Krzysztof Kaczmarek*

Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii

Streszczenie

Rozwój sieci telekomunikacyjnych spowodował głębokie przemiany społeczne i polityczne. Powszechny dostęp do internetu spowodował, że znaczna część aktywności społecznych przeniosła się do świata wirtualnego. Jednak ta powszechność spowodowała pojawienie się nowych typów poważnych zagrożeń. Obecnie zdalnie mogą być przeprowadzane ataki terrorystyczne czy prowadzone działania wojenne. Liczące się na arenie międzynarodowej państwa posiadają własne służby działające w cyberprzestrzeni. Ze względu na zaszłości historyczne i położenie geopolityczne Finlandia i Estonia są często traktowane przez Kreml jako strefy wpływu Rosji. W celu osiągnięcia swoich celów państwo to wywiera presję na państwa będące historycznie częścią imperium rosyjskiego przy użyciu wszystkich możliwych środków, w tym przy użyciu sieci telekomunikacyjnych. Sztandarowym przykładem takiego działania był cybernetyczny atak na Estonię w 2007 r.

Słowa kluczowe: cyberbezpieczeństwo, NATO, Finlandia, Estonia, społeczeństwo informacyjne, telekomunikacja, terroryzm, postęp technologiczny, technologie informacyjne, komunikacja

* Dr Krzysztof Kaczmarek, Wydział Humanistyczny, Politechnika Koszalińska, e-mail: puola@tlen.pl, ORCID: 0000-0001-8519-1667.

Wstęp

Współcześnie dokonujący się postęp technologiczny w sposób wielopłaszczyznowy oddziałuje na niemal wszystkie aspekty funkcjonowania społeczeństw i państw. W odniesieniu do zmian będących skutkiem tego postępu często używanym terminem jest „społeczeństwo informacyjne", które jednak nie jest w sposób jednoznaczny zdefiniowane. Pojęcie to charakteryzuje się wielopłaszczyznowością i różnorodnością definicji[1]. Część autorów specjalizujących się w tej problematyce określa dane społeczeństwo informacyjnym, jeżeli w odniesieniu do niego przetwarzanie informacji z wykorzystaniem technologii informacyjnych i komunikacyjnych stanowi znaczącą wartość ekonomiczną, społeczną i kulturową[2]. Sama kolokacja „społeczeństwo informacyjne" we współczesnym znaczeniu pojawiła się po raz pierwszy w japońskich naukach społecznych na początku lat 60. XX wieku. W tamtym okresie funkcjonowały jeszcze inne proto-pojęcia opisujące zmiany społeczne spowodowane rozwijającymi się technologiami i powszechniejszym i szybszym dostępem do informacji takie jak „społeczeństwo postindustrialne" i „rewolucji białych kołnierzyków". Wspólną cechą tych proto-pojęć jest to, że wyizolowały jeden ze składników, tj. jedną część szybko zmieniającego się kompleksu gospodarczo-społecznego i sugerowały, że wystarczy opisać – zarówno w sensie opisowym, jak i metaforycznym – całość. W wyniku tego kilkadziesiąt terminów, każdy z innym podejściem, rozrastało się przez lata. Około 1980 r. połączyły się w kompleksowy, wspólny termin łączący pojęcie informacji i społeczeństwa: ta nowa koncepcja zawierała wszystkie poprzednie koncepcje częściowe, a nawet zachowywała ekspresyjną siłę, podejście i postawę, które reprezentowały[3].

W literaturze przedmiotu, zmiany procesów gospodarczych, ekonomicznych, społecznych i politycznych zachodzących na skutek zwiększenia tempa przepływu informacji są określane jako „rewolucja informacyjna". W zależności od podejścia metodologicznego i podmiotu badań początek rewolucji informacyjnej jest datowany pomiędzy latami 60. XX wieku, a początkiem lat 90. XX wieku.

1 S. Buregwa-Czuma, K. Garwol, *Definicje, właściwości i funkcje społeczeństwa informacyjnego*, „Dydaktyka informatyki" 2011, t. 6, s. 31.

2 http://paperroom.ipsa.org/papers/paper_64863.pdf.

3 L.Z. Karvalics, *Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression)*, Budapest 2007, s. 5–6.

Większość społeczeństw Europy znaczną część swojej działalności i aktywności przeniosła do sieci (komunikacja, bankowość elektroniczna, rozliczanie się z urzędami skarbowymi i dostęp do różnych baz danych). Również zarządzanie i sterowanie infrastrukturą odbywa się najczęściej poprzez internet. W związku z tym zapewnienie bezpieczeństwa cyfrowego społeczeństw jest jednym z kluczowych zadań władz państwowych. Funkcjonowanie społeczeństw informacyjnych, które w coraz większym stopniu są zależne od energii elektrycznej, opiera się na sieciach i systemach teleinformacyjnych. Powoduje to, że są one wyjątkowo podatne na zakłócenia, które mają wpływ na ich funkcjonowanie. Zagrożenia informatycznej strony funkcjonowania społeczeństw mają coraz poważniejsze konsekwencje, a ataki cybernetyczne mogą być wykorzystywane jako środek nacisku ekonomicznego i politycznego. W przypadku poważnych kryzysów działania w przestrzeni informatycznej mogą stanowić narzędzie oddziaływania uzupełniające tradycyjne siły zbrojne. Obecna era doświadcza nas szybszymi i rozleglejszymi zmianami niż kiedykolwiek w historii ludzkości. Ogrom informacji i eksplozja technologii informatycznych jest motorem napędowym, zmieniającym wszystkie aspekty życia społecznego, politycznego, kulturalnego i gospodarczego. Skutki rewolucji informacyjnej są szczególnie głębokie w zakresie strategii bezpieczeństwa narodowego.

Większość zjawisk i procesów politycznych ma swoje odzwierciedlenie w cyberprzestrzeni, a część z nich istnieje tylko w niej. Jednak źródła i przyczyny zjawisk społecznych (w tym politycznych) są umiejscowione poza przestrzenią wirtualną i wraz z procesami zachodzącymi przed erą internetu stanowią continuum. Dlatego w artykule zostały wykorzystane dwa podejścia badawcze. Pierwsze to zastosowanie metody instytucjonalno-prawnej, która polega na badaniu aktów normatywnych tworzonych przez instytucje[4]. Jej stosowanie wskazane jest przy badaniach systemów politycznych państw demokratycznych[5]. Metoda instytucjonalno-prawna może być stosowana

4 R. Żydok, *Przedmioty i metody badań politologicznych*, http://www.zydok.com/2008/01/przedmioty-i-metody-badan-politologicznych/#_ftn2.

5 R.M. Unger, *Legal Analisisas Institutional Imagination [w:]* R. Rawlings (red.), *Law, Society, and Economy: Centenary Essays for the London School of Economics and Political Science 1895–1995*, Oxford 1997, s. 177.

przy rozpoznawaniu stosunków międzynarodowych[6] oraz regulacji prawnych określających stosunki wewnątrzpaństwowe[7].

W artykule metoda instytucjonalno-prawna została użyta w celu zbadania ewolucji porządku prawnego Finlandii i Estonii w erze cyfryzacji oraz wpływy działań Federacji Rosyjskiej na te państwa.

Ponieważ głównym celem artykułu jest ukazanie Finlandii i Estonii w dobie zagrożeń hybrydowych (których składową są cyberwojna i cyberterroryzm), drugim podejściem badawczym jest podejście historyczne. Jest ono jednym z najczęściej stosowanych podejść badawczych w naukach politycznych[8]. Historia i nauki polityczne są ze sobą ściśle związane. Dziewiętnastowieczny angielski historyk, John Robert Seeley, stwierdził, że historia jest przeszłością polityki, a polityka jest teraźniejszością historii[9]. W wielu publikacjach opisujących metodologie badań w naukach politycznych przytoczone powyżej zdanie Freemana jest cytowane w kontekście uzasadniania użycia metody historycznej oraz opisywania politologii jako dziedziny naukowej[10]. Amerykański historyk i politolog Peter Charles Hoffer zaznacza, że podstawą zrozumienia każdego zjawiska będącego podmiotem badań politologicznych są wnikliwe badania nad historią tego zjawiska[11]. Również N. Jayapaln podkreśla, że dla zrozumienia ewolucji wszelkich zjawisk politycznych najistotniejsza jest znajomość historii[12]. Także Joseph W. Goodman podkreśla, że nawet przy opisywaniu takich zjawisk jak polityka telekomunikacyjna Unii Europejskiej, niezbędna jest dokładna analiza ich tła historycznego[13]. Leszek Moczulski w książce *Geopolityka. Potęga w czasie i przestrzeni* zaznacza, że zmienne układy przestrzenne

6 A. Chodubski, *Prognostyka jako wyzwanie metodologiczne w badaniu stosunków międzynarodowych*, Gdańsk 2009, s. 48.

7 J.S. Dryzek, *Discursive Democracy: Politics, Policy, and Political Science*, Cambridge 1994, s. 112.

8 T. Pawłuszko, *Wstęp do metodologii badań politologicznych. Skrypt akademicki*, Częstochowa 2013, s. 7.

9 G. Himmelfarb, *The New History and the Old: Critical Essays and Reappraisals. Revised Edition*, London 2004, s. 172.

10 C. Elman, M.F. Elman, *Introduction: Negotiating International History and Politics* [w:] C. Elman, M.F. Elman (red.), *Bridges and Boundaries: Historians, Political Scientists, and the Study of International Relations*, Cambridge 2001, s. 2–4.

11 P.C. Hoffer, *The Historians' Paradox. The study of History in Our Time*, New York 2008, s. 106–127.

12 N. Jayapalan, *Historiography*, New Delhi 2008, s. 10.

13 J.W. Goodman, *Telecommunications Policy-making in the European Union*, Norhampton 2006, s. 50.

nie odchodzą w przeszłość bez śladu[14]. Jednocześnie literatura określa układy przestrzenne w kategoriach gospodarczo-politycznych[15]. Podejście historyczne jest niezbędne dla zrozumienia genezy współczesnych zjawisk politycznych i zagrożeń hybrydowych ze strony Federacji Rosyjskiej, na jakie Estonia i Finlandia są narażone w szczególności.

Finlandia i Estonia wobec zagrożeń cyfrowych

Pierwszym państwem, które przekonało się, że korzyści płynące z cyberprzestrzeni idą w parze z nieznanymi wcześniej zagrożeniami była Estonia, najbardziej zinformatyzowane państwo świata, w którym obywatele mogli niemal wszystkie sprawy urzędowe załatwić online. W kwietniu i maju 2007 r. państwo to padło ofiarą skoordynowanych i zakrojonych na szeroką, niespotykaną wcześniej, skalę ataków cybernetycznych. Wydaje się uzasadnione twierdzenie, że Estonia stała się pierwszą ofiarą wojny cybernetycznej, w której jedno państwo sparaliżowało funkcjonowanie kluczowych instytucji i infrastruktury drugiego. Estonia mogła również stać się ofiarą testowania nowego rodzaju broni i taktyki wojennej. Pomimo braku (lub nieujawnianiu) jednoznacznych dowodów można przyjąć, że za tamtym atakiem stała Rosja. Wskazuje na to kontekst tamtych wydarzeń.

Estonia i Rosja mają długą historię sporów w stosunkach dwustronnych, a konflikty między etnicznymi Rosjanami i Estończykami sięgają setek lat przed powstaniem nowoczesnych państw narodowych. Po radzieckiej aneksji państw bałtyckich w 1940 r. i w czasie zimnej wojny Kreml przeniósł do Estonii setki tysięcy etnicznych Rosjan. Cel tych masowych migracji był dwojaki: zwiększenie spójności w bloku wschodnim i „zrusyfikowanie" kultury estońskiej. Po zakończeniu zimnej wojny i rozpadzie ZSRR, rząd w Tallinie wprowadził politykę mającą na celu minimalizację rosyjskich wpływów na kulturę estońską. Ataki cybernetyczne na Estonię miały miejsce w czasie, kiedy poziom napięcia między etnicznymi Estończykami a rosyjską mniejszością narodową osiągał apogeum. W dniu 30 kwietnia 2007 r. rząd Estonii przesunął Brązowego Żołnierza – pomnik upamiętniający radzieckie uwolnienie Estonii od nazistów – z Tõnismägi Park w centrum Tallina na cmentarz wojskowy w Tallinnie.

14 L. Moczulski, *Geopolityka. Potęga w czasie i przestrzeni*, Warszawa 2010, s. 316.
15 Ibidem, s. 317.

Ta decyzja wywołała zamieszki wśród rosyjskojęzycznej społeczności, która stanowiła w tamtym czasie około 26% populacji Estonii. Dla etnicznych Estończyków Brązowy Żołnierz symbolizował zniewolenie i ucisk. Ale dla mniejszości rosyjskiej przeniesienie to oznaczało dalszą marginalizację ich tożsamości etnicznej. Oprócz zamieszek i aktów przemocy, od 27 kwietnia do 18 maja, ataki DDoS (*Distributed Denial of Service*, rozproszona odmowa usługi) spowodowały zamknięcie stron internetowych wszystkich ministerstw, dwóch największych banków i kilku partii politycznych oraz parlamentarny serwer poczty elektronicznej. Estońscy urzędnicy, tacy jak minister spraw zagranicznych Urmas Paet, szybko oskarżyli Rosję o przeprowadzenie ataków, ale eksperci Komisji Europejskiej i NATO nie byli w stanie znaleźć wiarygodnego dowodu na udział Kremla w atakach DDoS[16].

Ataki na Estonię spowodowały szybką reakcję międzynarodową. W tamtym czasie państwo to nie posiadało odpowiednich służb przeciwdziałających cyberterroryzmowi i nie było przygotowane na ten typ ataku. Rządowy Zespół ds. Reagowania na Zagrożenia Cyfrowe (*ComputerEmergencyResponse Team* – dalej cyt.: CERT), aby przywrócić normalne operacje sieciowe, potrzebował pomocy ze strony partnerów fińskich, niemieckich, izraelskich i słoweńskich. Estoński CERT otrzymał również pomoc ze strony NATO. Co więcej, podczas kryzysu wśród państw zachodnich wystąpił wysoki poziom wymiany informacji wywiadowczych. Podczas gdy rosyjskojęzyczni hakerzy wykorzystali internet jako broń i narzędzie mobilizacji, Estonia i jej sojusznicy wykorzystali sieci cyfrowe, aby skutecznie przeciwdziałać atakom[17]. Po tamtych wydarzeniach władze Estonii podjęły szereg działań mających na celu zapobieżenie podobnym aktom terroru w przyszłości.

Estonia była jednym z pierwszych państw, które opracowały krajową strategię na rzecz bezpieczeństwa cybernetycznego (w 2008 r.). Zaktualizowana strategia została opublikowana w 2014 r. Obecnie Estonia posiada szeroki zakres ustawodawstwa obejmującego bezpieczeństwo informacji i cyberbezpieczeństwo. Estonia ma ugruntowany CERT pod kontrolą Urzędu Systemu Informacyjnego. Poza organami krajowymi, wpływ na bezpieczeństwo cyfrowe państwa ma fakt, że Centrum Doskonałości Bezpieczeństwa Cybernetycznego NATO (*CooperativeCyberDefence Centre of Excellence*, dalej cyt.: CCDCOE) mieści się w Estonii. Pomimo braku sformalizowanych partnerstw

16 S. Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, „Journal of Strategic Security" 2011, nr 2, s. 49–60.
17 Ibidem.

publiczno-prywatnych, w celu zwiększenia poziomu bezpieczeństwa cyfrowego, podmioty publiczne ściśle współpracują z odpowiednimi organizacjami sektora prywatnego[18].

We wszystkich swoich działaniach mających na celu zmniejszenie ingerowania Rosji w swoje sprawy wewnętrzne Estonia mogła liczyć na wsparcie i pomoc Finlandii. Finów i Estończyków łączy nie tylko bliskie pokrewieństwo etniczne i kulturowe, ale również poczucie zagrożenia ze strony Rosji. Aby zrozumieć obawy Finów należy przeanalizować tło historyczne stosunków fińsko-rosyjskich.

Po zakończeniu II wojny światowej, w przeciwieństwie do Estonii, Finlandia nie została zaanektowana przez Związek Radziecki i zachowała własną państwowość. Stała się jednak państwem zależnym od Moskwy zarówno pod względem polityki wewnętrznej, jak i zagranicznej. Przez cały okres powojenny rząd w Helsinkach próbował zachować równowagę pomiędzy niedawaniem Moskwie najmniejszego pretekstu do niezadowolenia, a nawiązywaniem stosunków ekonomiczno-gospodarczych z państwami zachodnimi[19]. Zwolennikiem prowadzenia takiej polityki był ówczesny prezydent Finlandii Juho Kusti Paasikivi, a po 1956 r. jego następca na urzędzie Urho Kaleva Kekkonen, który sprawował funkcję prezydenta aż do 1981 r. Zakładali oni, że Finlandia jest niepodległa tylko ze względu na swoje marginalne znaczenie dla Związku Radzieckiego. Znaczenie to mogło pozostać marginalne tylko dzięki unikaniu wszelkich układów międzynarodowych z państwami zachodnimi. Polityka taka, zwana później „finlandyzacją", była na początku nazywana linią polityczną Paasikivilego-Kekkonena[20]. Według fińskiego historyka, Jussi Hanhimäkiego, w okresie zimnej wojny Finlandia prowadziła jedną z najefektywniejszych polityk zagranicznych w Europie, która przeszła do historii jako „dyplomacja w saunie"[21]. Efektywna dyplomacja Helsinek pozwoliła Finlandii na integrację z Europą Zachodnią, pomimo długotrwałego znajdowania się tego państwa w radzieckiej strefie wpływów. Pomimo wielu kryzysów w stosunkach ze Związkiem Radzieckim, Finowie zdołali zachować niepodległość i równowagę w stosunkach politycznych, gospodarczych i kulturowych z państwami Europy

18 EU Cybersecurity Dashboard, *A Path to a Secure European Cyberspace*, http://cybersecurity.bsa.org/countries.html.

19 M. Jakobson, *Finland in the new Europe*, Westport 1998, s. 49.

20 F. Singleton, *The Myth of „Finlandisation"*, *„International Affairs"* 1981, nr 2.

21 M. Hanhimäki, *Security and Identity: the Nordic Countries and the United States since 1945* [w:] G. Lundestad (red.), *No End to Alliance: The United States and Western Europe: Past, Present and Future*, New York 1998, s. 87.

Środkowo-Wschodniej i Europy Zachodniej. Po upadku Związku Radzieckiego polityka Finlandii uległa reorientacji. Przyspieszył proces jej integracji ze strukturami gospodarczymi i militarnymi Europy Zachodniej.

Prawdopodobnie z obawy przed reakcją Moskwy Finlandia nie przystąpiła do NATO. Jednak nie oznacza to braku współpracy. Obecnie Finlandia jest jednym z pięciu państw (zwanych „partnerami o zwiększonych możliwościach"), które wnoszą szczególnie istotny wkład w operacje prowadzone przez NATO i wspierają inne cele Sojuszu. Dzięki temu ma ona zwiększone możliwości dialogu i współpracy z państwami sprzymierzonymi. W obecnym kontekście bezpieczeństwa międzynarodowego i rosnącymi obawami dotyczącymi rosyjskiej działalności wojskowej, NATO zacieśnia współpracę z Finlandią i Szwecją. Oznacza to poszerzenie dialogu politycznego, w tym na najwyższym szczeblu, wymianę informacji na temat wojny hybrydowej, koordynację szkoleń i ćwiczeń oraz rozwijanie wspólnej świadomości sytuacyjnej, aby w razie potrzeby przeciwdziałać wspólnym zagrożeniom i podejmować wspólne działania. Obydwa państwa uczestniczą we Wzmocnionych Siłach Odpowiedzi NATO (*NATO Response Force*, NRF), podlegając decyzjom krajowym, ale jednocześnie prowadzą regularne konsultacje z NATO w sprawie bezpieczeństwa w regionie Morza Bałtyckiego. W 2017 r. w Finlandii powstało Europejskie Centrum Doskonałości w Zakresie Zwalczania Zagrożeń Hybrydowych (*The European Centre of Excellence for CounteringHybridThreats*, dalej cyt.: HybridCoE) z siedzibą w Helsinkach. Centrum jest wspierane przez NATO i Unię Europejską[22]. Głównym celem powstania HybridCoE było stworzenie jednej instytucji koordynującej wykrywanie zagrożeń hybrydowych i reakcji na nie na poziomie UE i NATO. Obszary działania HybridCoE obejmują: 1) zachęcanie do dialogu i konsultacji na poziomie strategicznym między partnerami z UE i NATO; 2) wykrywanie działań hybrydowych skierowanych przeciwko zachodnim demokracjom przez podmioty państwowe i niepaństwowe oraz zwiększanie odporności partnerów na tego typu zagrożenia przez wykrywanie słabych punktów w ich systemach bezpieczeństwa; 3) przeprowadzanie szkoleń i organizowanie ćwiczeń opartych na scenariuszach mających na celu zwiększenie indywidualnych zdolności uczestników, a także interoperacyjności między uczestnikami UE i NATO w celu przeciwdziałania zagrożeniom hybrydowym; 4) prowadzenie badań i analiz zagrożeń hybrydowych oraz opracowywanie

22 NATO, *Relations with Finland*, https://www.nato.int/cps/en/natohq/topics_49594.htm?selectedLocale=en.

metod przeciwdziałania takim zagrożeniom; 5) tworzenie płaszczyzny współpracy dla ekspertów rządowych i pozarządowych mających na celu poprawę świadomości sytuacyjnej zagrożeń hybrydowych[23].

Obecnie aktywnie w działaniach HybridCoE uczestniczą UE, NATO oraz Czechy, Dania, Estonia, Finlandia, Francja, Włochy, Niemcy, Łotwa, Litwa, Holandia, Norwegia, Polska, Hiszpania, Szwecja, Wielka Brytania i USA. Uczestnictwo w działaniach Centrum jest otwarte również dla pozostałych państw członkowskich UE i NATO[24].

Współpraca Finlandii i Estonii w obszarze przeciwdziałania zagrożeniom cyfrowym

Stosunki Finlandii i Estonii charakteryzują się silnymi powiązaniami historycznymi i kulturowymi, a kontakty między tymi dwoma państwami są bardzo częste, wielopłaszczyznowe i wieloaspektowe. Niemal wszystkie estońskie ministerstwa ściśle współpracują z fińskimi. Dwustronna współpraca i kontakty pomiędzy estońskimi a fińskimi partnerami są szczególnie silne i częste w dziedzinie obrony, gospodarki, edukacji i badań, kultury, spraw wewnętrznych i wymiaru sprawiedliwości[25].

Obecnie szczególne miejsce we współpracy Estonii i Finlandii zajmują technologie informacyjne i komunikacyjne (*Information and Communication Technologies*, dalej cyt.: ICT). Państwa te ściśle współpracują w dziedzinie e-zarządzania i wymiany danych elektronicznych. Memorandum w sprawie cyfrowej współpracy Finlandii i Estonii zostało podpisane przez premierów Andrusa Ansipa (Estonia) i Jyrki Katainena (Finlandia) 10 grudnia 2013 r. Uzgodniono wówczas, że oba państwa będą współpracować w dziedzinie ITC i X-Road (X-Road to kluczowy element e-Estonii synchronizujący działanie państwowych i prywatnych e-serwisowych baz danych, platforma wymiany danych). Ustalono wówczas również, że Estonia i Finlandia będą wspólnie pracować nad dalszym rozwojem krajowej warstwy wymiany danych, tj. X-Road. Jesienią 2015 r. w Finlandii uruchomiono wersję testową platformy Palveluväylä (opartej na X-Road), która oferuje możliwość transgranicznego korzystania

23 Hybrid CoE, *About Us*, https://www.hybridcoe.fi/about-us/.
24 Ibidem.
25 Ministerstwo Spraw Zagranicznych Republiki Estonii, *Relations between: Finland*, http://vm.ee/en/countries/finland?display=relations#Co-operation.

z e-usług. W dniu 10 maja 2016 r. premierzy Taavi Rõivas (Estonia) i Juha Sipilä (Finlandia) podpisali wspólną deklarację o kontynuacji współpracy, która miała koncentrować się na uruchomieniu wymiany danych między obu państwami na podstawie platformy X-Road. Obecnie istnieją już rozwiązania techniczne, które umożliwiają wymianę danych między różnymi instytucjami Estonii i Finlandii za pośrednictwem X-Road. W czerwcu 2017 r. powołano Nordycki Instytut Rozwiązań Interoperacyjnych (*Nordic Institute for Interoperability Solutions*) do opracowania sposobu wymiany danych X-Road. Zostały utworzone specjalne kanały do realizacji transgranicznych usług elektronicznych z wymianą danych. Oba państwa współpracują przy uruchamianiu wymiany danych w następujących dziedzinach: dane rejestru ludności, dane z rejestru handlowego, recepty cyfrowe, dane o ubezpieczeniach społecznych, dane o ubezpieczeniach zdrowotnych oraz dane żeglugowe.

W dniu 7 lutego 2018 r. miała miejsce konferencja dotycząca pogłębienia współpracy pomiędzy obydwoma państwami. W konferencji brali udział ministrowie transportu Finlandii i Estonii oraz przedstawiciele samorządów z obu państw, a w czasie jej trwania przedstawiono studium wykonalności tunelu kolejowego łączącego Tallin i Helsinki (FinEst). Po zakończeniu studium wykonalności, estońskie Ministerstwo Spraw Gospodarczych i Komunikacji oraz fińskie Ministerstwo Gospodarki i Transportu utworzyły grupę roboczą, która określi kolejne etapy projektu tunelowego. Jednym z zadań grupy roboczej jest prowadzenie dalszych badań nad możliwością finansowania tej inwestycji. W trakcie swojej pracy grupa robocza weźmie pod uwagę wyniki i zalecenia z badania projektu FinEst. W świetle rozwoju technologicznego zostaną również rozważone dalekosiężne wpływy gospodarcze tunelu, opcje finansowania i kwestie dotyczące transportu i logistyki[26]. Tunel będzie mógł być również wykorzystany do budowy infrastruktury teleinformatycznej pozwalającej na bezpieczniejszą transmisją danych. Współpraca obronna między Estonią i Finlandią jest aktywna i obejmuje regularne konsultacje polityczne i wojskowe, a także praktyczne wspólne inicjatywy. Estonia i Finlandia podpisały umowę ramową o współpracy obronnej i na tej podstawie państwa kontynuują wymianę informacji na temat stanu bezpieczeństwa na Morzu Bałtyckim, planowania obrony, rozwoju zdolności wojskowych, badań i rozwoju w dziedzinie obronności, ćwiczeń szkoleniowych i cyberobrony. Oba państwa także ściśle współpracują w dziedzinie edukacji obronnej i szkolenia wojskowego,

26 Ibidem.

a także w dziedzinie wspólnych zamówień i kontroli zbrojeń. Od lat Finlandia wspiera Baltic Defense College (BALDEFCOL), wysyłając tam swojego instruktora[27]. Współpraca Finlandii i Estonii w misji UNIFL ONZ (tymczasowych sił Organizacji Narodów Zjednoczonych w Libanie) w Libanie rozpoczęła się w maju 2015 r., kiedy Estonia wniosła swój wkład wielkości plutonu piechoty do wspólnego batalionu Finlandii i Irlandii. Estoński pluton piechoty służy w zachodnim sektorze UNIFIL obok granicy z Izraelem, a jego głównym obowiązkiem było prowadzenie obserwacji i patroli oraz obsadzanie stanowisk kontrolnych. Członkowie Estońskich Sił Obronnych również współpracowali z siłami zbrojnymi Libanu. Wspólny batalion Finlandii i Irlandii przestanie działać pod koniec 2018 r. Finlandia uczestniczy w Centrum Doskonałości Bezpieczeństwa Cybernetycznej NATO z siedzibą w Estonii od października 2015 r. W centrum pracują dwaj fińscy eksperci. Estonia jest jednym z państw założycielskich Europejskiego Centrum Doskonałości do Zwalczania Zagrożeń Hybrydowych, które znajduje się w Finlandii[28].

Kolejnym przykładem na bliską współpracę Finlandii i Estonii w obszarze bezpieczeństwa było wspólne posiedzenie parlamentarnych komisji obrony Finlandii i Estonii. Najistotniejsze wnioski, jakie padły po tym wydarzeniu można wymienić w kilku punktach: 1) współpraca w dziedzinie obronności między państwami funkcjonuje dobrze; 2) brak członkostwa Finlandii w NATO nie jest przeszkodą w zacieśnianiu współpracy obronnej obu państw; 3) obok Szwecji, Stanów Zjednoczonych i Wielkiej Brytanii, Estonia jest dla Finlandii najważniejszym partnerem; 4) współpraca Finlandii i Estonii będzie się zaciskać dzięki wspólnym ćwiczeniom wojskowym i wspólnemu zakupowi sprzętu wojskowego.

W czasie spotkania potwierdzono zainteresowanie obu stron wzmocnieniem bezpieczeństwa w regionie Morza Bałtyckiego i Zatoki Fińskiej. Podkreślono również, że jednoczesna współpraca na poziomie Unii Europejskiej i NATO może zwiększyć poziom bezpieczeństwa partnerów znajdujących się we wspólnej przestrzeni informacyjnej. Członkowie narodowej komisji obronnej parlamentu Finlandii przedstawili przegląd planu rozwoju swojej armii i wydatków na obronę państwa, która zbliża się do poziomu 2% PKB ustalonego przez NATO[29].

27 Ibidem.
28 Ibidem.
29 Baltic News Service, *Defense committees of Estonian, Finnish parliaments hold joint meeting*. http://www.leta.lv/eng/defence_matters_eng/defence_matters_eng/news/1B718AD5-E90C-465F-86F7-03AC0ACF8D3F/.

Finlandia bierze udział również w corocznych ćwiczeniach cyberobrony organizowanych przez NATO CCD COE. Centrum organizuje największe na świecie i najbardziej złożone międzynarodowe ćwiczenia cyberbezpieczeństwa Locked Shields oraz doroczną konferencję na temat cyberkonfliktów CyCon. Sercem Centrum jest zróżnicowana grupa ekspertów – badaczy, analityków, szkoleniowców, edukatorów – z 20 krajów. Współpraca przedstawicieli sił zbrojnych, ekspertów rządowych i przedstawicieli przemysłu oznacza, że NATO CCD COE zapewnia unikalny, międzynarodowy 360-stopniowy ogląd współczesnego wymiaru cyberbezpieczeństwa[30].

Współpraca Finlandii i Estonii na płaszczyźnie bezpieczeństwa cyfrowego odbywa się również na płaszczyźnie niedostępnej dla opinii publicznej. Obecnie Estonia jest postrzegana jako najbardziej cyfrowe państwo świata, a przez to najbardziej narażona na zagrożenia cyberatakami. Można postawić tezę, że również Finlandia wielokrotnie padała ofiarą ataków. Jednak prawdopodobnie większość z nich jest nieznana opinii publicznej. Fińskie służby raczej nie informują ani o swoich działaniach, ani o ich wynikach. Jeden z nielicznych komentarzy dotyczył ujawnionych włamań do systemu informatycznego Ministerstwa Spraw Zagranicznych Finlandii. Incydent ten miał miejsce kilka lat wcześniej, ale został wykryty dopiero w 2013 r. Jednak sekretarz stanu w MZS Peter Stenlund oświadczył jedynie: Sprawcy wiedzą, że my wiemy, kim oni są, i wystarczy[31]. Stąd też wniosek, że Finlandia jest atakowana równie często jak Estonia, jednak są to informacje utajnione. Drugą poszlaką takiego stanu rzeczy jest zacieśnianie współpracy w ramach ochrony przed cyberatakami tych państw. Nie bez znaczenia pozostaje również fakt, że zarówno Finlandia, jak i Estonia są postrzegane przez Moskwę jako rosyjski obszar wpływów.

Zakończenie

Przykład ataku cybernetycznego na Estonię z 2007 r. udowodnił, że pierwszym elementem współczesnego konfliktu może być właśnie zniszczenie infrastruktury innego państwa przy pomocy narzędzi cyfrowych (oprogramowania). W niektórych przypadkach cyberataki mogą być skuteczniejsze od użycia klasycznych środków bojowych. Niewątpliwy postęp w dziedzinie

30 NATO CCD COE, *About Cyber Defence Centre*, https://ccdcoe.org/about-us.html.
31 TVP INFO, *Obce rządy przeprowadziły atak cybernetyczny na fińskie MSZ*, https://www.tvp.info/15888554/finlandia-msz-bylo-szpiegowane-przez-lata.

przeciwdziałania cyberatakom idzie w parze z doskonaleniem się grup przestępczych i terrorystycznych w tym obszarze. Dlatego w przypadku każdego państwa jest istotne stworzenie skutecznych procedur przeciwdziałania atakom cyfrowym. DDoSowy atak z 2007 r. był w gruncie rzeczy dość prymitywny i łatwy do wykrycia. O wiele niebezpieczniejsze są trudne do wykrycia działania wywiadowcze (jak to miało miejsce w przypadku szpiegowania MSZ Finlandii). Jednak żadne z działań służb zapewniających cyberbezpieczeństwo państwa nie powinno być upublicznione. Zagrożenia wynikające z powszechnego stosowania technologii informacyjnych nie dotyczą tylko państwa w znaczeniu instytucjonalnym. Z nowoczesnych technologii korzystają w życiu codziennym mieszkańcy niemal wszystkich państw świata. Jednocześnie większość urządzeń podłączonych do internetu nie posiada skutecznych zabezpieczeń przed złośliwym oprogramowaniem. Większość urządzeń mobilnych posiada wbudowane kamery, a aplikacje szpiegujące są powszechnie dostępne. Powoduje to potencjalną możliwość szpiegowania każdego w każdej sytuacji; nawet osób pełniących funkcje istotne dla bezpieczeństwa państwa. Jednocześnie w społeczeństwach sieciowych nie istnieje powszechna świadomość zagrożeń, jakie niesie za sobą korzystanie z urządzeń online. Wydaje się, że zarówno Estonia, jak i Finlandia znajdują się w obszarze zainteresowań służb Federacji Rosyjskiej. Mając tego świadomość państwa te starają się przeciwdziałać wrogiej aktywności.

Dotychczasowe tempo rozwoju technologii informacyjnych pozwala przypuszczać, że zagrożenia cybernetyczne mogą dotyczyć coraz większej części populacji i mieć coraz większy wpływ na funkcjonowanie państw. Aby temu przeciwdziałać państwa powinny ze sobą współpracować. Wydaje się, że działania takie zostały już zainicjowane po obu stronach Zatoki Fińskiej.

Bibliografia

Literatura

Buregwa-Czuma S., Garwol K., *Definicje, właściwości i funkcje społeczeństwa informacyjnego*, „Dydaktyka informatyki" 2011, t. 6.

Chodubski A., *Prognostyka jako wyzwanie metodologiczne w badaniu stosunków międzynarodowych*, Gdańsk 2009.

Dryzek J.S., *Discursive Democracy: Politics, Policy, and Political Science*, Cambridge 1994.

Elman C., Elman M.F., *Introduction: Negotiating International History and Politics* [w:] C. Elman, M.F. Elman (red.), *Bridges and Boundaries: Historians, Political Scientists, and the Study of International Relations*, Cambridge 2001.

Goodman J.W., *Telecommunications Policy-making in the European Union*, Norhampton 2006.

Hanhimäki M., *Security and Identity: the Nordic Countries and the United States since 1945* [w:] G. Lundestad (red.), *No End to Alliance: The United States and Western Europe: Past, Present and Future*, New York 1998.
Herzog S., *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, „Journal of Strategic Security" 2011, nr 2.
Himmelfarb G., *The New History and the Old: Critical Essays and Reappraisals. Revised Edition*, London 2004.
Jakobson M., *Finland in the new Europe*, Westport 1998.
Jayapalan N., *Historiography*, New Delhi 2008.
Karvalics L.Z., *Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression)*, Budapest 2007.
Moczulski L., *Geopolityka. Potęga w czasie i przestrzeni*, Warszawa 2010.
Pawłuszko T., *Wstęp do metodologii badań politologicznych. Skrypt akademicki*, Częstochowa 2013.
Unger R.M., *Legal Analisisas Institutional Imagination* [w:] R. Rawlings (red.), *Law, Society, and Economy: Centenary Essays for the London School of Economics and Political Science 1895–1995*, Oxford 1997.

Inne źródła

Baltic News Service, *Defense committees of Estonian, Finnish parliaments hold joint meeting*. http://www.leta.lv/eng/defence_matters_eng/defence_matters_eng/news/1B718AD5--E90C-465F-86F7-03AC0ACF8D3F/.
EU Cybersecurity Dashboard, *A Path to a Secure European Cyberspace*, http://cybersecurity.bsa.org/countries.html.
Hoffer P.C., *The Historians' Paradox. The study of History in Our Time*, New York 2008.
http://paperroom.ipsa.org/papers/paper_64863.pdf.
Hybrid CoE, *About Us*, https://www.hybridcoe.fi/about-us.
Ministerstwo Spraw Zagranicznych Republiki Estonii, *Relations between: Finland*, http://vm.ee/en/countries/finland?display=relations#Co-operation.
NATO CCD COE, *About Cyber Defence Centre*, https://ccdcoe.org/about-us.html (odczyt: 22.06.2018).
NATO, *Relations with Finland*, https://www.nato.int/cps/en/natohq/topics_49594.htm?selectedLocale=en.
Singleton F., *The Myth of „Finlandisation"*, „International Affairs"1981, nr 2.
TVP INFO, *Obce rządy przeprowadziły atak cybernetyczny na fińskie MSZ*, https://www.tvp.info/15888554/finlandia-msz-bylo-szpiegowane-przez-lata.
Żydok R., *Przedmioty i metody badań politologicznych*, http://www.zydok.com/2008/01/przedmioty-i-metody-badan-politologicznych/#_ftn2.

Prevention of digital threats on the example of the Republic of Estonia and the Republic of Finland

Abstract

The development of the telecommunication networks has caused social and political changes. Common access to the internet causes a large part of social activities to move to the virtual world. However, this universality has caused the emergence of new types of serious threats. Currently, terrorist attacks or warfare can be carried out remotely. Internationally important countries have their own services operating in cyber-space. Due to historical reasons and geopolitical location, Finland and Estonia are often treated

by the Kremlin as Russia's influence zones. In order to achieve its goals, the state puts pressure on countries that historically were parts of the Russian Empire using all possible means, including telecommunications networks. The flagship example of such action was the cybernetic attack on Estonia in 2007.

Key words: cybersecurity, NATO, Finland, Estonia, information society, telecommunication, terrorism, technological progress, information technology, Communications