Świat Idei i Polityki
ISSN 1643-8442
DOI: 10.15804/siip201805
2018, tom 17

Marcin Wałdoch

ORCID ID: 0000-0002-8778-1780

Strategie cyberbezpieczeństwa Nowej Zelandii i Polski w procesie globalizacji

Streszczenie: W prezentowanym badaniu wykonano analizę porównawczą strategii cyberbezpieczeństwa Nowej Zelandii i Polski. W wyniku przeprowadzonego badania potwierdzono hipotezę, że strategie cyberbezpieczeństwa Nowej Zelandii i Polski wykazują różnice wynikające ze swoistości systemów politycznych tych państw. Ponadto ujawniono, że w sferze cyberprzestrzeni występują sojusze i modele relacji międzynarodowych znane ze świata rzeczywistego. Nowa Zelandia pozostaje więc bliskim partnerem bezpieczeństwa cybernetycznego USA, Australii i Kanady, podczas gdy Polska ukierunkowana jest na współpracę w ramach struktur Unii Europejskiej, co wskazywać może na regionalizację obecnie obowiązujących strategii cyberbezpieczeństwa.

Słowa kluczowe: cyberbezpieczeństwo, Nowa Zelandia, Polska, globalizacja, analiza porównawcza

Wstęp

Interesujący wymiar cyberbezpieczeństwa prezentuje w swojej książce *Broń matematycznej zagłady* Cathy O'Neil, która wskazuje, jak bardzo bezpieczeństwo ekonomiczne, społeczne i narodowe

jest uzależnione od rynków finansowych i informacji, które krążą w cyberprzestrzeni w powiązaniu z mechanizmem „dyskryminacji poprzez algorytmy", na których bazują systemy informatyczne[1]. Z taką wersją zagrożeń dla cyberbezpieczeństwa państwo nie zdoła się zmierzyć w krótkim czasie, a jedynie poprzez wpływanie na strukturę społeczną, bowiem to ludzie zapatrzeni w zyski finansowe kreują narzędzie cyfrowe, które pogłębiają społeczne nierówności, a te z kolei podminowują poczucie bezpieczeństwa. Strategie cyberbezpieczeństwa nie są kreowane celem przeciwdziałania nierównościom społecznym, a raczej ku zabezpieczeniu swoistego *status quo* w świecie wirtualnym. Państwa zaś w toku konieczności zapewniania dla legitymizacji władzy poprzez wypełnianie, przynajmniej w państwach o reżimach demokratycznych, warunków tzw. umowy społecznej, zmuszone są przeciwdziałać zjawiskom globalnym, które nadwyrężają między innymi finanse publiczne i infrastrukturę narodową. W tym obecnie są to między innymi problemy z wypracowaniem jednolitego systemu podatkowego wobec kryptowalut czy skuteczne przeciwdziałanie zjawisku offshoringu kapitałowego. Są to zjawiska, które lokują się na granicy pojęć cyberbezpieczeństwo i cyberprzestępczość.

W 2016 r. szacowano, że narodowe strategie cyberbezpieczeństwa posiadało na świecie ponad 50 państw. Większość postulatów tych strategii odnosiła się do dwóch wytycznych – zarówno do stworzenia centralnego organu w ramach administracji publicznej, który będzie koordynował działania z zakresu cyberbezpieczeństwa, jak i Computer Emergency Response Team (CERT). Wymóg czasu związany z koniecznością tworzenia ogólnonarodowych strategii cyberbezpieczeństwa wyjaśnia się zmieniającą się naturą zagrożeń w sieci. Jeśli we wcześniejszych latach były to pojedyncze ataki, to obecnie są to częstokroć ataki o dużej skali, sponsorowane przez państwa. Tym samym cyberataki mogą wyrządzić więcej szkód aniżeli konwencjonalny terroryzm. Ukazuje się przykłady takich zdarzeń jak ataki cybernetyczne na Estonię w 2007 r., wojnę cybernetyczną pomiędzy

[1] C. O'Neil, *Broń matematycznej zagłady. Jak algorytmy zwiększają nierówności i zagrażają demokracji*, przeł. M.Z. Zieliński, Warszawa 2017, passim.

Gruzją i Rosją w 2008 r., atak na irański program nuklearny w 2010 r. (robak komputerowy STUXNET). Dla wzrostu świadomości istniejących dla państw i obywateli zagrożeń w cyberprzestrzeni ważnym wydarzeniem było ujawnienie przez amerykańskiego sygnalistę Edwarda Snowdena kulisów działalności Narodowej Agencji Bezpieczeństwa USA (NSA). To 2008 r. uznaje się za kamień milowy rozwoju i implementacji strategii cyberbezpieczeństwa na świecie. Wyjątkiem w tym zakresie pozostają Stany Zjednoczone, które pierwszą strategię cyberbezpieczeństwa opublikowały w 2003 r.[2] E. Snowden ukazał światu istotę funkcjonowania programu PRISM, który pozwala na dostęp do danych osobowych, w tym i prywatnych danych, które użytkownicy spoza USA magazynują na największych światowych dostawcach usług teleinformatycznych, takich jak Google lub Facebook[3]. Cyberprzestrzeń po atakach cybernetycznych na Estonię, Gruzję, ale i Syrię uznano za piąty teatr wojny, tym samym cyberprzestrzeń stała się istotnym aspektem wpływającym na stosunki międzynarodowe i przy tym nowym wymiarem aktywności państw, ich współpracy, ale i rywalizacji[4]. Cyberprzestępczość, która jest „drugą stroną medalu" cyberbezpieczeństwa, jak podają szacunki z 2012 r., kosztowała Nowozelandczyków 463 miliony dolarów nowozelandzkich, jednak nadal kwestie cyberbezpieczeństwa nie są poważnie traktowane przez obywateli kraju kiwi[5]. Interesujące pozostają także relacje pomiędzy firmami z branży *high-tech*; często są to

[2] N. Shafqat, A. Masood, *Comparative analysis of various national security strategies*, „International Journal of Computer Science and Information Security" 2016, Vol. 14, No. 1, s. 129, 131.

[3] Zob. J. Ball, *Edward Snowden NSA files: secret surveillance and our revelations so far*, „The Guardian" 21.08.2013, https://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations, 16.04.2018. O Snowdenie i ujawnionych przez niego informacjach powstał film fabularny w 2016 r. w reżyserii Oliviera Stone'a pod tytułem „Snowden".

[4] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, s. 9–10.

[5] L. Fourie, H. Hettema, T. Kingston, S. Pang, A. Sarrafzadeh, P. Watters, *The Global cybersecurity workforce – an ongoing human capital crisis*, „Global Business and Technology Association Conference" 2014, s. 173–184.

podmioty będące korporacjami transnarodowymi, a nie instytucjami państwowymi. Rzadko bowiem pamięta się o tym, że to państwa dają główne bodźce w postaci wielkich inwestycji w sektor badań i rozwoju. Przykładem mogą być inwestycje w innowacje, które są kapitałochłonne i obciążone wysokim ryzykiem niepowodzenia[6]. Na co dzień też w przekazie medialnym niewiele się mówi i pisze o rzeczywistych twórcach takich projektów jak World Wide Web (WWW), który został zapoczątkowany w instytucji publicznej, sponsorowanej przez państwo, jaką był i pozostał europejski CERN[7]. Obywatele świata stają się w coraz wyższym stopniu uzależnieni w życiu codziennym od kolejnych usług cyfrowych w świecie wirtualnym. Mówi się wręcz o tym, że Internet „wciąga odbiorców"[8].

Stopień, wskaźnik lub indeks cyberbezpieczeństwa państw narodowych jest od 2014 r. mierzony w skali globalnej przez International Telecomunications Union (ITU). W toku prowadzenia analizy i następnie wydawania oceny przekładającej się na wskaźnik Globalnego Indeksu Cyberbezpieczeństwa wyodrębnia się cztery filary i dwadzieścia cztery podfilary oceny. Cztery główne filary oceny występują pod nazwami: prawa, techniki, organizacji, budowy wydolności – efektywności systemu i kooperacji[9]. Wskaźnik ów jest redukcją pewnej rzeczywistości, ale obrazuje różnice stopnia bezpieczeństwa cybernetycznego, stąd autor sięgnął i do tych danych. Niezwykły stopień nasycenia społeczeństw urządzeniami posiadającymi stały dostęp do Internetu tworzy globalną sieć o niezwykłej mocy przyciągania dla przeciętnego obywatela; można stwierdzić, że większość ludzi na świecie ma codzienny kontakt z Internetem,

[6] M. Mazzucato, *Governement – investor, risk-taker, innovator*, https://www.ted.com/talks/mariana_mazzucato_government_investor_risk_taker_innovator#t-461560, 26.04.2018.

[7] M. Lakomy, dz. cyt., s. 41.

[8] T. Harris, *How a handful of the companies control billions of minds every day*, https://www.ted.com/talks/tristan_harris_the_manipulative_tricks_tech_companies_use_to_capture_your_attention#t-65596, 26.04.2018.

[9] *Global Security Index 2017*, Geneva 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01–2017-R1-PDF-E.pdf, 16.04.2018.

a w sieci z innymi ludźmi, co czyni z Internetu newralgiczny etap i element ludzkiej cywilizacji.

Jako metodę badawczą przyjęto komparatystykę. Wykonano analizę porównawczą strategii cyberbezpieczeństwa Polski i Nowej Zelandii. Tym samym przeprowadzono analizę porównawczą dwóch specyficznych przypadków[10]. Odnoszenie polskiej rzeczywistości politycznej do przestrzeni życia politycznego Nowej Zelandii zdaje się pozostawać o tyle zasadne, że państwo to pomimo niedługiej historii nazywane jest „małym mocarzem" areny międzynarodowej dzięki utrzymywaniu obrazu godnego zaufania partnera i podmiotu reagującego na problemy globalne, skąd też wypływa wysoka reputacja Nowej Zelandii[11]. Polska zaś takiej pozycji na arenie międzynarodowej nie posiada, choćby z tej przyczyny, że jako suwerenny byt funkcjonuje na scenie międzynarodowej dopiero od około 30 lat. Zasadnym może się więc okazać dokonanie komparatystyki, celem uzyskania wiedzy, która ułatwi rządzącym podejmowanie optymalnych dla Polski decyzji politycznych. Zasadniczą różnicą jest też to, że ów „mały mocarz" jest w stosunku do Polski państwem rzeczywiście niewielkim pod względem ludnościowym (około 4,9 mln mieszkańców w 2018 r.)[12], co jednak nie różnicuje specyfiki zagrożeń z cyberprzestrzeni dla państw małych i średnich, ale wskazuje inne bariery, które napotykają państwa małe i średnie w potrzebie sprostania wyzwaniom cyberbezpieczeństwa w globalizacji[13]. Dotąd nie przeprowadzono analizy porównawczej strategii cyberbezpieczeństwa Nowej Zelandii i Polski, ani w literaturze polskiej, ani anglojęzycznej, co wskazuje na istnienie luki poznawczej, której wypełnienie

[10] Zob. J. Bajer, *Badania porównawcze w politologii. Zagadnienia metodologiczne*, „Studia Politicae Universitatis Silesiensis" 2012, nr 8, s. 15–48; A. Chodubski, *Wstęp do badań politologicznych*, Gdańsk 2006, s. 125–126.

[11] L. Czechowska, *Mały mocarz: Nowa Zelandia jako przykład roli międzynarodowej osiągniętej dobrą reputacją*, „Athenaeum. Polskie Studia Politologiczne" 2017, vol. 54, s. 7–22.

[12] *Population clock*, http://archive.stats.govt.nz/tools_and_services/population_clock.aspx?url=/tools_and_services/population_clock.aspx, 26.04.2018.

[13] J. Burton, *Small states and cyber security: The case of New Zealand*, „Political Science" 2013, nr 65 (2), s. 216–238.

może podnieść nie tylko stan wiedzy, ale i wpłynąć na usprawnienie procesów rządzenia. Źródłami danych dla prowadzonego badania były dokumenty instytucji publicznych, na których wykonano analizę leksykalną, oraz dane ilościowe, rankingowe odnoszące się do oceny cyberbezpieczeństwa państw.

Ramą teoretyczną prowadzonego badania jest teoria krytyczna stosunków międzynarodowych, a szczególnie ten jej aspekt, który związany jest z postulatem badania relacji pomiędzy państwami, aby „zastanawiać się nad możliwościami rozszerzenia racjonalnej, sprawiedliwej i demokratycznej organizacji polityki na całym świecie”[14]. Materiały empiryczne czerpano z dokumentów oficjalnych instytucji państwowych (akty prawne, strategie cyberbezpieczeństwa), które pozyskiwano również w drodze zapytań o dostęp do informacji publicznej.

Hipotezą prowadzonego badania jest przypuszczenie, że strategie cyberbezpieczeństwa Nowej Zelandii i Polski wykazują różnice wynikające ze swoistości systemów politycznych tych państw. Dla rozwiązania tak sformułowanej hipotezy autor postawił następujące pytania badawcze: jaką wagę do kooperacji z innymi państwami i społecznością międzynarodową przykłada się w strategiach cyberbezpieczeństwa wskazanych państw? W jakim stopniu identyfikacja zagrożeń i narzędzi ochrony jest analogiczna w obu strategiach? W jaki sposób odzwierciedla się specyfika kultury politycznej i doświadczeń historycznych Nowej Zelandii i Polski w strategiach cyberbezpieczeństwa? W jakim stopniu te dwa państwa są suwerenne w podejmowaniu decyzji o formach cyberbezpieczeństwa i kształcie własnych strategii w tym zakresie? W jakiej mierze dotychczasowe członkostwo w sojuszach i organizacjach międzynarodowych i regionalnych rezonuje w strategiach cyberbezpieczeństwa obu państw?

[14] R. Devetak, *Teoria krytyczna*, [w:] *Teorie stosunków międzynarodowych*, red. S. Burchill, R. Devetak, A. Linklater, M. Paterson, C. Reus-Smit, J. True, przeł. P. Frankowski, Warszawa 2006, s. 206.

Przypadek polski

Rzeczpospolita Polska jest państwem unitarnym o bikameralnym parlamencie i systemie rządów parlamentarno-gabinetowym. Reżim polityczny określa się jako demokrację liberalną. Polska pozostaje członkiem licznych organizacji międzynarodowych i regionalnych, takich jak ONZ, NATO, Unia Europejska, Grupa Wyszehradzka. Od upadku porządku zimnowojennego Polska ciąży ku Zachodowi i za priorytet kolejnych rządów uznaje się udział w Sojuszu Północnoatlantyckim. Polska według Globalnego Indeksu Cybebezpieczeństwa (Global Cybersecurity Index, GCI) znajdowała się w 2014 r. na świecie na 11. pozycji wraz z kilkoma innymi państwami i wagą 0,529 na 1,0 (USA były na pierwszej pozycji z wynikiem 0,824). W Europie Polskę plasuje się na 8. pozycji według GCI[15]. Natomiast nowszy raport i stworzony na jego bazie GCI z 2017 r. plasuje Polskę na 33. pozycji na świecie w zakresie cyberbezpieczeństwa. O ile więc Polska zyskała w ogólnej punktacji, bo w 2017 r. uzyskała 0,622 GCI, to inne państwa na świecie również inwestują w cyberbezpieczeństwo w tempie, za którym zwyczajnie Polska zdaje się nie nadążać[16]. Przykładowo wydatki Ministerstwa Cyfryzacji na cyberbezpieczeństwo (m. in. zakup materiałów, wyposażenia, normy, szkolenia, dotacje celowe, zakup analiz, tłumaczenia) wyniosły za lata 2016–2018 ok. 800 tys. zł, uwzględniając okres do kwietnia 2018 r.[17] Może to mieć negatywne konsekwencje polityczne i ekonomiczne dla Polski. Jak państwo polskie wypada w najnowszych rankingach cyberbezpieczeństwa, będzie wiadomym w ostatnim kwartale 2018 r.[18] Polska strategia cyberbezpieczeństwa, w sensie legislacyjnym, jest uchwałą

[15] M. Menting, *Global Security Index*, New York 2014, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf, 16.04.2018.

[16] *Global Security Index 2017*, dz. cyt.

[17] Dane pozyskane przez autora z Ministerstwa Cyfryzacji w drodze zapytania o informację publiczną na podstawie *Ustawy o dostępie do informacji publicznej* z 2001 r. Odpowiedź na zapytanie o informację publiczną z Ministerstwa Cyfryzacji do Marcina Wałdocha z 18 maja 2018 r. Zob. archiwum autora.

[18] Tentative Timeframe, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv3_documents/Tentative%20timeframe.pdf, 16.04.2018.

Rządu RP z mocą wiążącą dla podmiotów administracji publicznej, a w sposób pośredni oddziałuje ona na obywateli i przedsiębiorców. Jest to dokument bazujący na *Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństw sieci i systemów informatycznych na terytorium Unii*[19]. Stanowi także odpowiedź na raport Najwyższej Izby Kontroli (NIK) na temat bezpieczeństwa w cyberprzestrzeni z 2015 r., w którym wskazano, że w Polsce brakowało instytucji koordynującej zadania z zakresu cyberbezpieczeństwa. Przede wszystkim zaś w Polsce brakowało rozwiązań systemowych w tym zakresie. Wykazano wręcz inercję w tej mierze instytucji państwa, pisząc w przywołanym raporcie, że

> (…) działania podmiotów państwowych związane z ochroną cyberprzestrzeni były prowadzone w sposób rozproszony i bez spójnej wizji systemowej. Sprowadzały się one do doraźnego, ograniczonego reagowania na bieżące wydarzenia oraz biernego oczekiwania na regulacje unijne[20].

Ponadto do czasu powstania raportu w 2015 r. nawet nie zidentyfikowano zagrożeń dla bezpieczeństwa w cyberprzestrzeni, nie wypracowano żadnej spójnej strategii działania. Prezesowi Rady Ministrów zarzucono, że unikał odpowiedzialności za politykę bezpieczeństwa w cyberprzestrzeni, co mogło pogłębiać spory kompetencyjne. Ponadto właściwy dla omawianej przestrzeni w tamtym okresie Minister Administracji i Cyfryzacji nie wypełniał należycie swoich zadań, ale i tak, co wskazał NIK, gdyby chciał je realizować, to nie miał ku temu ani kompetencji, ani wystarczających środków. Negatywnie na jakość bezpieczeństwa w sieci wpływało prawo, które było nieadekwatne do zadań i wadliwie sformułowane. Pozytywnie

---

[19] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństw sieci i systemów informatycznych na terytorium Unii*, Dziennik Urzędowy Unii Europejskiej, L 194, 19.07.2016.

[20] *NIK o bezpieczeństwie w cyberprzestrzeni*, 30.06.2015, https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html, 6.04.2018.

zaś zostały ocenione wysiłki na rzecz cyberbezpieczeństwa podejmowane w ramach Ministerstwa Obrony Narodowej (MON) i w Agencji Bezpieczeństwa Wewnętrznego (ABW). NIK wreszcie też krytycznie ocenił wcześniejszą polską „strategię cyberbezpieczeństwa", zatwierdzoną przez Rząd RP w 2013 r. (była to *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*). Miażdżącą ocenę NIK wystawił całości struktur państwa polskiego do 2015 r., wskazując, że nie podjęto w zakresie bezpieczeństwa teleinformatycznego w Polsce żadnych prac legislacyjnych, nie monitorowano pod tym kątem prawa, nie wskazano pożądanych kierunków zmian w prawie. Natomiast znane rozwiązania prawne pod kątem między innymi zbierania informacji o incydentach w sieci uznano za wadliwe, tak jak i inne zapisy z *Prawa telekomunikacyjnego* pod omawianym kątem. Swoistym substytutem braku spójnych działań instytucji państwa do 2015 r. były wysiłki podejmowane przez Naukową i Akademicką Sieć Komputerową (NASK) i ABW, czego owocem był system wczesnego ostrzegania ARAKIS[21]. Jak napisano w dokumencie *Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*:

> Każde znaczące zakłócenie funkcjonowania cyberprzestrzeni, czy to o charakterze globalnym, czy lokalnym, będzie miało wpływ na bezpieczeństwo obrotu gospodarczego, poczucie bezpieczeństwa obywateli, sprawność funkcjonowania instytucji sektora publicznego, przebieg procesów produkcyjnych i usługowych, a w rezultacie na ogólnie pojmowane bezpieczeństwo narodowe.

W polskiej strategii bezpieczeństwa cybernetycznego dokładnie zdefiniowano, skąd mogą pochodzić zagrożenia, a będą ich źródłem: grupy przestępcze – terrorystyczne i działające przez wzgląd na chęć zysku; grupy na usługach państw obcych. Ogólnie celem działalności wymierzonej w cyberbezpieczeństwo staje się według władz polskich nie samo uzyskanie informacji, ale przede wszystkim zapewnienie dzięki jej pozyskaniu destabilizacji państwa[22]. Stworzenie strategii

[21] Tamże.

[22] *Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022.*

cyberbezpieczeństwa RP motywuje się przede wszystkim dwojakim obliczem obecnego rozwoju teleinformatycznego, który staje się „kręgosłupem postępu". W tej mierze sektor teleinformatyczny tworzy możliwości rozwoju gospodarczego i społecznego w niespotykanym dotąd tempie, ale też i jest narażony na działania mające za zadanie stawianie barier temu rozwojowi. Najistotniejszym celem twórców było uzyskanie, dzięki wypracowaniu spójnej strategii, wysokiego stopnia odporności krajowych systemów informatycznych na zagrożenia. Rząd RP wyraził w dokumencie stanowisko, zgodnie z którym Internet uznany jest za „istotny element funkcjonowania społeczeństwa" i jako taki ma pozostawać wolny i otwarty.

W polskiej strategii wskazano:

- cele w zakresie cyberbezpieczeństwa teleinformatycznego;
- główne podmioty zaangażowane we wdrażanie strategii w zakresie bezpieczeństwa teleinformatycznego;
- ramy zarządzania służące realizacji celów krajowej strategii w zakresie bezpieczeństwa teleinformatycznego;
- na potrzebę zapobiegania i reagowania w odniesieniu do incydentów oraz przywracania stanu normalnego zakłóconego incydentem, w tym zasady współpracy pomiędzy sektorami publicznym i prywatnym;
- podejście do oceny ryzyka;
- kierunki podejścia do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa;
- działania odnoszące się do planów badawczo-rozwojowych w zakresie bezpieczeństwa teleinformatycznego;
- podejście do współpracy międzynarodowej w zakresie cyberbezpieczeństwa[23].

Strategia ta zawiera cztery cele szczegółowe, które streścić można następująco: 1) osiągnięcie zdolności koordynowania w skali kraju

Poszanowanie praw i wolności w cyberprzestrzeni. Kompleksowe podejście do bezpieczeństwa. Cyberbezpieczeństwo istotnym elementem polityki państwa, https://www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627–4050-a6f4–5cd3–351aa025be09, 05.04.2017.

[23] Tamże.

działań, które będą służyły zabezpieczeniu bezpieczeństwa cybernetycznego teleinformatycznego państwa; 2) wzmacnianie zdolności do przeciwdziałania; 3) działanie na rzecz wzrostu kompetencji i potencjału narodowego; 4) budowa silnej pozycji międzynarodowej Polski w zakresie cyberbezpieczeństwa. Wyrazem rozumienia przez Rząd RP rzeczywistości społeczeństwa informacyjnego jest uwzględnienie wysokiej dynamiki procesów w cyberprzestrzeni i wskazanie konieczności ciągłego monitorowania regulacji prawnych i ich adekwatności do zmieniającego się otoczenia systemowego. W strategii nie wskazano definicji cyberprzestrzeni, ale znajdują się w niej jasne wskazania zagrożeń cyberbezpieczeństwa. Kluczowym elementem dla powodzenia zapewniania bezpieczeństwa w cyberprzestrzeni ze strony władz państwowych jest w ujęciu tego dokumentu współpraca międzynarodowa o charakterze analogicznym do zagrożeń, czyli jest to współpraca transgraniczna. Ważnym aspektem polskiej strategii cyberbezpieczeństwa jest przestrzeń militarna i podkreślenie działań Służb Zbrojnych RP w zapewnieniu tego wymiaru bezpieczeństwa[24].

Rząd założył w strategii, że do 2022 r. podniesiony zostanie poziom cyberbezpieczeństwa RP przy jednoczesnym poszanowaniu praw i wolności obywateli. Właśnie zmiany w prawie są elementem strategii cyberbezpieczeństwa RP; za inicjowanie zmian w prawie pod tym kątem odpowiadają właściwi ministrowie. W strategii cyberbezpieczeństwa RP na lata 2017–2022, choć nie znajduje się tam definicja cyberprzestrzeni, wskazano, że cyberprzestrzeń RP jest rozumiana podobnie jak w poprzednich dokumentach, więc jako „cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)”[25].

Dla skoordynowania wysiłków na rzecz zapewnienia realizacji zapisów strategii, podjęto decyzję o powołaniu Narodowego Centrum

[24] *Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, dz. cyt.

[25] Z. Chmielewski, *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich,* „Studia z Polityki Publicznej” 2016, nr 2 (10), s. 107.

Cyberbezpieczeństwa (NCC), które jest obecnie czynne całą dobę, siedem dni w tygodniu. NCC działa w strukturach NASK i zostało otwarte 4 lipca 2017 r. NCC podzielono na cztery piony: badawczo-rozwojowy, operacyjny, szkoleniowy i analityczny. Na incydenty naruszające bezpieczeństwo sieci reaguje działający w ramach pionu operacyjnego CERT Narodowy. Jak zauważyła minister Anna Streżyńska, ochronie w ramach zapewnienia cyberbezpieczeństwa ze strony państwa będą podlegać szczególnie pojedynczy obywatele, a nie tylko instytucje publiczne, ponieważ to obywatele nie mają możliwości zapewnić sobie bezpieczeństwa w sieci samodzielnie wobec generowanych tam zagrożeń[26]. Wobec licznych incydentów w sieci w latach 2016–2018, a tych według NASK-PIB (z zastrzeżeniem, że statystyki nie obejmują wszystkich incydentów w sieci, było sporo) było około 230 mln – w tym: 2,3 mln serwerów pozwalających na amplifikację ataków DDoS; około 1,5 mln botów; 772 tys. stron phisingowych; 670 tys. złośliwych stron WWW, 270 aktywnych serwerów C&C; około 2,9 mln serwerów podatnych na znane podatności (są to dane tylko odnoszące się do Polski). Ponadto NASK odnotował 3128 incydentów z 21711 zgłoszeń indywidualnych bądź z instytucji, a w tym: 1439 dotyczyło oszustw; 854 złośliwego oprogramowania; 262 prób włamań; 157 gromadzenia informacji; 118 włamań; 53 ataki DoS/DDoS. Na tak ogromną skalę incydentów NCC (w tym jednostka CERT Polska) dysponuje niewielkim, wynoszącym rocznie około 8 mln zł budżetem[27].

W ujęciu ponadnarodowym Polska współpracuje w zakresie cyberbezpieczeństwa w ograniczonym zakresie i raczej w warunkach konkurencji o palmę pierwszeństwa w Europie Środkowo-Wschodniej z państwami Grupy Wyszehradzkiej. Współpraca ta blednie na tle rzeczywistych wysiłków państw V4, które ukierunkowują się na współpracę z globalnymi liderami przestrzeni cyfrowej. Szczególnie

[26] *NCC – na straży cyberbezpieczeństwa,* Ministerstwo Cyfryzacji, https://www.gov.pl/cyfryzacja/ncc-na-strazy-cyberbezpieczenstwa, 6.04.2018.

[27] Dane pozyskane przez autora z NASK w drodze zapytania o informację publiczną na podstawie *Ustawy o dostępie do informacji publicznej* z 2001 r. Odpowiedź na zapytanie o informację publiczną z NASK do Marcina Wałdocha z 7 maja 2018 r. Zob. archiwum autora.

w tej mierze istotne są działania na forum Unii Europejskiej[28]. Bezpieczeństwo cybernetyczne UE jest uwzględnione w dokumencie *Dyrektywa Parlamentu Europejskiego i Rady UE z 2016 r. z dnia 6 lipca 2016 r.* Sieci i działalność systemów i usług informatycznych mają zasadnicze znaczenie dla działalności gospodarczej i społecznej. Podkreśla się w tym względzie znaczenie sieci dla wysokorozwiniętego rynku wewnętrznego. Tym samym skala i częstotliwość oraz wpływ incydentów sieci ma kluczowe znaczenie dla utrzymania funkcjonowania Internetu i systemów informatycznych. Sieć ułatwia przepływ transgraniczny towarów i usług oraz osób. Stąd bezpieczeństwo sieci ma zasadnicze znaczenie dla bezpieczeństwa rynku wewnętrznego. Na bazie deklaracji postanowiono powołać wspólną grupę z przedstawicielami państw członkowskich, Komisji Europejskiej oraz Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA). Grupę tę tworzy się dla wzmocnienia współpracy, jak i dla określenia strategicznych celów grupy. Organizację tę powołano, aby chronić instytucje unijne, administrację publiczną, ale też żeby w jak najwyższym stopniu podnieść kulturę korzystania z sieci i rozwiązań cyfrowych. Do 2016 r. brakowało bowiem wspólnego podejścia do sieci i jej operatorów w dziedzinie bezpieczeństwa w sieci. Nowa dyrektywa unijna przewiduje również udział uczelni w zakresie wzmacniania cyberbezpieczeńswa, to na uczelniach wyższych mają powstawać innowacyjne projekty związane ze wzrostem możliwości w zakresie cyberbezpieczeństwa administracji publicznej i obywateli. Dyrektywa ta jest też w zasadzie wyrazem chęci wdrażania rozwiązań systemowych na poziomie całej Unii. Nie wyczerpuje ona jednak możliwego zestawu działań na rzecz cyberbezpieczeństwa i umożliwia operatorom usług kluczowych oraz dostawcom usług teleinformatycznych wdrażanie rozwiązań o wyższym rygoryzmie bezpieczeństwa. W dokumencie podkreślono wagę istniejących

[28] B. Olszewski, *Perspektywy regionalizacji cyberbezpieczeństwa w ramach Grupy Wyszehradzkiej*, https://www.researchgate.net/profile/Boguslaw_Olszewski/publication/316861426_Perspektywy_regionalizacji_cyberbezpieczenstwa_w_ramach_Grupy_Wyszehradzkiej/links/5914af08aca27200fe4e8c2e/Perspektywy-regionalizacji-cyberbezpieczenstwa-w-ramach-Grupy-Wyszehradzkiej.pdf, 3.05.2018.

instytucji europejskich gwarantujących bezpieczeństwo UE, w tym Europejskiego Systemu Nadzoru Finansowego oraz Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych, które pełnią rolę nadzorczą i kontrolną nad agencjami ratingowymi i repozytoriami transakcji. Bezpieczeństwo cybernetyczne w tym względzie odnosi się do potrzeby zapewnienia ciągłości pracy rynków finansowych, stąd dużą wagę przykłada się do szacowania ryzyka operacyjnego. Twórcy dyrektywy wskazali także na dużą wagę i znaczenie internetowych platform handlowych dla gospodarki w społeczeństwie informacyjnym. Istotne znaczenie w dyrektywie przyjmują takie kategorie związane z cyberprzestrzenią jak: wyszukiwarki internetowe, usługi przetwarzania w chmurze, a ponadto sporządzenie wykazu usług kluczowych, rozpatrzenie wspólnego wykazu czynników międzysektorowych w celu ustalenia, czy ewentualny incydent mógłby mieć istotny skutek zakłócający, procesy konsultacji między państwami w przypadku usługodawców świadczących swoje usługi na terytorium więcej niż jednego państwa. Usługi kluczowe i ich operatorów ocenia się pod kątem tego, które z nich są rzeczywiście istotne dla sektora danego pod kątem utrzymania krytycznej działalności gospodarczej i społecznej. Usługodawcę identyfikuje się jako kluczowego, dzięki temu, że weryfikuje się jego działalność z listą tzw. usług kluczowych – jeśli podmiot je wykonuje, to jest dostawcą kluczowym. W szacowaniu zasięgu i wagi incydentów w sieci w zapisach rzeczonej dyrektywy zalecono, aby wzięto pod uwagę liczbę użytkowników danej usługi, którą dotknął incydent, oraz liczbę ogólną użytkowników danego dostawcy usług. Elementem oceny ryzyka płynącego z potencjalnego incydentu jest wskazanie, jak ten incydent można zniwelować, czyli ile to zajmie czasu i jakim nakładem środków uda się naprawić wyrządzone szkody oraz jakie będzie to miało przełożenie na bezpieczeństwo publiczne. Dyrektywa posiada zapisy, które regulują konieczność posiadania przez państwa odpowiedniej infrastruktury technicznej oraz organizacyjnej dla przeciwdziałania atakom cybernetycznym. Tym samym wprowadzono kategorię CSIRT, która to jest ważna dla określania właściwych organów lub zespołów reagowania na incydenty bezpieczeństwa komputerowego. Od wszystkich państw oczekuje się, że wdrażając

przepisy dyrektywy, będą konsultowały się z ENISA. Szczególnie ENISA ma pomagać państwom członkowskim poprzez analizy ich strategii bezpieczeństwa w sieci. Według dyrektywy bezpieczeństwo sieci i systemów informatycznych obejmuje bezpieczeństwo danych przechowywanych, przekazywanych i przetwarzanych. Jak napisano w dyrektywie, próbując zabezpieczyć informacje i dane:

> Dostawcy usług cyfrowych powinni zapewnić poziom bezpieczeństwa współmierny do stopnia ryzyka, na jakie narażone jest bezpieczeństwo świadczonych przez nich usług cyfrowych, ze względu na znaczenie tych usług dla działalności innych przedsiębiorców Unii[29].

Dyrektywa unijna wyznaczyła konieczność – obowiązek posiadania przez państwa członkowskie strategii w zakresie bezpieczeństwa sieci i systemów informatycznych. Utworzono wspomnianą przeze mnie wcześniej grupę współpracy, tworząc sieć reagowania na incydenty w sieci pod nazwą CSIRT. W europejskiej dyrektywie wskazano literalnie znaczenie takich sformułowań jak sieci i systemy informatyczne, przez co rozumie się sieci łączności elektronicznej. Bezpieczeństwo sieci i systemów informatycznych oznacza odporność sieci i systemów informatycznych przy danym poziomie zaufania. Incydent – oznacza każde zdarzenie, które ma rzeczywiście niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych. Ryzyko oznacza każdą dającą się racjonalnie określić okoliczność lub zdarzenie, które ma potencjalny niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych. Co interesujące, UE pozostawia państwom dowolność w kreowaniu strategii, ale w ograniczonym zakresie, bowiem w dyrektywie zaznaczano, że owa strategia musi posiadać: cele i priorytety w zakresie bezpieczeństwa sieci i systemów informatycznych, ramy zarządzania służące realizacji celów i priorytetów krajowej strategii w zakresie bezpieczeństwa

[29] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństw sieci i systemów informatycznych na terytorium Unii*, Dziennik Urzędowy Unii Europejskiej, L194, 19.07.2016, s. 8.

sieci i systemów informatycznych, w tym role i zakresy obowiązków organów rządowych i innych właściwych podmiotów, określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym współpracy między sektorami publicznym i prywatnym, wskazówki odnoszące się do programów edukacyjnych, informacyjnych, i szkoleniowych dotyczących strategii w zakresie bezpieczeństwa sieci, wskazówki odnoszące się do planów badawczo-rozwojowych dotyczących strategii w zakresie bezpieczeństwa sieci i systemów informatycznych, plan oceny ryzyka służący ocenie ryzyka, wykaz różnych podmiotów zaangażowanych we wdrażanie strategii w zakresie bezpieczeństwa sieci i systemów informatycznych. Państwa mogą się też zwracać o pomoc do ENISA w opracowywaniu strategii cyberbezpieczeństwa. Państwa zostały zobowiązane do przekazywania Komisji swoich strategii w terminie trzech miesięcy od ich uchwalenia. ENISA ma gwarantować wymianę najlepszych praktyk. Ponadto strategie cyberbezpieczeństwa muszą uwzględniać bezpieczeństwo systemów i obiektów; postępowanie w przypadku incydentu; zarządzanie ciągłością działania; monitorowanie, audyt i testowanie; zgodność z normami międzynarodowymi. A na podstawie dyrektywy wskazano, że dostawcy usług spoza Unii muszą posiadać swoje przedstawicielstwo na terenie Unii. Do 9 maja 2019 r. przyjęto datę graniczną dla oceny spójności polityk narodowych w zakresie przyjętych strategii cyberbezpieczeństwa. Państwa zostają dyrektywą również zobowiązane do ustanowienia przynajmniej jednego organu nadzorującego cyberbezpieczeństwo, który przyjmuje się nazywać w nomenklaturze UE „właściwym organem”[30]. Stąd tak istotne wydaje się postrzeganie zagadnień cyberbezpieczeństwa w Polsce nie tylko poprzez pryzmat polskiej strategii, ale i jej swoistych ram, którą tworzy wskazana dyrektywa unijna.

W Polsce odrębne, pozapaństwowe instytucje tworzą swoje centra cyberbezpieczeństwa, w większości z myślą o bezpieczeństwie swoich klientów. Tego rodzaju centrum otworzył Związek Banków Polskich w 2016 r.[31] Dzieje się to w odpowiedzi na poczucie zagroże-

[30] Tamże.

[31] *Otwarcie Bankowego Centrum Cyberbezpieczeństwa*, https://zbp.pl/wydarze-

nia w cyberprzestrzeni, które przejawiają Polacy. W 2017 r. trzech na czterech Polaków nie było pewnych bezpieczeństwa systemów elektronicznej bankowości. Ogólnie zaś tylko 21% Polaków czuło się osobiście odpowiedzialnymi za swoje bezpieczeństwo w świecie wirtualnym, oczekując od instytucji publicznych ochrony w tym zakresie[32]. Innym przykładem mogą być firmy przemysłowe oraz inne usługowe, które wydają w Polsce coraz więcej pieniędzy na zapewnienie sobie cyberbezpieczeństwa. Jak się notuje, *phising* był głównym rodzajem zagrożenia (39% przypadków)[33]. Jest to charakterystyczne dla Polski, że firmy samodzielnie starają się sprostać wyzwaniom cyberbezpieczeństwa. Za hasło propagandowe w zderzeniu z faktami należy więc uznać deklaracje polityków, którzy twierdzą, jak premier rządu RP Mateusz Morawiecki, że cyberbezpieczeństwo stanie się polską kompetencją narodową[34], gdyż Polsce daleko do liderów cyberbezpieczeństwa w skali globalnej.

Przypadek nowozelandzki

Nowa Zelandia, podobnie jak Polska, jest państwem unitarnym, wykazuje się jednak znacznymi różnicami ustrojowymi i o innym typem kultury politycznej. Jest to państwo stosunkowo młode oraz silnie związane z Koroną Brytyjską, bowiem nadal głową państwa pozostaje królowa brytyjska. W Nowej Zelandii panuje reżim demokratyczny o cechach liberalnych przy systemie rządów

---

nia/archiwum/wydarzenia/2016/lipiec/otwarcie-bankowego-centrum-cyberbezpieczenstwa, 23.04.2018.

[32] *3 na 4 Polaków nie jest pewnych bezpieczeństwa systemów bankowości elektronicznej*, „newsrm.tv" 30.10.2017, http://newsrm.tv/komunikat-pr/3–4-polakow-pewnych-bezpieczenstwa-systemow-bankowosci-elektronicznej/, 3.05.2018.

[33] PAP, *Cyberataki: 96 proc. firm w Polsce było na celowniku hakerów*, „Business Insider Polska" 23.03.2017, *https://businessinsider.com.pl/wiadomosci/cyberbezpieczenstwo-firm-w-polsce/41tn5b0*, 23.04.2018.

[34] W. Kulik, *Cyberbezpieczeństwo polską „kompetencją narodową"*, Benchmark.pl, 20.06.2017, http://www.benchmark.pl/aktualnosci/cyberbezpieczenstwo-polska-kompetencja-narodowa.html, 23.04.2018.

gabinetowo-parlamentarnych. Władza uchwałodawcza skupiona jest w unikameralnym parlamencie. Nowozelandzka strategia bezpieczeństwa znalazła się według pakistańskich badaczy na 4. miejscu spośród 12 analizowanych państw wysoko rozwiniętych[35]. Natomiast według Globalnego Wskaźnika Cyberbezpieczeństwa w 2014 r. Nowa Zelandia jest plasowana na 4. miejscu na świecie oraz na 4. miejscu wśród państw Azji i Pacyfiku, na 2. miejscu za Malezją i Australią[36]. Według badania z 2017 r. GCI dla Nowej Zelandii wynosiło 0,718, co dawało Nowej Zelandii 19. miejsce w 2017 r. na świecie i dopiero 6. miejsce w regionie Azji i Pacyfiku, gdzie na 1. miejscu (nawet przed USA) w 2017 r. został wskazany Singapur ze wskaźnikiem 0,925[37]. Dla Nowej Zelandii w 2017 r. wskaźnik GCI był nieco niższy aniżeli w 2014 r., kiedy Nowa Zelandia uzyskała 0,735 GCI[38].

Cyberprzestrzeń jest definiowana w strategii cyberbezpieczeństwa Aotearoa jako Internet i urządzenia ICT (technologie informacyjne i komunikacyjne) podłączone do Internetu; cyberbezpieczeństwo posiada zaś w strategii swoją jasną i klarowną definicję[39]. Najnowsza strategia cyberbezpieczeństwa Nowej Zelandii została stworzona w 2015 r. i zastąpiła wcześniejszy dokument z 2011 r. Nowozelandzka strategia posiada cztery główne cele, tj. 1) podnoszenie odporności na zagrożenia cyberprzestrzeni; 2) zwiększenie potencjału nowozelandzkiego w cyberprzestrzeni; 3) prewencja; 4) współpraca międzynarodowa. Dużą wagę nowozelandzcy twórcy strategii cyberbezpieczeństwa przyłożyli do udziału sektora prywatnego oraz organizacji pozarządowych (takich jak NZ Internet Taskforce) w zapewnieniu bezpieczeństwa cyberprzestrzeni. Odpowiedni poziom bezpieczeństwa sieci gwarantuje według Nowozelandczyków stabilny rozwój gospodarczy oraz transparentność mechanizmów rynkowych. Dzięki zapewnieniu bezpieczeństwa użytkowników cyberprzestrzeni Nowozelandczycy mają nadzieję pozostawać państwem rozpoznawanym na

[35] N. Shafqat, A. Masood, dz. cyt., s. 130.

[36] *Global Cybersecurity Index 2014*, dz. cyt.

[37] *Global Security Index 2017*, Geneva 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01–2017-R1-PDF-E.pdf, 16.04.2018.

[38] *Global Cybersecurity Index 2014*, dz. cyt.

[39] N. Shafqat, A. Masood, dz. cyt., s. 132.

świecie jako miejsce, gdzie można w bezpieczny sposób inwestować oraz magazynować dane. Jednocześnie zagrożenia płynące z świata wirtualnego rozpoznawane są w Nowej Zelandii jako elementy nastające na bezpieczeństwo narodowe. Stąd zapewnienie bezpieczeństwa w tej przestrzeni uznaje się również za element wypełniania zobowiązania nakładanego przez prawa człowieka, czyli zobowiązania do możliwości niezakłóconej wymiany informacji, swobody ekspresji poglądów i wolności słowa przy zachowaniu prawa do prywatności. Wśród instytucji odpowiedzialnych za zapewnienie bezpieczeństwa w cyberprzestrzeni wymieniono w nowozelandzkiej strategii: Grupę Policyjną ds. Przestępstw Elektronicznych ustanowioną w 1984 r., Narodowe Centrum Cyberbezpieczeństwa ustanowione w 2011 r., Narodową Policję Cybernetyczną ustanowioną w 2012 r. Rząd podjął też wysiłki na rzecz wzmocnienia świadomości zagrożeń w społeczeństwie w kontakcie z cyberprzestrzenią w latach 2012 i 2013. Jak podaje się w wynikach badań, w 2014 r. 22% nowozelandzkich internautów doznało włamania na konto e-mailowe, 83% nigdy nie zmieniało haseł do swoich kont, 34% nie posiadało haseł do swoich smartfonów, a 26% wierzyło, że osobiście nie są celami ataków cybernetycznych. Te dane wskazują potrzebę prowadzenia kampanii na rzecz wzrostu świadomości płynących z świata wirtualnego dla jego użytkowników[40]. Stąd powołano inicjatywę Connect Smart, której zadaniem jest przede wszystkim edukacja społeczeństwa w zakresie cyberbezpieczeństwa. Dla Nowej Zelandii jest charakterystycznym to, że państwo to w wielu obszarach ukierunkowuje się na współpracę z Australią, podobnie jest w zakresie cyberbezpieczeństwa. Oba państwa ustanowiły transtasmańską współpracę w tym obszarze poprzez wymianę informacji i wspólne ćwiczenia. Drugą płaszczyzną zacieśniania współpracy są wspólne działania podejmowane w zakresie cyberbezpieczeństwa przez Nową Zelandię z pozostałymi państwami anglosaskimi, czyli z Kanadą, Stanami Zjednoczonymi i Wielką Brytanią. W wymiarze międzynarodowym

[40] *New Zealand's Cyber Security Strategy 2015*, https://www.dpmc.govt.nz/sites/default/files/2017–03/nz-cyber-security-strategy-december-2015.pdf, 26.04.2018.

Nowa Zelandia bierze udział także w pracach grupy Five Eyes oraz w ramach ASEAN[41].

W zakresie cyberbezpieczeństwa Nowa Zelandia inaczej aniżeli w każdym innym wymiarze bezpieczeństwa nie czerpie przewagi nad innymi państwami z faktu swej geograficznej izolacji. Ataki cybernetyczne nie znają po prostu granic geograficznych, a zagrożenie ma wymiar globalny i dotyczy również tak odległego państwa jak kraj kiwi. Dodatkowo o ile wcześniej można było rozpoznać przeciwnika, o tyle, co słusznie zauważają Nowozelandczycy, obecnie anonimowość stałą się jedną z cech charakterystycznych doby informacjonizmu, a cyberprzestrzeń stała się kluczowym wymiarem konfliktu asymetrycznego. Stąd zarówno poszczególne, pojedyncze nawet osoby, jak i niewielkie organizacje i małe państwa potencjalnie stanowią duże zagrożenie dla całych państw, takich jak Nowa Zelandia. Nowozelandczycy w tym względzie zauważają, że około 30 państw świata już zadeklarowało użycie cyberprzestrzeni jako elementu pola walki, nie tylko w sensie defensywnym, ale przede wszystkim jako środek ofensywny. W tym względzie pisze się w Nowej Zelnadii nawet o swoistej „militaryzacji cyberprzestrzeni" w zależności od rodzaju kultury politycznej wybranych państw. W Nowej Zelandii otwarto Centrum Cyberbezpieczeństwa 28 września 2011 r. Politycznym wymiarem problemów cyberbezpieczeństwa Nowej Zelandii o znaczeniu międzynarodowym było między innymi zakwestionowanie bezpieczeństwa użycia urządzeń teleinformatycznych chińskiej firmy Huawei, którą Stany Zjednoczone, Australia i Nowa Zelandia oskarżają o szpiegostwo na rzecz rządu Chińskiej Republiki Ludowej. Takie przypadki powodują wzrost świadomości politycznej Nowozelandczyków i co za tym idzie ukierunkowywania się na współpracę w zakresie cyberbezpieczeństwa na poziomie międzynarodowym[42].

Od kwietnia do czerwca 2017 r. w Nowej Zelandii powołany do życia w kwietniu 2017 r. CERT odnotował 364 cyberataki; aż 34%

[41] *New Zealand's Cyber Security Strategy 2016. Action Plan Annual Report*, https://www.dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-action-plan-annual-report-2016, 26.04.2018.

[42] J. Burton, *Cyber security: the strategic challenge and New Zealand's response*, „New Zealand International Review" 2013, vol. 38, s. 5–8.

z tych incydentów było związane z tzw. phisingiem, czyli z wyłudzeniami danych i pieniędzy w sieci. Te incydenty kosztowały Nową Zelandię według tamtejszego CERT około 700 tys. dolarów nowozelandzkich. Dodatkowo zauważono wzrost użycia tzw. *ransomware*, czyli oprogramowań szantażujących użytkowników i żądających okupu. Największe zaś nasilenie cyberatakami w raportowanym okresie miało miejsce w regionie Wellington, gdzie doszło do 82 odnotowanych incydentów wobec 62 w Auckland, co może wskazywać na wagę stolicy jako centrum życia politycznego państwa w optyce cyberprzestępców chcących być może pozyskać także dane istotne dla życia politycznego (tym bardziej że wśród strat poniesionych przez poszkodowanych wymienia się w liczbie 8% ogólnych szkód straty wynikające z utraty danych). Uniknięcie i przeciwdziałanie rodzajom zagrożeń i incydentów w cyberprzestrzeni jest nieodzownie związane z rozwijaniem przez Nową Zelandię współpracy międzynarodowej w zakresie cyberbezpieczeństwa[43].

W Nowej Zelandii funkcjonuje dokument pod nazwą *First National Cybercrime Strategy 2014–2017*. Policja oferuje również treningi z zakresu cybebezpieczeństwa przedstawicielom wymiaru sprawiedliwości.

Zakończenie

W wyniku przeprowadzonego badania potwierdzono hipotezę, stanowiącą przypuszczenie, że strategie cyberbezpieczeństwa Nowej Zelandii i Polski wykazują różnice wynikające ze swoistości systemów politycznych tych państw.

Ujawniono bowiem swoistości związane z charakterystyką wskazanych strategii cyberbezpieczeństwa, a odnoszące się zarówno do kultury politycznej (skala zaangażowania), jak i do systemów politycznych dwóch porównywanych pod tym kątem państw. Polska jest bowiem zakotwiczona w perspektywach na cyberbezpieczeństwo

[43] CERTNZ, *Quarterly Report*, https://www.cert.govt.nz/assets/Uploads/Quarterly-report/CERT-NZ-Report-Apr-Jun17.pdf, 23.04.2018.

wyznaczonych przez UE i NATO, czyli w północnoatlantyckim systemie bezpieczeństwa. Zaś Nowa Zelandia tworzy swą strategię cyberbezpieczeństwa i jej wizje w odniesieniu do bliskich relacji z Wielką Brytanią oraz pozostałymi państwami kręgu kultury anglosaskiej, tj. Australią, Kanadą i USA, ukierunkowując się w wyższym stopniu niż Polska na współpracę bilateralną.

Tabela 1. Różnice i podobieństwa strategii cyberbezpieczeństwa Nowej Zelandii i Polski

	Nowa Zelandia	**Polska**
Ocena cyberbezpieczeństwa według indeksu GCI w 2017 r.	0,735, 19. miejsce na świecie	0,622, 33. miejsce na świecie
Rok powstania ostatniej strategii cyberbezpieczeństwa i lata obowiązywania	2015 – do czasu wdrożenia nowej strategii	2017 na lata 2017–2022
Organ odpowiedzialny za wykonanie strategii cyberbezpieczeństwa	Minister Komunikacji	Minister Cyfryzacji
Wiążące przepisy prawa ponadnarodowego dla krajowej strategii cyberbezpieczeństwa, do których odwołali się twórcy strategii	Nie	Tak
Rok powołania komórki CERT	2011	1996
Koncepcja partnerstwa publiczno-prawnego dla cyberbezpieczeństwa	Tak	Tak
Uznanie roli partnerstwa prywatno-publicznego	Tak	Tak
Otwarcie na współpracę międzynarodową	Tak	Tak
Najczęściej występujący rodzaj zagrożenia	*phising*	*phising*
Jedna strategia cyberbezpieczeństwa	Tak	Tak
Ideologia partii władzy wdrażającej ostatnią strategię cyberbezpieczeństwa	Partia Narodowa – ideologia to liberalny konserwatyzm	Prawo i Sprawiedliwość – ideologia to konserwatyzm chrześcijańsko-narodowy

	Nowa Zelandia	**Polska**
Jasna definicja cyberprzestrzeni w strategii	Tak – cyberprzestrzeń to: „Globalna sieć współzależnej infrastruktury informatycznej, sieci telekomunikacyjne oraz komputerowe systemy operacyjne w których odbywa się komunikacja online".	Tak – „cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)".
Nazwa instytucji koordynującej wysiłki na rzecz cyberbezpieczeństwa według zapisów strategii	National Cyber Security Centre	Narodowe Centrum Cyberbezpieczeństwa w ramach NASK
Zapewnianie ochrony praw człowieka, w tym wolności słowa, ekspresji poglądów	Tak	Tak
Akcje edukujące społeczeństwo w zakresie cyberbezpieczeństwa o wymiarze ogólnokrajowym	Tak	Nie – planowane wdrożenie systemu ostrzegania dla obywateli
Główne cele strategii	1) podnoszenie odporności na zagrożenia cyberprzestrzeni; 2) zwiększenie potencjału nowozelandzkiego w cyberprzestrzeni; 3) prewencja; 4) współpraca międzynarodowa	1) osiągnięcie zdolności koordynowania w skali kraju działań, które będą służyły bezpieczeństwu cybernetycznemu i teleinformatycznemu państwa; 2) wzmacnianie zdolności do przeciwdziałania; 3) działanie na rzecz wzrostu kompetencji i potencjału narodowego; 4) budowa silnej pozycji międzynarodowej Polski w zakresie cyberbezpieczeństwa
Określenie tzw. usług krytycznych	Tak	Tak

	Nowa Zelandia	**Polska**
PKB *per capita* w 2016 r.	37 165 USD, 32. miejsce na świecie	27 690 USD, 44. miejsce na świecie
Odwołania w strategiach do organizacji ponadnarodowych i dokumentów prawa międzynarodowego	Tak, do: ICANN (Internetowa Korporacja ds. Nadawania Nazw i Numerów)	Tak, do: UE, NATO, ONZ, OBWE

Źródło: Opracowanie własne na podstawie: International Monetary Fund 2017.

W Nowej Zelandii politycy związani z konserwatystami, tacy jak David Farrar, opowiadają się przeciwko jakiejkolwiek ingerencji rządów narodowych w Internet i jego funkcjonowanie pod pretekstem zwiększania cyberbezpieczeństwa[44]. Charakterystyczne jest zarówno dla strategii cyberbezpieczeństwa Nowej Zelandii jak i Polski to, że obie te strategie obejmują zarówno świat cywilny, jak i wojskowy, kiedy dla innych państw, przykładowo takich jak Stany Zjednoczone i Holandia, utworzono dwie odrębne strategie cyberbezpieczeństwa, jedną dla życia cywilnego, drugą zaś dla wojska[45].

Wysoki wskaźnik GCI dla państw może stanowić ważny odnośnik dla decyzji o prowadzeniu inwestycji oraz jest miernikiem stopnia bezpieczeństwa państwa, który będzie odgrywał coraz większą rolę w międzynarodowej reputacji państw. Wskazane różnice w strategiach cyberbezpieczeństwa Polski i Nowej Zelandii są probierzem twierdzenia o braku możliwości implementacji holistycznego podejścia do zagadnień cyberbezpieczeństwa, pomimo globalnej natury zagrożeń w sieci.

Ujawniają się procesy związane z unifikacją i dywersyfikacją w podejściu do zagadnień bezpieczeństwa w cyberprzestrzeni, co uwidacznia się w przyjmowaniu wzorców uniwersalnych, jak i swoistościach regionalnych wobec wyzwań globalizacji. Na przykładzie

[44] D. Farrar, *Project Speargun was the ditched cyber security project*, „Kiwiblog", 25.09.2016, https://www.kiwiblog.co.nz/2014/09/project_speargun_was_the_ditched_cyber_security_project.html, 6.04.2016.

[45] N. Shafqat, A. Masood, dz. cyt., s. 130.

Polski i Nowej Zelandii można stwierdzić, że państwa tworzą sojusze na rzecz cyberbezpieczeństwa, które zgodne są z dotychczasowymi relacjami tych podmiotów na arenie międzynarodowej. Znaczy to, że sojusze w cyberprzestrzeni podążają za sojuszami w świecie rzeczywistym i transponują do świata wirtualnego uwarunkowania relacji międzynarodowych. Możliwe jest też pogłębianie się uzależnienia państw małych i średnich, które nie są światowymi innowatorami w zakresie technologii teleinformatycznych, od liderów wirtualnej rzeczywistości, co będzie też powodowało nasilanie się zależności tych państw od państw wiodących w polityce międzynarodowej.

Bez względu na różnice ideologiczne strategie cyberbezpieczeństwa stają się egzemplifikacją unifikacji postaw i przyjmowania uniwersalnych postaw instytucji państwowych wobec świata wirtualnego – tak przynajmniej należy wnioskować na bazie niniejszej analizy.

Słabsza pozycja Polski w rankingach cyberbezpieczeństwa od tych zajmowanych przez Nową Zelandię może mieć związek z rocznym PKB *per capita*, które jest wyższe dla kraju kiwi niż dla Polski, co wydatnie odzwierciedla możliwości finansowe w zakresie zapewnienia bezpieczeństwa w świecie wirtualnym, ale może też wskazywać na szersze zjawisko wymagające dalszych badań, a odnoszące się do wskazania relacji między PKB *per capita* a stopniem bezpieczeństwa w cyberprzestrzeni w państwach świata.

Bibliografia

3 na 4 Polaków nie jest pewnych bezpieczeństwa systemów bankowości elektronicznej, „newsrm.tv" 30.10.2017, http://newsrm.tv/komunikat-pr/3–4-polakow-pewnych-bezpieczenstwa-systemow-bankowosci-elektronicznej/, 3.05.2018.

Bajer J., *Badania porównawcze w politologii. Zagadnienia metodologiczne*, „Studia Politicae Universitatis Silesiensis" 2012, nr 8.

Ball J., *Edward Snowden NSA files: secret surveillance and our revelations so far*, „The Guardian" 21.08.2013, https://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations, 16.04.2018.

Burton J., *Cyber security: the strategic challenge and New Zealand's response*, „New Zealand International Review" 2013, Vol. 38.

Burton J., *Small states and cyber security: The case of New Zealand*, „Political Science" 2013, nr 65 (2).

CERTNZ, *Quarterly Report*, https://www.cert.govt.nz/assets/Uploads/Quarterly-report/CERT-NZ-Report-Apr-Jun17.pdf, 23.04.2018.

Chmielewski Z., *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej" 2016, nr 2 (10).

Chodubski A., *Wstęp do badań politologicznych*, Gdańsk 2006.

Czechowska L., *Mały mocarz: Nowa Zelandia jako przykład roli międzynarodowej osiągniętej dobrą reputacją*, „Athenaeum. Polskie Studia Politologiczne" 2017, Vol. 54.

Devetak R., *Teoria krytyczna*, [w:] *Teorie stosunków międzynarodowych*, red. S. Burchill, R. Devetak, A. Linklater, M. Paterson, C. Reus-Smit, J. True, przeł. P. Frankowski, Warszawa 2006.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństw sieci i systemów informatycznych na terytorium Unii, Dziennik Urzędowy Unii Europejskiej, 19.07.2016, L 194/1.

Farrar D., *Project Speargun was the ditched cyber security project*, „Kiwiblog" 25.09.2016, https://www.kiwiblog.co.nz/2014/09/project_speargun_was_the_ditched_cyber_security_project.html, 6.04.2016.

Fourie L., Hettema H., Kingston T., Pang S., Sarrafzadeh A., Watters P., *The Global cybersecurity workforce – an ongoing human capital crisis*, „Global Business and Technology Association Conference" 2014.

Global Security Index 2017, Geneva 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01–2017-R1-PDF-E.pdf, 16.04.2018.

Harris T., *How a handful of the companies control billions of minds every day*, https://www.ted.com/talks/tristan_harris_the_manipulative_tricks_tech_companies_use_to_capture_your_attention#t-65596, 26.04.2018.

Kulik W., *Cyberbezpieczeństwo polską „kompetencją narodową"*, Benchmark.pl 20.06.2017, http://www.benchmark.pl/aktualnosci/cyberbezpieczenstwo-polska-kompetencja-narodowa.html, 23.04.2018.

Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji I współpracy państw*, Katowice 2015.

Mazzucato M., *Governement – investor, risk-taker, innovator*, https://www.ted.com/talks/mariana_mazzucato_government_investor_risk_taker_innovator#t-461560, 26.04.2018.

Menting M., *Global Security Index*, New York 2014, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf, 16.04.2018.

New Zealand's Cyber Security Strategy 2015, https://www.dpmc.govt.nz/sites/default/files/2017–03/nz-cyber-security-strategy-december-2015.pdf, 26.04.2018.

New Zealand's Cyber Security Strategy 2016. Action Plan Annual Report, https://www.dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-action-plan-annual-report-2016, 26.04.2018.

NCC – na straży cyberbezpieczeństwa, Ministerstwo Cyfryzacji, https://www.gov.pl/cyfryzacja/ncc-na-strazy-cyberbezpieczenstwa, 6.04.2018.

NIK o bezpieczeństwie w cyberprzestrzeni, 30.06.2015, https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html, 6.04.2018.

Odpowiedź na zapytanie o informację publiczną z Ministerstwa Cyfryzacji do Marcina Wałdocha z dnia 18 maja 2018 r.

Odpowiedź na zapytanie o informację publiczną z NASK do Marcina Wałdocha z dnia 7 maja 2018 r.

Olszewski B., *Perspektywy regionalizacji cyberbezpieczeństwa w ramach Grupy Wyszehradzkiej*, https://www.researchgate.net/profile/Boguslaw_Olszewski/publication/316861426_Perspektywy_regionalizacji_cyberbezpieczenstwa_w_ramach_Grupy_Wyszehradzkiej/links/5914af08aca27200fe4e8c2e/Perspektywy-regionalizacji-cyberbezpieczenstwa-w-ramach-Grupy-Wyszehradzkiej.pdf, 3.05.2018.

O'Neil C., *Broń matematycznej zagłady. Jak algorytmy zwiększają nierówności i zagrażają demokracji*, przeł. M.Z. Zieliński, Warszawa 2017.

Otwarcie Bankowego Centrum Cyberbezpieczeństwa, https://zbp.pl/wydarzenia/archiwum/wydarzenia/2016/lipiec/otwarcie-bankowego-centrum-cyberbezpieczenstwa, 23.04.2018.

PAP, *Cyberataki: 96 proc. firm w Polsce było na celowniku hakerów*, „Business Insider Polska" 23.03.2017, https://businessinsider.com.pl/wiadomosci/cyberbezpieczenstwo-firm-w-polsce/41tn5b0, 23.04.2018.

Population clock, http://archive.stats.govt.nz/tools_and_services/population_clock.aspx?url=/tools_and_services/population_clock.aspx, 26.04.2018.

Shafqat N., Masood A., *Comparative analysis of various national security strategies*, „International Journal of Computer Science and Information Security" 2016, Vol. 14, No. 1.

Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Poszanowanie praw i wolności w cyberprzestrzeni. Kompleksowe podejście do bezpieczeństwa. Cyberbezpieczeństwo istotnym elementem polityki państwa, https://www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627–4050-a6f4–5cd3–351aa025be09, 5.04.2017.

Tentative Timeframe, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv3_documents/Tentative%20timeframe.pdf, 16.04.2018.

Cybersecurity strategies of New Zealand and Poland in the process of globalization

Summary: In this paper an author conduct comparative analysis of New Zealand and Poland cybersecurity strategies. During this research a hypothesis was confirmed that cybersecurity strategies of analyzed countries differ because of their political systems of these countries. Moreover an author has highlighted that alliances known from real world are transformed into cyberspace. Thus New Zealand stay close, when creating cybersecurity, to USA, Australia and Canada, when Poland is committed to the European Union structures.

Keywords: cybersecurity, New Zealand, Poland, globalization, comparative analysis