanie skutków incydentów cybernetycznych, rozwijanie odpowiednich umiejętności, kultury i wiedzy na temat cyberbezpieczeństwa.

Ukraina

Ukraina w 2017 roku zdefiniowała podstawy ochrony istotnych interesów państwa i obywateli, a także priorytety i cele organów państwowych w ustawie o podstawowych zasadach zapewnienia cyberbezpieczeństwa przyjętej przez ukraiński parlament[41]. Powstały dzięki temu instytucje i organy państwowe odpowiedzialne za zwalczanie cyberprzestępstw. Następstwem tego było wprowadzenie w maju 2021 roku strategii cyberbezpieczeństwa, która została podzielona na dziewięć sekcji, w tym m.in.: kontekst globalny, realizacja strategii cyberbezpieczeństwa Ukrainy na lata 2016–2020, zasady budowy krajowego systemu cyberbezpieczeństwa, wyzwania i cyberzagrożenia, priorytety i cele strategiczne cyberbezpieczeństwa, kierunki aktywności

40 *Government Cyber Security Strategy 2022–2030*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf [dostęp: 10.05.2023].

41 *Про основні засади забезпечення кібербезпеки України*, https://zakon.rada.gov.ua/laws/show/2163-19#Text [dostęp: 21.05.2023].

polityki zagranicznej państwa w obszarze cyberbezpieczeństwa i mechanizmy realizacji strategii i zapewnienia otwartości[42]. Jednym z jej rezultatów było utworzenie wojsk obrony cyberprzestrzeni. Dokument artykułuje również ukraińskie dążenie do zintegrowania kraju z Unią Europejską i Sojuszem Północnoatlantyckim. Strategia weszła w życie przed atakiem Rosji na Ukrainę, ale w tym dokumencie jako główne źródło zagrożenia wymieniono Rosję, ponieważ to z jej strony odnotowywano najczęstsze ataki na ukraińską infrastrukturę krytyczną, wojnę informacyjną oraz działania służb wywiadowczych w środowisku cyberprzestrzeni.

Francja

Francja znajduje się na drugim miejscu w Europie pod względem inwestycji na cyberbezpieczeństwo jako system informatyczny. Pierwsze wzmianki o cyberzagrożeniach odnotowano w 2008 roku w białej księdze obrony i bezpieczeństwa. Zdefiniowano w niej zagrożenie cyberbezpieczeństwa jako element strategiczny[43]. Ujęcie terminu cyberzagrożenia było krokiem milowym w rozpoznaniu tego zagrożenia, a wprowadzenie w tamtym czasie odpowiednich procedur ograniczyło ataki na infrastrukturę krytyczną Francji. Jednakże ciągły wzrost znaczenia systemów informatycznych oraz bardzo szybki rozwój technologii wymagały od Francuzów ciągłych zmian, żeby utrzymać zdolność do ochrony i reagowania obronnego na zagrożenia. W zagwarantowaniu bezpieczeństwa ważne było zwiększenie budżetu na bezpieczeństwo łączności elektronicznej oraz rozbudowę kryptologii.

W 2018 roku został opracowany strategiczny przegląd obrony, który został porównany do białej księgi w sprawie obrony i bezpieczeństwa narodowego z 1972 roku uważanej za rewolucyjny pogląd na inne zagrożenie[44]. Wtedy to została przyjęta doktryna nuklearna, a w 2018 roku doktryna cyberobrony. Przegląd został podzielony na trzy części. Pierwsza dotyczyła zagrożeń cyberświata, sposobu organizacji cyberobrony na świecie oraz przedstawiała

42 *Cybersecurity Strategy of Ukraine for 2021–2025*, https://www.rnbo.gov.ua/en/Diialnist/4838.html [dostęp: 21.05.2023].
43 P. Mickiewicz, *System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, t. 11, nr 1, s. 68–69.
44 *Strategic review of cyber defence February 2018 – France*, http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf [dostęp: 29.04.2023].

regulacje prawne cyberprzestrzeni. Druga dotyczyła „Państwa odpowiedzialnego za cyberobronę narodu". W przeglądzie szczegółowo opisano mechanizmy zarządzania cyberobroną, przedstawiono zalecenia dotyczące ochrony operatorów infrastruktury krytycznej oraz zidentyfikowano nową kategorię infrastruktury krytycznej – infrastrukturę nadkrytyczną. Ta kategoria odnosiła się do infrastruktur, które odgrywają główną rolę we wspieraniu innych infrastruktur krytycznych, czyli łączności elektronicznej i dostawców energii elektrycznej. Ostatnia część szczegółowo opisywała strategię Francji dotyczącą działań międzynarodowych. Rok później francuskie Ministerstwo Sił Zbrojnych opublikowało wojskową cyberstrategię.

W 2022 roku Emmanuel Macron zatwierdził dokument „National Strategic Review 2022", w którym zostały określone cele strategiczne – odporność cybernetyczna i jej poprawa jako warunek suwerenności Francji[45].

Zakończenie

Wszystkie organizacje, instytucje międzynarodowe, poszczególne kraje na świecie robią wszystko, żeby ewentualne ataki na ich sieci informatyczne nie spowodowały paraliżu funkcjonowania państwa, gdyby została wyłączona ich wirtualna infrastruktura. Uruchomienie art. 51 Karty Narodów Zjednoczonych: „Nic w niniejszej Karcie nie może uchybiać niepozbywalnemu prawu do samoobrony indywidualnej lub zbiorowej w przypadku napaści zbrojnej na któregokolwiek członka Narodów Zjednoczonych, zanim Rada Bezpieczeństwa nie podejmie niezbędnych zarządzeń w celu utrzymania międzynarodowego pokoju i bezpieczeństwa. Środki podjęte przez członków w wykonaniu tego prawa do samoobrony będą natychmiast podane do wiadomości Radzie Bezpieczeństwa i w niczym nie mogą uszczuplać władzy i odpowiedzialności Rady Bezpieczeństwa, wynikających z niniejszej Karty, do podejmowania w każdym czasie takiej akcji, jaką ona uzna za niezbędną do utrzymania lub przywrócenia międzynarodowego pokoju i bezpieczeństwa" lub art. 5 Traktatu północnoatlantyckiego: „Strony zgadzają się, że zbrojna napaść na jedną lub więcej z nich w Europie lub Ameryce Północnej będzie uznana za napaść przeciwko nim wszystkim i dlatego zgadzają się, że jeżeli taka zbrojna napaść nastąpi,

45 *National strategic review 2022 – France*, http://www.sgdsn.gouv.fr/uploads/2022/12/rns-uk-20221202.pdf [dostęp: 29.04.2023].

to każda z nich, w ramach wykonywania prawa do indywidualnej lub zbiorowej samoobrony, uznanego na mocy art. 51 Karty Narodów Zjednoczonych, udzieli pomocy Stronie lub Stronom napadniętym, podejmując niezwłocznie, samodzielnie jak i w porozumieniu z innymi Stronami, działania, jakie uzna za konieczne, łącznie z użyciem siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego" musiałoby pociągnąć za sobą ogromne straty w ludziach, a także w sferze materialnej[46]. Konsekwencją ataku cybernetycznego musiałby być np. wybuch elektrowni atomowej państwa albo zniszczenie infrastruktury krytycznej zagrażające funkcjonowaniu państwa, a taki atak musiałby zagrażać bezpieczeństwu międzynarodowemu oraz pokojowi na świecie. Uruchomienie całej procedury musiałoby się wiązać z przestrzeganiem zasad międzynarodowego prawa humanitarnego konfliktów zbrojnych – konieczności wojskowej czy proporcjonalności. I tak do dziś prawo międzynarodowe nie reguluje kwestii odwetowych i nie wiadomo jak mógłby wyglądać taki konflikt. Nie wiadomo, czy w przypadku zintensyfikowanego ataku cyber pociągnie on za sobą konsekwencje militarne (zbrojne). Bardzo ważnym aspektem w przypadku uruchomienia któregokolwiek artykułu będzie rozróżnienie ataku hakerskiego od działań terrorystycznych. Bardzo trudno będzie zdefiniować różnice pomiędzy tymi działaniami. Można to porównywać do Grupy Wagnera, która, jak wiadomo, pochodzi z Rosji, a nawet niedawno otworzyła swoje biuro w Petersburg, żeby zachęcić do wstępowania w jej szeregi. Rosja nie przyzna się, że to w imię jej interesów walczy Grupa Wagnera.

Żeby zdefiniować prawo cyberprzestrzeni, należy podejść do danego zagadnienia w sposób nowatorski ze względu na jego międzynarodowy charakter, zasięg terytorialny, a także różnice w jego klasyfikowaniu. Proces tworzenia będzie bardzo długotrwały lub nigdy nie zostanie zakończony. Nasuwa się również pytanie, kto miałby się zająć całym procesem legislacyjnym, ponieważ wiele państw na świecie ma ze sobą konflikt interesów. Jak pokazałem w niniejszym artykule, bardzo wiele strategii i dokumentów normujących sferę cyber powiela się, a niejednokrotnie są wręcz takie same. Niezwykle trudno będzie ujednolicić regulacje prawne cyberprzestrzeni dla wszystkich krajów ze względu na różnice w prawie cywilnym czy karnym.

46 Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych, Dz.U. 1947, nr 23, poz. 90, art. 51; Traktat Północnoatlantycki..., art. 5.

Znaczącym elementem jest współpraca instytucji i organów państwowych z sektorem prywatnym, gdyż to w tych sektorach najbardziej rozwija się sfera cyberprzestrzeni. Cyberprzestrzeń powinna być dobrem wspólnym wszystkich obywateli ze względu na posiadane zasoby takie, jak: informacje, wiedza, wymiana doświadczeń, edukacja, handel, prowadzenie biznesu czy nawiązywanie kontaktów zawodowych i prywatnych z całego świata.

Bibliografia

Action Plan 2010–2015 for Canada's Cyber Security Strategy, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf [dostęp: 30.05.2023].

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Australia's Cyber Security Strategy 2016, https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf [dostęp: 30.05.2023].

Australia's Cyber Security Strategy 2020, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf [dostęp: 30.05.2023].

Australia-Defence 2000 Our Future Defence Force, https://apps.dtic.mil/sti/pdfs/ADA481122.pdf [dostęp: 30.05.2023].

Australian Cyber Security Strategy 2009, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AGCyberSecurityStrategyforwebsite.pdf [dostęp: 30.05.2023].

Australian Defence Cyber Security Strategy 2022, https://www.defence.gov.au/sites/default/files/2022-08/defence-cyber-security-strategy.pdf [dostęp: 30.05.2023].

Chałubińska-Jentkiewicz K., Brzostek A., *Strategie cyberbezpieczeństwa współczesnego świata*, Warszawa 2021.

Cyber Security Strategy for Germany 2021, https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf;jsessionid=32AA015A2C6C40289805C972412BA64B.2_cid322?__blob=publicationFile&v=4 [dostęp: 20.05.2023].

Cybersecurity and infrastructure Security Agency 2023–2025, https://www.cisa.gov/sites/default/files/publications/StrategicPlan_20220912-V2_508c.pdf [dostęp: 20.05.2023].

Cybersecurity in the United Nations system organizations 2021, https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf [dostęp: 22.05.2023].

Cybersecurity Strategy of Ukraine for 2021–2025, https://www.rnbo.gov.ua/en/Diialnist/4838.html [dostęp: 21.05.2023].

Cyber-Sicherheit und Streitkräfte, https://www.bundestag.de/resource/blob/414822/04afe986fd8aba8fe0c534d95c389309/WD-2-037-11-pdf-data.pdf [dostęp: 25.05.2023].

Defending Australia in the Asia Pacific century: force 2030, https://www.ssri-j.com/MediaReport/Document/AustraliaDefenceWhitePaper2009.pdf [dostęp: 30.05.2023].

Dereń J., Rabiak A., *NATO a aspekty bezpieczeństwa w cyberprzestrzeni* [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Warszawa 2004.

Government Cyber Security Strategy 2022–2030, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf [dostęp: 10.05.2023].

Grzelak M., *Międzynarodowa strategia USA dla cyberprzestrzeni*, „Bezpieczeństwo Narodowe" 2011, nr 2.

International Strategy for Cyberspace the White House 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [dostęp: 12.05.2023].

Japan Cybersecurity Strategy 2015, https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf [dostęp: 30.05.2023].

Karpiuk M., *Cybersecurity as an element in the planninc activities of public administration*, „Cybersecurity and Law" 2021, nr 1.

Koncepcja strategiczna NATO (Tłumaczenie robocze BBN). „Koncepcja strategiczna obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego, przyjęta przez szefów państw i rządów w Lizbonie 20 listopada 2010 r.", tłum. A. Juszczak, https://www.bbn.gov.pl/ftp/dok/01/koncepcja_strategiczna_nato_tlumaczenie.pdf [dostęp: 15.05.2023].

Mickiewicz P., *System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, t. 11, nr 1.

National Cyber Security Action Plan 2019–2024, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf [dostęp: 30.05.2023].

National Cyber Strategy 2022 UK, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf [dostęp: 10.05.2023].

National Defence Strategy of The United States of America, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF [dostęp: 30.05.2023].

National Security Strategy October. The White House, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf [dostęp: 30.05.2023].

National Security Strategy of Japan 2022, https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf [dostęp: 30.05.2023].

National Security Strategy of the United States of America December 2017, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [dostęp: 17.05.2023].

National Security Strategy of the United States of America September 2017, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [dostęp: 17.05.2023].

National strategic review 2022 – France, http://www.sgdsn.gouv.fr/uploads/2022/12/rns-uk-20221202.pdf [dostęp: 29.04.2023].

Nato 2022 Strategic Concept, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf [dostęp: 3.06.2023].

Про основні засади забезпечення кібербезпеки України, https://zakon.rada.gov.ua/laws/show/2163-19#Text [dostęp: 2105.2023].

Public Safety Canada Horizontal Evaluation of Canada's Cyber Security Strategy Final Report 2017, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-cnd-scrt-strtg/vltn-cnd-scrt-strtg-en.pdf [dostęp: 30.05.2023].

Strategic review of cyber defence February 2018 – France, http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf [dostęp: 29.04.2023].

The UK Cyber Security Strategy Protecting and promoting the UK in a digital world, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [dostęp 26.06.2023].

Wspólny Komunikat do Parlamentu Europejskiego i Rady. Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020JC0018&from=EN [dostęp: 20.06.2023].

International Legal Regulations of Cyberspace

Summary

This article aims to present the different approaches of countries around the world regarding the legal regulations of cyberspace. The creation of a unified legal system for cyberspace will be a difficult process due to major conflicts of interest. International organizations such as the EU and NATO, which bring together countries that have a similar vision of the world and how it should function, contribute to the unification of legal norms governing cyberspace in specific countries. On the other hand, vague initiatives of the world's largest organization – the UN as well as the lack of implementation of newly adopted regulations by all member countries, unfortunately slow down the fight against cyberterrorism and cybercrimes that are transnational in nature. All countries around the world are increasing financial investment in improving information networks, creating new institutions to combat threats in the digital space and adapting laws to a dynamically changing world.

Key words: cyberspace, cyber security, international law, international organizations