Politeja
Nr 5(86), 2023, s. 307-327
https://doi.org/10.12797/Politeja.20.2023.86.14

Agnieszka WARCHOŁ
Uniwersytet Komisji Edukacji Narodowej w Krakowie
agnieszka.warchol@up.krakow.pl

OD OFIARY DO ŚWIATOWEGO LIDERA

ESTONIA PO CYBERATAKACH Z 2007 ROKU

ABSTRACT **From Victim to Leader – Estonia after the 2007 Cyberattacks**
In the spring of 2007, Estonia became the target of co-ordinated cyberattacks. The attacks were part of a wider political conflict between Estonia and Russia over the relocation of a Soviet-era monument in Tallinn. The aim of this article is to present the effects of the cyberattacks on Estonian cybersecurity. The article consists of several parts. The first deals with the main causes of the conflict. In the second part, the author presents information about the direct results of the cyberattacks on Estonia. The last part presents strategic, legal and organisational changes in Estonian cybersecurity. At present, Estonia is one of the most developed nations regarding the ubiquitous use of information and communication technology in all aspects of state functioning. The study used the following research methods: historical method, comparative analysis, literature analysis and criticism, source analysis and criticism, and case study.

Keywords: Estonia, cyberattacks, cyberwar, cybersecurity, political conflict

Słowa kluczowe: Estonia, cyberataki, cyberwojna, cyberbezpieczeństwo, konflikt polityczny

WPROWADZENIE

Cyberatak na Estonię z 2007 roku został nazwany *pierwszą cyberwojną w historii*[1]. Poprzedził go zdecydowanie najsłabszy moment w relacjach na linii Tallinn–Moskwa po odzyskaniu niepodległości przez Estonię[2]. Przeniesienie pomnika Brązowego Żołnierza z centrum estońskiej stolicy na pobliski cmentarz wojskowy doprowadziło do zamieszek ze strony mniejszości rosyjskojęzycznej, a w efekcie do kryzysu dyplomatycznego i agresywnych działań w cyberprzestrzeni, których ofiarą padła Estonia, a dokładnie jej systemy i instytucje – zarówno z sektora państwowego, jak i prywatnego. Cyberprzestrzeń była atrakcyjnym narzędziem do realizacji interesów różnych podmiotów państwowych i międzynarodowych z co najmniej dwóch powodów. Po pierwsze, stała się odrębną areną oddziaływania, np. poprzez rozprzestrzenianie dezinformacji, propagandy[3] i ataków za pomocą złośliwego oprogramowania. Po drugie, działania w niej prowadzone manifestują się w świecie fizycznym, np. w czasie konfliktu w 2007 roku to w sferze wirtualnej – za pośrednictwem portali społecznościowych – grupy rosyjskojęzyczne tworzyły plany wydarzeń realizowanych w świecie realnym w konkretnych miejscach, np. przy pomniku Ofiar II Wojny Światowej w centrum Tallinna[4].

Bez wątpienia sprzeczności i frustracje społeczne w pierwszej fazie konfliktu[5] zwróciły uwagę Estonii na konieczność dokładnego monitorowania ruchów Rosji. Estońscy specjaliści z pomocą zachodnich zespołów ds. reagowania na incydenty komputerowe odparli cyberatak, a władze rosyjskie zaprzeczyły, że go zaaranżowały i wspierały. Ataki w cyberprzestrzeni wykorzystano jako narzędzie do wywarcia wpływu na decyzję przeciwnika, w tym przypadku: o rezygnacji z usunięcia monumentu z centrum estońskiej stolicy[6].

---

1 M. Landler, J. Markoff, *In Estonia, What May Be the First War in Cyberspace*, The New York Times, 28 V 2007, [online] https://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html, 22 XI 2022.

2 A. Tiido, *Wpływ kwestii mniejszości rosyjskiej na stosunki pomiędzy Republiką Estońską a Federacją Rosyjską*, [online] https://depotuw.ceon.pl/bitstream/handle/item/2197/streszczenie.pdf?sequence=3, 22 XI 2022.

3 W rosyjskich mediach Estonię zaczęto nazywać „eSStonią". Jednym z bezpośrednich powodów była śmierć jednej osoby na skutek zamieszek przy pomniku Brązowego Żołnierza w centrum Tallinna, w dniu, kiedy pomnik miał zostać przeniesiony na pobliski cmentarz wojskowy. Do walk ulicznych doszło między przeciwnikami decyzji estońskich władz, w większości przedstawicielami mniejszości rosyjskojęzycznej, a estońską policją. W rosyjskich mediach pojawiły się także informacje o łamaniu praw i wolności rodaków mieszkających w Estonii podczas przesłuchań, których miała dopuszczać się miejscowa policja. Te wiadomości były przez Estończyków dementowane i nazywane rosyjską dezinformacją, podobnie jak oskarżenia względem Estonii dotyczące kolaboracji z faszystami czy czczenia symboli nazistowskich. Zob. P. Pomerantsev, *To nie jest propaganda. Przygody na wojnie z rzeczywistością*, przeł. A. Paszkowska, Warszawa 2020, s. 97, 122.

4 Za przykład może posłużyć warta pod pomnikiem, którą pełniła grupa nazywająca siebie Nocną Strażą.

5 A. Antoszewski, R. Herbut, *Leksykon politologii*, Wrocław 2004, s. 175.

6 D.F. Baltrusaits, *Cyber War: Do We Have the Right Mindset?*, [w:] *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, red. E.G. Carayannis, D.F.J. Campbell, M.P. Efthymiopoulos, Cham 2018, s. 794.

Dla Rosji kwestia tożsamości narodowej oparta na dziedzictwie kulturowym, a przez to oddziaływanie na rosyjskojęzyczną populację Estonii są ważne w celu podtrzymania swojej obecności i wpływów w tym kraju, podobnie jak w innych krajach postradzieckich. Dodatkowo wielu Rosjan przebywających w Estonii postrzegało wysiłki tego państwa, by uwolnić się od sowieckiej spuścizny – np. poprzez promowanie języka estońskiego, regulacje prawne odnoszące się do kwestii obywatelstwa mieszkańców tego kraju czy usuwanie sowieckich symboli i pomników – jako próbę zdegradowania ich narodu[7]. W następstwie przesunięcia pomnika obie izby rosyjskiego parlamentu wezwały Prezydenta Federacji Rosyjskiej Władimira Putina do nałożenia sankcji na Estonię lub zerwania stosunków dyplomatycznych z tym krajem[8]. Oficjalnie 21 stycznia 2007 roku Putin potępił działania estońskiego rządu[9].

W praktyce trudno określić, kiedy dokładnie konflikt się zakończył, zwłaszcza że dotyczył sfery cybernetycznej. Działania w cyberprzestrzeni zostały wygaszone, a strona atakująca nie zdecydowała się na uruchomienie prac na innych płaszczyznach. Okres po zakończeniu konfliktu charakteryzuje się zazwyczaj wysokim ryzykiem niestabilności[10]. Tak też było w tym przypadku, a dalsze czynności podejmowane przez Estonię miały na celu odbudowę infrastruktury teleinformatycznej, przywrócenie stanu sprzed incydentu oraz uspokojenie nastrojów społecznych.

Celem niniejszego tekstu jest próba przedstawienia działań Estonii podejmowanych po konflikcie politycznym z Federacją Rosyjską w 2007 roku, a konkretnie po atakach cybernetycznych na jej infrastrukturę teleinformatyczną, w stosunku do sektora prywatnego i publicznego, a także wskazanie, że ów konflikt zapoczątkował budowę potęgi cybernetycznej Estonii. Do realizacji przedstawionego celu wykorzystano następujące metody badawcze: metoda historyczna, analiza porównawcza, analiza i krytyka źródeł, analiza i krytyka piśmiennictwa, studium przypadku. Następstwem określenia celu są następujące pytania badawcze: Jakie były konsekwencje tych wydarzeń dla Estonii? Jakie sfery zostały objęte działaniami naprawczymi? Dlaczego Estonia nazywana jest Nadbałtycką Doliną Krzemową i jakie podejmuje inicjatywy, by utrzymać status lidera w sferze cyfrowej? Przedstawiana problematyka nie wyczerpuje w całości zagadnienia wpływu konfliktu politycznego z Rosją na bezpieczeństwo Estonii, ale skupia się wyłącznie na wybranych subiektywnie aspektach. Na potrzeby niniejszej pracy zostaną omówione jedynie bezpośrednie skutki cyberataku na cyberbezpieczeństwo Estonii.

Kwestie konsekwencji cyberataku z 2007 roku można rozpatrywać w dwóch aspektach. Aspekt postrzegania dotyczy skutków wizerunkowych, czyli tego, jak Estonia zaczęła być odbierana po cyberatakach, zarówno w skali regionalnej, jak i globalnej.

---

7 S.L. Myers, *Russia Rebukes Estonia for Moving Soviet Statue*, The New York Times, 27 IV 2007, [online] https://www.nytimes.com/2007/04/27/world/europe/27cnd-estonia.html, 22 XI 2022.

8 *Tamże*.

9 I. Juurvee M. Mattiisen, *Report the Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict*, VIII 2020, s. 16, [online] https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf, 20 XI 2022.

10 *Building Sustainable Peaces: Timing and Sequencing of Post-Conflict Reconstruction and Peacebuilding*, red. A. Langer, G.K. Brown, Oxford 2016, s. 143.

W tekście przyjęto założenie, że fakt, iż stała się ona ofiarą zmasowanych ataków w cyberprzestrzeni o niespotykanej dotąd dla podmiotu państwowego skali, bez wątpienia pozwolił jej wykreować pewien scenariusz, którego rozpowszechnianie utrwaliło określony wizerunek. To wizerunek państwa-ofiary, wysoko zaawansowanego technologicznie, które poradziło sobie z atakami. Następnym krokiem było stworzenie wizerunku cyfrowego lidera na arenie międzynarodowej, uzasadnionego przez cyfrowe projekty i technologicznie dobrze funkcjonujące mechanizmy, które Estonia wdraża.

Drugi aspekt, równie ważny przy omawianiu konsekwencji wydarzeń z 2007 roku, dotyczy działań związanych *stricte* z estońskim cyberbezpieczeństwem. Cyberbezpieczeństwo to proces, który ma na celu zapewnienie bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, a więc jego struktur, osób fizycznych i osób prawnych, a także systemów teleinformatycznych oraz zasobów informacyjnych[11]. Ten proces w przypadku Estonii nie rozpoczął się w 2007 roku. Władze państwowe, dostrzegając wyzwania, szanse i zagrożenia w tej materii, znacznie wcześniej podejmowały prekursorskie działania w zakresie bezpieczeństwa informacyjnego[12]. Bardzo istotne są również działania *post factum*, czyli te, które spowodowały dalszy rozwój Estonii i doprowadziły ją do roli lidera w dziedzinie cyfryzacji – nie tylko na rynku europejskim, lecz także globalnym. Bez wątpienia władze Estonii nie zmarnowały szansy, którą paradoksalnie dał im konflikt z Rosją. Mimo że atak nie spowodował długotrwałych szkód materialnych, utraty życia ani znacznych strat finansowych, to wskazał rządowi

[11] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015*, Warszawa 2015, [online] http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf, 15 XI 2022.

[12] Do mobilizacji w zakresie prac nad estońskim cyberbezpieczeństwem przyczyniły się też inne wydarzenia, np. wojna w Gruzji w 2008 roku, podczas której równolegle do działań konwencjonalnych prowadzono działania w sferze wirtualnej. Eksperci wskazują, że był to pierwszy pełnowymiarowy konflikt, w którym walki toczyły się równocześnie na następujących płaszczyznach: lądzie, morzu, powietrzu i w cyberprzestrzeni. Cyberataki przeprowadzano przy pomocy podobnych metod i technik jak rok wcześniej w Estonii. Gruzińskie sieci były bardziej podatne na atak niż estońskie. Estonia, wykorzystując swoje doświadczenie, wysłała dwóch specjalistów z estońskiego Zespołu Reagowania na Incydenty Komputerowe (CERT-EE), by wspomóc Gruzję. Zarówno w estońskim, jak i w gruzińskim przypadku podobne były tło polityczne oraz metody stosowane przez agresora, a także hipotetyczny sprawca. Są też pewne różnice: główne cele ataku i jego ostateczne skutki, związane z różnymi stopniami zaawansowania technologicznego dwóch omawianych państw. Po aneksji Krymu w 2014 roku w Estonii ponownie wzrosły obawy dotyczące stabilności regionalnej i własnego bezpieczeństwa narodowego, w tym cyberbezpieczeństwa. Bezpieczeństwo cybernetyczne było również jednym z priorytetów estońskiego przywództwa grupie Nordic-Baltic Eight (NB8) w 2014 roku. Wszystkie te wydarzenia przyczyniły się w mniejszym bądź większym stopniu do wypracowania nowych reform i strategicznych dokumentów na poziomie nie tylko państwowym, lecz także regionalnym i międzynarodowym. Zob. A. Kozłowski, *Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan*, „European Scientific Journal" 2020, vol. 3, s. 239; *Estonia's National Cybersecurity and Cyberdefense Posture*, Cyberdefense Report, Zürich, IX 2020, [online] https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Estonia.pdf, 7 XI 2022; P. Pernik, P. Maldre, *Rising Challenges: Cybersecurity in the Baltic Sea Region*, [w:] *Baltic Visions: European Cooperation, Regional Stability*, red. K. Redłowska, Warszawa 2015, s. 44; *Nordic Baltic Cooperation (NB8)*, Republic of Estonia. Ministry of Foreign Affairs, [online] https://www.vm.ee/en/international-relations-estonian-diaspora/regional-cooperation/nordic-baltic-cooperation-nb8, 3 II 2023.

słabości w sferze cyfrowej, np. w aspekcie e-administracji, co jedynie zwiększyło jego determinację do przeciwdziałania podobnej cyberagresji w przyszłości oraz jej możliwym skutkom[13]. Dodatkowo, jak wskazuje Thomas Rid, atak spotkał się *z nieproporcjonalną reakcją natury psychologicznej i politycznej, zarówno w samej Estonii, jak i na arenie międzynarodowej*[14].

KONTEKST WYDARZEŃ I PRZEBIEG ATAKU

Estonia przez prawie pół wieku przynależała do Związku Radzieckiego. Została włączona do strefy wpływów Kremla na mocy paktu Ribbentrop-Mołotow, podpisanego 23 sierpnia 1939 roku w Moskwie, a przywrócenie niepodległości proklamowała 20 sierpnia 1991 roku. Od tego czasu Estonia budowała własne instytucje demokratyczne, chcąc przywrócić porządek prawny sprzed 1940 roku. Władze kraju radykalnie zmieniły politykę etniczną, manifestując swoją niezgodę na ingerowanie Federacji Rosyjskiej w wewnętrzne sprawy kraju pod pretekstem ochrony rodaków oraz chcąc ograniczyć wpływ mniejszości rosyjskiej na przebieg wydarzeń[15]. Z czasem Estończycy zaczęli pozbywać się również symboli radzieckich i przywracać międzywojenną symbolikę państwową[16].

W 2007 roku Estończycy przenieśli pomnik Brązowego Żołnierza z centrum stolicy na pobliski cmentarz wojskowy. Monument miał dwojakie znaczenie: dla obywateli Estonii był symbolem zniewolenia ich kraju przez Związek Radziecki, natomiast dla mniejszości rosyjskiej stanowił pamiątkę po odbiciu Tallinna z rąk nazistów i oddawał hołd żołnierzom poległym w tej operacji. Protesty nasilały się w wyniku dezinformacji rosyjskich mediów, które głosiły, że pomnik i sowieckie groby wojenne są niszczone przez estońskie władze[17]. W następstwie działań Estończyków przez dwie noce – z 26 na 27 oraz z 27 na 28 kwietnia 2007 roku – w stolicy wybuchały zamieszki, prowokowane przez rosyjską młodzież[18]. W tym samym czasie prokremlowska organizacja młodzieżowa zablokowała estońską ambasadę w Moskwie[19]. Władze rosyjskie potępiły działania Estończyków. Następnie konflikt polityczny przeniósł się ze sfery materialnej do przestrzeni wirtualnej.

---

13 D.F. Baltrusaits, *Cyber War...*, s. 794.

14 T. Rid, *Wojna informacyjna*, przeł. F. Tryl, Warszawa 2022, s. 502.

15 A. Szabaciuk, *Polityka etniczna Republiki Estońskiej*, „Wschodnioznawstwo" 2016, no. 10, s. 220.

16 *Tamże*, s. 222.

17 P. Davies, *Cyberattacks Likely to Rise in Wake of Ukraine War: This Is What Estonia Learnt from Web War One*, Euronews, 1 VII 2022, [online] https://www.euronews.com/next/2022/05/26/cyberattacks-likely-to-rise-in-wake-of-ukraine-war-this-is-what-estonia-learnt-from-web-wa, 8 XI 2022.

18 M. Kofin, *Atak cybernetyczny i awaria systemów informatycznych – paraliż państwa i życia obywateli na przykładzie Estonii, Gruzji, Litwy oraz Polski*, [w:] *Obywatel w internecie*, red. M. Butkiewicz, P.P. Płatek, Warszawa 2017, s. 14.

19 *Tamże*.

Ataki w sieci były zsynchronizowane z protestami ulicznymi, a także z przekazami medialnymi płynącymi z mediów przychylnych Kremlowi, co sprawiło, że eskalacja konfliktu przypadła na przełom kwietnia i maja 2007 roku. W czasie śledztwa Estonii udało się ustalić, że większość ataków pochodziła spoza granic państwa, a znaczną część przeprowadzano z Federacji Rosyjskiej. Choć estońskie władze, m.in. minister spraw zagranicznych Urmas Paet, oskarżały Kreml o bezpośredni udział w cyberatakach[20], twierdząc, że były one próbą sparaliżowania estońskich przedsiębiorstw i urzędów państwowych, to eksperci z Unii Europejskiej i NATO nie zgromadzili wystarczających dowodów na poparcie tej tezy. Odrzucona została też dyplomatyczna prośba Estonii o pomoc w namierzeniu napastników[21], a rosyjskie organy ścigania odmówiły współpracy ze swoimi estońskimi odpowiednikami w identyfikacji sprawców[22]. Wobec tego postępowanie, które miało wyjaśnić źródło ataku, zostało zakończone z powodu braku możliwości dalszego prowadzenia śledztwa[23].

Przypisanie konkretnemu państwu odpowiedzialności za działania w cyberprzestrzeni jest niezwykle trudne, co wynika ze specyfiki tej sfery. Poszlaki prowadziły na rosyjskie fora internetowe, gdzie publikowano konkretne instrukcje, jak przeprowadzić atak w sieci na estońskie instytucje. Dzięki temu liczba potencjalnych atakujących zdecydowanie rosła, a możliwość wykrycia sterującego atakiem – malała. Fakt, że aktywność pochodziła z rosyjskich stron internetowych, nie dowodzi, że za atakiem stał Kreml, jednak kontekst polityczny, zachowanie władz rosyjskich po ataku oraz poszlaki wyeksponowane przez estońskich śledczych wskazują, że cyberataki na Estonię nie były jedynie działaniami „haktywistów", którzy chcieli zademonstrować swój sprzeciw przeciwko decyzji estońskich władz o usunięciu pomnika, lecz mogły być próbą ingerencji Federacji Rosyjskiej w wewnętrzne sprawy Estonii.

Cyberoperację można podzielić na kilka faz. Pierwsza to faza rozpoczęcia – atak zaczął się późnym wieczorem 27 kwietnia 2007 roku. Jako pierwsze zostały zablokowane strony rządowe. Druga faza ataków rozpoczęła się z początkiem maja, gdy doszło do blokady stron internetowych sektora prywatnego[24]. 9 maja, czyli w Dzień Zwycięstwa obchodzony w Rosji, ruch na estońskich stronach internetowych wzrósł ponad 20-krotnie[25]. W celu dokładniejszej analizy ataków można wyróżnić aż pięć etapów działań (zob. tabela 1).

---

[20] A. Bright, *Estonia Accuses Russia of „Cyberattack"*, The Christian Science Monitor, 17 V 2007, [online] https://www.csmonitor.com/2007/0517/p99s01-duts.html, 11 XI 2022.

[21] D.F. Baltrusaits, *Cyber War...*, s. 794.

[22] C.C. Bryant, *Cybersecurity 2020: What Estonia Knows about Thwarting Russians*, The Christian Science Monitor, 4 II 2020, [online] https://www.csmonitor.com/World/Europe/2020/0204/Cybersecurity-2020-What-Estonia-knows-about-thwarting-Russians, 9 XI 2022.

[23] W. Majkowski, *Koniec śledztwa w sprawie cyberataku na Estonię*, Polityka Globalna, 21 VIII 2012, [online] http://www.politykaglobalna.pl/2012/08/koniec-sledztwa-w-sprawie-cyberataku-na-estonie/, 12 XI 2022.

[24] J. Jalonen, *Dni, które wstrząsnęły Estonią*, przeł. P. Bukalska, Tygodnik Powszechny, 12 V 2019, [online] http://www.eesti.pl/index.php?dzial=panstwo&strona=cyberataki, 22 XI 2022.

[25] A. Nowak, *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe AON" 2013, no. 3, s. 11.

Tabela 1. Kampania zmasowanych ataków na Estonię – poszczególne fazy

Faza	Działania
I	Działania internautów popierających rosyjską mniejszość o charakterze spontanicznym. Tę fazę charakteryzuje samoistne organizowanie się użytkowników sieci. Pojawiły się pierwsze ataki typu DDoS przeciwko stronom internetowym władz Estonii. Stali za nimi zarówno wyspecjalizowani hakerzy, jak i *script kiddies*, którzy dzięki blogom, instrukcjom w witrynach i forach internetowych zdołali przeprowadzić bądź zainicjować nieskomplikowane ataki.
II	Większy stopień zaawansowania. Zaczęto stosować sieci *botnet*, które towarzyszyły prostszym metodom wykorzystywanym przez hakerów i *script kiddies*.
III	Celem stały się usługi i strony internetowe z sektora prywatnego.
IV	Bardziej skomplikowane ataki na systemy bankowe, m.in.: blokada możliwości świadczenia usług online, odcięcie od zagranicznych sieci bankowych. Celem stała się również państwowa infrastruktura krytyczna.
V	Masowy charakter ataków. Do cyberataków wykorzystano sieć *botnet* składającą się z 85 tys. komputerów.

Źródło: M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, s. 184-202.

Między 27 kwietnia a 11 maja 2007 roku doszło do 128 ataków metodą DDoS (ang. *distributed denial-of-service*)[26], z czego 115 przeprowadzono za pomocą techniki ICMP flood[27], a 4 z wykorzystaniem TCP SYN flood[28]. Ataki były wymierzone w witryny internetowe: policji, parlamentu, rządu, Ministerstwa Polityki Społecznej, Ministerstwa Rolnictwa, Ministerstwa Finansów i Ministerstwa Ochrony Środowiska. Oprócz wymienionych stron internetowych zaatakowane zostały konta e-mail najważniejszych polityków oraz sektor prywatny. Atakujący zainteresowali się także infrastrukturą krytyczną kraju, w tym systemem bankowym i dostawcami usług internetowych – w rezultacie największe banki zawiesiły usługi online i wstrzymały zagraniczne transakcje[29]. Dodatkowo ataki spowodowały, że obywatele Estonii przez pewien czas nie mieli dostępu do systemu ratownictwa, bo numer alarmowy został zablokowany.

Co ciekawe, cyberataki ominęły sieć elektroenergetyczną i transport. Wydaje się, że gdyby sprawcy chcieli w nie uderzyć, to mieli ku temu okazje. Eksperci wskazują, że ataki na elementy infrastruktury krytycznej przeprowadzono nie po to, by wyrządzić poważne szkody, ale by wywołać strach; były pokazem siły, który miał przynieść efekty

[26] Atak DDoS polega na bombardowaniu systemu żądaniami dostępu, powodując jego niewydolność. Zob. P. Łoczuk, *Internet jako nowoczesne pole bitwy*, [w:] *Obywatel w internecie...*, s. 31.

[27] Zob. *ICMP Flood*, Fundacja Instytut Cyberbezpieczeństwa, 27 X 2022, [online] https://instytutcyber.pl/artykuly/icmp-flood/, 2 II 2023.

[28] Zob. *TCP SYN Flood*, Imperva, [online] https://www.imperva.com/learn/ddos/syn-flood/, 2 II 2023.

[29] M. Kofin, *Atak cybernetyczny...*, s. 15.

stricte polityczne[30]. W obliczu ataków Estonia zmobilizowała specjalistów w dziedzinie informatyki, skupionych w Estonian Computer Emergency Response Team (CERT-EE), i podjęła akcję obronną, która okazała się sukcesem. Cyberwalka trwała trzy tygodnie. Estonię wspomogły oddziały CERT[31] z innych krajów europejskich oraz organizacje: FIRST[32] i TERENA TF-CSIRT[33].

Konflikt z Federacją Rosyjską łączy się z marcowymi wyborami parlamentarnymi, podczas których obywatele mogli oddać głos przez internet. Było to wydarzenie na skalę światową, bo chociaż w innych państwach zdarzało się to wcześniej, to jedynie w odniesieniu do wyborów lokalnych. Z możliwości i-votingu skorzystało ponad 30 tys. obywateli Estonii. To pokazuje, jak bardzo to państwo było już wówczas zaawansowane technologicznie. Zaawansowanie technologiczne Estonii sprawiło, że – wbrew pozorom – mocno odczuła ona agresję w cyberprzestrzeni. Co prawda nie zostały naruszone newralgiczne elementy funkcjonowania państwa, ale sprawcom ataku udało się zasiać strach i niepewność.

Już wtedy 60% obywateli tego kraju codziennie korzystało z internetu[34], a 97% transakcji bankowych odbywało się w internecie, na co zresztą zwracał uwagę ówczesny prezydent Estonii Toomas Hendrik Ilves na spotkaniu z prezydentem USA George'em W. Bushem[35]. Spotkanie odbyło w czerwcu 2007 roku, niedługo po ataku cybernetycznym wymierzonym w Estonię, i było jego pokłosiem – Bush wystosował zaproszenie do Ilvesa na początku maja jako demonstrację poparcia i solidarności z zaatakowaną Estonią. Obrona przed tą nową formą działań wymierzonych w inne państwo zajmowała ważne miejsce w programie wizyty. Ponadto Bush poparł propozycję Estonii dotyczącą powołania w Tallinnie z udziałem USA centrum badań nad cyberbezpieczeństwem NATO[36].

Cyberagresja, z którą musiało mierzyć się państwo, była nowym doświadczeniem, nie tylko dla Estonii, lecz także dla społeczności międzynarodowej. Cyberataki – pierwszy raz na taką skalę – zilustrowały, jak bez użycia siły można sparaliżować działanie instytucji i pozbawić ludzi dostępu do usług. Przypadek Estonii nie ukazuje typu idealnego wojny cybernetycznej. Wyznaczył jednak granicę, która oddziela okres prowadzenia wojny konwencjonalnej od konfliktu cyfrowego. NATO nie uznało tego zdarzenia za atak zbrojny, dlatego nie udzieliło Estonii wsparcia na podstawie art. 5

30 M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, s. 184-202.

31 CERT – ang. Computer Emergency Response Team.

32 Zob. strona FIRST, [online] http://www.first.org/, 22 XI 2022.

33 Zob. strona GEANT, [online] https://geant.org/, 22 XI 2022.

34 K. Ruus, *Cyber War I: Estonia Attacked from Russia*, The European Institute, [online] https://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia, 9 XI 2022.

35 *Estonia Presses Bush for Cyber-Attack Research Center*, The Wall Streat Journal, 25 VI 2007, [online] https://www.wsj.com/articles/BL-WB-2739, 8 XI 2022.

36 V. Socor, *Estonian President's U.S. Visit Reflects a Special Relationship*, The Jamestown Foundation, 28 VI 2007, [online] https://jamestown.org/program/estonian-presidents-u-s-visit-reflects-a-special-relationship/, 8 XI 2022.

Traktatu Północnoatlantyckiego[37]. Według NATO cyberatak nie jest działaniem zbrojnym naruszającym suwerenność innego podmiotu[38].

SKUTKI CYBERATAKÓW

Konsekwencje zmasowanych cyberataków na Estonię w 2007 roku można rozpatrywać w trzech aspektach: prawnym, organizacyjnym oraz rozwoju zdolności cybernetycznych Estonii. Mimo że obywatele tego kraju odczuli skutki ataków, np. poprzez przerwanie ciągłości wykonywanych usług bankowych, to szybkie podjęcie działań naprawczych przez państwo, wspierane przez sektor prywatny, spowodowało, że w ostatecznym rozrachunku Estonia na ataku skorzystała – a z czasem zyskała renomę lidera w sektorze cyfrowym.

Bezpośrednio po cyberataku pojawiła się wśród estońskich specjalistów w zakresie cyberbezpieczeństwa refleksja, że Estonia potrzebuje nowych strategicznych dokumentów i ram prawnych, które odstraszałyby potencjalnych cyberagresorów, ale także pozwalały identyfikować i karać sprawców, gdyby odstraszanie zawiodło[39]. Jedną z najbardziej znaczących zmian w estońskim prawie była modyfikacja kodeksu karnego w celu karania sprawców tzw. przestępstw komputerowych[40]. Znowelizowany kodeks karny zawiera szereg przepisów dotyczących cyberataków i cyberprzestępczości – zapisy koncentrują się na kwestiach kary i odpowiedzialności za popełnienie czynów zabronionych[41]. Inne zmiany prawne są ukierunkowane na ochronę danych, np. w 2007 roku wprowadzono aktualizacje procedur dostępu do informacji w Ustawie o informacji publicznej[42] oraz poprawki do Ustawy o komunikacji elektronicznej[43], które ustanawiają wspólne standardy bezpieczeństwa[44].

---

37 Zob. C. Czosseck, R. Ottis, A.M. Talihä, *Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security,* „Journal of Cyber Warfare and Terrorism" 2011, vol. 1, no. 1.

38 S. Lee, *Ethics of Cyberattack*, [w:] *The Ethics of Information Warfare*, red. K.W. Miller, M. Taddeo, Oxford 2014, s. 107.

39 S. Herzog, *Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity*, „Georgetown Journal of International Affairs" 2017, vol. 18, no. 3, s. 71.

40 J.A. Lewis, *Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States*, Institutions for Development Sector, VII 2016, [online] https://publications.iadb.org/publications/english/document/Advanced-Experiences-in-Cybersecurity-Policies-and-Practices-An-Overview-of-Estonia-Israel-South-Korea-and-the-United-States.pdf, 18 XI 2022.

41 *Penal Code*, Riigi Teataja, 6 VI 2001, [online] https://www.riigiteataja.ee/en/eli/522012015002/consolide, 9 XI 2022.

42 *Public Information Act*, Riigi Teataja, 15 XI 2000, [online] https://www.riigiteataja.ee/en/eli/514112013001/consolide, 9 XI 2022.

43 *Electronic Communications Act*, Riigi Teataja, 8 XII 2004, [online] https://www.riigiteataja.ee/en/eli/501042015003/consolide, 9 XI 2022.

44 J.A. Lewis, *Advanced Experiences...*

W 2008 roku rząd przedstawił pierwszą strategię bezpieczeństwa cybernetycznego. Określono w niej zasady, cele i metodologię poprawy krajowej infrastruktury cybernetycznej[45], nie tylko w strukturach rządowych, lecz także na poziomie społeczeństwa[46]. W dziedzinie edukacji obywateli rząd za pośrednictwem swojej agencji Information Technology Foundation for Education oferował szkolenia dla szkół i przedszkoli, jednocześnie angażując w ten proces rodziców i nauczycieli[47]. Ponadto w 2013 roku uruchomiono projekt partnerstwa państwowo-prywatnego, który miał na celu podniesienie umiejętności i świadomości w zakresie bezpieczeństwa użytkowników tzw. inteligentnych urządzeń, programistów oraz sprzedawców[48]. Wszechobecność technologii internetowych w sposób szczególny umożliwia zaangażowanie jednostek w oddolne budowanie pokoju[49].

Dodatkowo koncepcja bezpieczeństwa narodowego z 2010 roku wprowadziła pojęcie bezpieczeństwa zintegrowanego – kompleksowego zaangażowania całości rządowej administracji i społeczeństwa w kwestie bezpieczeństwa państwa[50]. W następstwie przyjęcia dokumentu Estonia zaktualizowała i uporządkowała akty prawne, na których podstawie funkcjonuje system bezpieczeństwa całościowego. Najważniejszymi przykładami takich działań były przyjęcie ustawy o obronie narodowej w 2015 roku, zastępującej wcześniejsze oddzielne regulacje dotyczące czasu pokoju i wojny, oraz nowelizacja ustawy o sytuacjach nadzwyczajnych z 2017 roku[51]. Wymienione regulacje przyczyniły się do budowy dojrzałej i kompleksowej kultury i polityki bezpieczeństwa cybernetycznego[52]. Estonia jest krajem, w którym planowanie strategiczne stoi na pierwszym miejscu, co zapewnia spójność całej architektury bezpieczeństwa cybernetycznego[53].

Za koordynację polityk w zakresie cyberbezpieczeństwa na poziomie państwowym od 2011 roku odpowiedzialne jest Ministerstwo Gospodarki i Łączności (est. Majandus-ja Kommunikatsiooniministeerium)[54]. W ramach ministerstwa działa Estoński

[45] M. Ghildiyal, *How Did Estonia Prepare for a Secure Cyber Security Architecture?*, CeSCube, 11 III 2022, [online] https://www.cescube.com/vp-how-did-estonia-prepare-for-a-secure-cyber-security-architecture, 12 XI 2022.

[46] *Cyber Security Strategy 2008*, Ministry of Economic Affairs and Communication, 2014, [online] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf, 12 XI 2022.

[47] M. Ghildiyal, *How Did Estonia...*

[48] *Tamże*.

[49] R. Nolte-Laird, *Peacebuilding Online: Dialogue and Enabling Positive Peace*, Dunedin 2021, s. 49.

[50] *National Security Concept of Estonia*, Kaitseministeerium, 12 V 2010, [online] https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia.pdf, 10 XI 2022.

[51] P. Szymański, *Nowe pomysły na obronę totalną. Bezpieczeństwo całościowe w Finlandii i Rosji*, Warszawa 2020, s. 40.

[52] D. Tomic, E. Saljic, D. Cupic, *Cybersecurity Policies of East European Countries*, Dubai 2018, s. 5-6.

[53] *Tamże*.

[54] *Riigi küberturvalisuse tagamine*, Majandus-ja Kommunikatsiooniministeerium, [online] https://www.mkm.ee/digiriik-ja-uhenduvus/kuberturvalisus/riigi-kuberturvalisuse-tagamine, 7 XI 2022.

Urząd ds. Systemu Informacji (est. Riigi Infosüsteemi Amet), centralny organ odpowiedzialny za bezpieczeństwo cybernetyczne[55]. Urząd przygotowuje także raporty i rekomendacje dla społeczeństwa, np. w kwestii cyberbezpieczeństwa w związku z cyberatakami prowadzonymi równolegle do działań konwencjonalnych w wojnie rosyjsko-ukraińskiej, która rozpoczęła się rosyjską agresją 24 lutego 2022 roku[56]. Za obronę narodową, w tym cyberobronę, odpowiada Ministerstwo Obrony Narodowej (est. Kaitseministeerium)[57]. W ramach Estońskich Sił Obrony (est. Eesti kaitsevägi) w 2018 roku powstało oddzielne dowództwo (est. Küberväejuhatus), które nadzoruje operacje w cyberprzestrzeni[58].

W następstwie cyberataków Estonia zwiększyła starania dotyczące ochrony infrastruktury teleinformatycznej[59]. Jednym z bezpośrednich skutków było powołanie Ligi Obrony Cybernetycznej (ang. The Estonian Defence League's Cyber Unit, LOC). Ta pierwsza na świecie cyberarmia składa się z oddziału ochotników, głównie specjalistów z zakresu bezpieczeństwa cybernetycznego, ale i wszystkich tych, którzy chcą się przyczynić do zwiększenia bezpieczeństwa w sieci (są wśród nich prawnicy, ekonomiści, studenci). Celem organizacji jest ochrona estońskiej cyberprzestrzeni poprzez współpracę między członkami LOC, rozpowszechnianie wiedzy i szkoleń, edukację w zakresie bezpieczeństwa informacji oraz udział w międzynarodowych szkoleniach dotyczących cyberbezpieczeństwa[60]. Nową cyberarmię powołała do życia ochotnicza Estońska Liga Obrony Totalnej (ELOT), która wspiera państwowe siły zbrojne[61]. Liga skupia ok. 17 tys. członków. Wraz ze stowarzyszonymi organizacjami, takimi jak: Ochotnicza Organizacja Obrony Kobiet (Naiskodukaitse), Młode Orły (Noored Kotkad) i Córki Domu (Kodutütred), ELOT ma ponad 28 tys. wolontariuszy w akcji[62]. Łączenie różnych zawodów, praktyk i wizji ochotników z sektora prywatnego to jeden ze sposobów budowy cyberobrony przez Estonię.

Kraj ten stał się również centrum koordynacji działań cybernetycznych dla różnych organizacji międzynarodowych. W maju 2008 roku w Tallinnie uruchomiono Centrum Doskonalenia Obrony Cybernetycznej NATO (ang. NATO Cooperative Cyber

---

55 *Estonia Faces Its Most Extensive Cyberattacks since 2007 after Soviet Monument Removal*, Baltic News Network, 18 VIII 2022, [online] https://bnn-news.com/estonia-faces-its-most-extensive-cyber attacks-since-2007-after-soviet-monument-removal-237275, 8 XI 2022.

56 *Venemaa sõda Ukrainas läbi küberdomeeni prisma*, Riigi Infosüsteemi Amet, 1 III 2022, [online] https://www.ria.ee/kuberturvalisus/kuberruumi-analuus-ja-ennetus/ohuhinnangud?view_instance=1&current_page=1, 7 XI 2022.

57 Strona Kaitseministeerium, [online] https://kaitseministeerium.ee/et, 7 XI 2022.

58 *Küberväejuhatus*, Eesti Kaitsevägi, [online] https://mil.ee/uksused/kubervaejuhatus/, 7 XI 2022.

59 P. Davies, *Estonia Hit by „Most Extensive" Cyberattack since 2007 Amid Tensions with Russia over Ukraine War*, Euronews, 19 VIII 2022, [online] https://www.euronews.com/next/2022/08/18/estonia-hit-by-most-extensive-cyberattack-since-2007-amid-tensions-with-russia-over-ukrain, 18 X 2022.

60 *Estonian Defence League's Cyber Unit*, Kaitseliit, [online] http://www.kaitseliit.ee/en/cyber-unit, 12 XI 2022.

61 *Tamże*.

62 *Tamże*.

Defence Centre of Exellence). Estonia wyszła z koncepcją centrum doskonalenia cyberobrony już w 2004 roku, ale Sojusz podszedł lekceważąco do propozycji, wskazał też na inne ważne w tamtym czasie inicjatywy, np. pomoc w wojnie w Afganistanie. Sfera cybernetyczna nie była jeszcze wtedy w centrum jego zainteresowania[63]. Sytuacja uległa zmianie po cyberatakach na jedno z państw NATO trzy lata później – wówczas zwrócono uwagę na tę inicjatywę i zintensyfikowano działania w tej materii. Pokłosiem były prace nad „Tallinn Manual", czyli dokumentem (w kilku wersjach) odnoszącym się do najpoważniejszych operacji cybernetycznych – czyli właśnie tych, które naruszają zakaz użycia siły, uprawniają państwa do skorzystania z prawa do samoobrony lub mają miejsce podczas konfliktu zbrojnego[64].

Zadaniami Centrum Doskonalenia Obrony Cybernetycznej NATO są wspieranie krajów w walce z cyberprzemocą, wzajemna wymiana informacji oraz szkolenie przyszłych profesjonalistów w dziedzinie cyberprzestrzeni. Obecnie w jego skład wchodzi 28 państw[65]. Wybór siedziby nie jest przypadkowy: od maja 2007 roku, kiedy Estonia stała się obiektem ataku cybernetycznego, Tallinn jest symbolem cyberwalki[66]. Centrum pozyskało akredytację w strukturze sił NATO, jednak trzeba pamiętać, że nie wchodzi w skład struktur dowodzenia Sojuszu, dlatego nie jest finansowane z jego budżetu – sponsorują je kraje członkowskie[67]. Utworzenie Centrum w Estonii pozwala jej budować wizerunek państwa innowacyjnego, kompetentnego i dobrze zarządzanego w dziedzinie bezpieczeństwa[68].

Estonia jest corocznym gospodarzem NATO Locked Shields, największych międzynarodowych technicznych ćwiczeń obrony teleinformatycznej na świecie[69]. Są one organizowane od 2010 roku przez Centrum Doskonalenia Obrony Cybernetycznej NATO wraz z estońskimi instytucjami rządowymi i koordynowane z terenów Estonii[70]. Ćwiczenia mają formułę zawodów, a nacisk kładziony jest na realistyczne scenariusze, najnowocześniejsze technologie i symulację złożoności masowego incydentu w cyberprzestrzeni[71]. W 2022 roku organizatorzy wykorzystali obecną sytuację geopolityczną

63 C.C. Bryant, *Cybersecurity 2020...*

64 *The Tallinn Manual*, CCDCOE, [online] https://ccdcoe.org/research/tallinn-manual/, 22 XI 2022.

65 Strona NATO Cooperative Cyber Defence Centre of Excellence, [online] https://ccdcoe.org/about-us/, 17 XI 2022.

66 Ang. *Distributed Dential-of-service* (rozproszona odmowa usługi) – ataki przeprowadzane za pomocą wielu komputerów, polegające na wysyłaniu do zainfekowanego komputera lub sieci dużej ilości zapytań lub informacji.

67 J. Dereń, A. Rabiak, *NATO a aspekty bezpieczeństwa w cyberprzestrzeni*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Warszawa 2014, s. 214.

68 P. Szymański, *Nowe pomysły na obronę totalną...*, s. 7.

69 R. Babraj, *NATO Locked Shields*, NASK, 23 IV 2018, [online] https://cyberpolicy.nask.pl/nato-locked-shields/, 8 XI 2022.

70 *Polacy z ABW, SKW, MON-u, WAT-u oraz CERT.PL zwyciężyli w ćwiczeniach NATO symulujących ataki internetowe*, Niebezpiecznik, 24 V 2022, [online] https://niebezpiecznik.pl/post/polacy-z-abw-skw-mon-u-oraz-cert-pl-zwyciezyli-w-cwiczeniach-nato-dot-atakow-internetowych/, 8 XI 2022.

71 R. Babraj, *NATO Locked Shields...*

do opracowania scenariuszy, które obejmowały przeprowadzenie ponad 8 tys. ataków na ok. 5,5 tys. wirtualnych systemów. Celami ataków były m.in.: systemy militarne, instalacje uzdatniania wody, systemy energetyczne, system telefonii 5G, system obrony przeciwlotniczej[72].

W Tallinnie zlokalizowana jest też Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi (EU-LISA)[73]. Agencja zarządza tego typu systemami, w tym niezbędnymi do funkcjonowania strefy Schengen, oraz udziela państwom członkowskim Unii Europejskiej wsparcia technologicznego w zwiększaniu bezpieczeństwa Europy[74].

E-STONIA

Mimo że Estonia to mały kraj, z populacją 1,3 mln, to ma silną infrastrukturę cyberobrony[75] i często nazywana jest Nadbałtycką Doliną Krzemową[76]. Według danych państwowej agencji statystycznej Statistics Estonia w 2022 roku aż 92,4% gospodarstw domowych miało dostęp do internetu, a 98% osób w wieku od 16 do 44 lat korzysta z niego codziennie lub prawie codziennie od 2019 roku[77]. Dla porównania: w Polsce regularną (co najmniej raz w tygodniu) obecność online w pierwszym kwartale 2022 roku zadeklarowało 77% dorosłych, o 4 punkty procentowe więcej niż przed rokiem[78]. W 2020 roku Estonia zajęła czwarte miejsce w *Global Cybersecurity Index*, przygotowywanym cyklicznie przez Międzynarodowy Związek Telekomunikacyjny (ang. International Telecommunication Union), jedną z wyspecjalizowanych organizacji ONZ[79].

Mieszkańcy Estonii to zatem jedno z najbardziej ucyfrowionych społeczeństw na świecie. Dodatkowo korzystają oni z usług wysoko rozwiniętej e-administracji, stąd szczególna dbałość państwa o zapewnienie bezpieczeństwa sieci komputerowych i systemów informatycznych.

---

72 *Locked Shields 2022*, Wojsko Polskie, [online] https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/locked-shields-2022/, 8 XI 2022.

73 P. Szymański, *Nowe pomysły na obronę totalną...*, s. 47.

74 *Regional Activities*, Ministry of Foreign Affairs Republic of Estonia, [online] https://vm.ee/en/international-law-cyber-diplomacy/cyber-diplomacy/regional-activities, 20 XI 2022.

75 P. Davies, *Estonia Hit by „Most Extensive" Cyberattack...*

76 S. Renteria, *Nadbałtycka Dolina Krzemowa*, PFR, 31 XII 2019, [online] https://pfr.pl/blog/nadbaltycka-dolina-krzemowa.html, 8 XI 2022.

77 *Information and Communication Technologies: Statistics Estonia*, [online] https://www.stat.ee/en/find-statistics/statistics-theme/technology-innovation-and-rd/information-and-communication, 20 XI 2022.

78 *Korzystanie z Internetu w 2022 roku*, komunikat z badań CBOS, Centrum Badań Opinii Społecznej, 2022, nr 77, [online] https://www.cbos.pl/SPISKOM.POL/2022/K_077_22.PDF, 20 XI 2022.

79 *Global Cybersecurity Index 2020*, ITU, 2023, [online] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E, 18 X 2022.

Podstawą cyfrowego społeczeństwa jest X-Road, oprogramowanie, które działa jak rozproszony rządowy system informacyjny i łączy ze sobą różne bazy danych i różne organizacje. *Jeśli coś stanie się z jedną częścią systemu, inna część systemu przejmuje kontrolę, a kopie zapasowe są umieszczane w różnych lokalizacjach i nie ma ani jednego punktu awarii* – skomentował działanie systemu Oliver Väärtnõu, dyrektor generalny firmy Cybernetica, która opracowała oprogramowanie X-Road[80]. Oprogramowanie zapewnia wymianę danych między podmiotami z różnych sektorów funkcjonowania państwa, takich jak szkolnictwo czy medycyna. Wszystkie dane wychodzące są podpisywane cyfrowo i szyfrowane, a wszystkie dane przychodzące – uwierzytelniane i rejestrowane[81]. Jest to oprogramowanie typu *open source.* X-Road jest wdrożony nie tylko w Estonii, lecz także w innych państwach, np. Finlandii, Japonii i Argentynie[82].

Ciekawą inicjatywą zmierzającą do podjęcia dodatkowych środków ostrożności w celu zapewnienia cyfrowej ciągłości jest tzw. ambasada danych. Zależność Estonii od technologii skłoniła przywódców tego kraju do poszukiwania partnerów dla tego przedsięwzięcia poza swoimi granicami, aby zabezpieczyć dane na wypadek ataku wojskowego lub innej poważnej sytuacji kryzysowej w państwie. Chcąc mieć pełną kontrolę i jurysdykcję nad swoimi danymi, rząd zdecydował się na ambasadę, ale bez ambasadorów i misji dyplomatycznych[83], czyli ambasadę danych, na mocy umowy obsługiwaną przez serwery w Luksemburgu. Warto wspomnieć, że jest to pierwszy tego typu projekt na świecie. Ambasada danych ma podtrzymać e-usługi w razie cyberataku na krajową infrastrukturę Estonii i zapewnić dalsze funkcjonowanie kluczowych usług e-administracji w jakiejkolwiek sytuacji kryzysowej w cyberprzestrzeni[84]. Jeśli systemy oparte na estońskiej infrastrukturze zostaną zaatakowane lub usługi zostaną zakłócone w przypadku zagrożenia krajowego, ambasady danych za granicą mogą pomóc w procesie odzyskiwania danych[85]. Estonia tworzy kopie zapasowe krytycznych danych i usług ważnych dla funkcjonowania państwa poza terytorium Estonii, pod warunkiem że dane i serwery w centrum danych są chronione takimi samymi gwarancjami prawnymi, jak dane i serwery w Estonii[86].

---

80 P. Davies, *Estonia Hit by „Most Extensive" Cyberattack...*, 18 X 2022.

81 Strona X-Road, [online] https://x-road.global/, 3 II 2023. Por. *Setting Up Government 3.0 Solutions Based on Open Source Software: The Case of X-Road*, [w:] *Electronic Government: 18th IFIP WG 8.5 International Conference, EGOV 2019, San Benedetto Del Tronto, Italy, September 2-4, 2019, Proceedings*, red. I. Lindgren i in., Cham 2019, s. 69-82.

82 Zob. *X-Road Community*, [online] https://x-road.global/xroad-world-map, 3 II 2023.

83 *Data Embassies: Sovereignty, Security, and Continuity for Nation-States*, Complex Discovery, 9 II 2022, [online] https://complexdiscovery.com/data-embassies-sovereignty-security-and-continuity-for-nation-states/, 22 XI 2022.

84 J. Collier, *Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom*, [w:] *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative*, red. M. Taddeo, L. Glorioso, Cham 2017, s. 192.

85 *Tamże*.

86 *Establishing the First Data Embassy in the World*, Observatory of Public Sector Innovation, 7 II 2017, [online] https://oecd-opsi.org/innovations/establishing-the-first-data-embassy-in-the-world/, 22 XI 2022.

Estonia stworzyła systemy wykrywania i ochrony incydentów, ćwiczyła współpracę zarówno z instytucjami publicznymi, jak i prywatnymi, znacząco przyczyniła się do wzrostu świadomości użytkowników i nieustannie uczestniczy w intensywnej współpracy międzynarodowej[87]. Dodatkowo jest prawdziwą kolebką start-upów[88]. To właśnie stamtąd pochodzą Skype, Playtech, Taxify, firma Bolt z sektora mobilności, a także aplikacja Wise do giełdowej wymiany kryptowalut[89]. Ponadto władze Estonii znacznie wcześniej niż władze innych państw zdecydowały się na cyfryzację państwa, wprowadzając cyfrowe głosowanie w wyborach, cyfrowe dowody osobiste czy chociażby połączenie z bezprzewodowym internetem dostępne w większości regionów kraju[90]. Warto też zwrócić uwagę, iż na mocy § 33 Ustawy o dostępie do informacji publicznej (est. Avaliku teabe seadus) każdej osobie przyznano prawo dostępu do informacji publicznej poprzez łącze internetowe, będące do dyspozycji w bibliotekach publicznych[91]. Tym samym Estonia stała się pierwszym krajem, który uznał prawo dostępu do internetu[92]. Biorąc pod uwagę centralną rolę cyfryzacji w jego rozwoju, kraj ten miał zatem naturalną motywację, aby po atakach z 2007 roku zintensyfikować działania w zakresie budowy cyberbezpieczeństwa.

ZAKOŃCZENIE

17 sierpnia 2022 roku Estonia została poddana najbardziej rozległym cyberatakom po 2007 roku[93]. Próby ataków DDoS były wymierzone zarówno w instytucje publiczne, jak i w sektor prywatny. Dzięki szybkiemu zastosowaniu odpowiednich środków zaradczych ataki w znacznym stopniu minęły niezauważone[94]. Odpowiedzialność za nie

87 *How Estonia Became a Global Heavyweight in Cyber Security*, e-Estonia, 14 VI 2017, [online] https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/, 10 XI 2022.

88 *Tamże*.

89 M. Fraser, *Prezydentka Estonii: brak ulg dla cyfrowych gigantów pozwolił na wzrost lokalnych startupów*, CyberDefence24, 21 IX 2021, [online] https://cyberdefence24.pl/polityka-i-prawo/prezydentka-estonii-brak-ulg-dla-cyfrowych-gigantow-pozwolil-na-wzrost-lokalnych-startupow, 8 XI 2022; *Estonia – ikona e-możliwości*, Thompson&Stein, [online] https://www.thompsonstein.com/estonia-ikona-e-mozliwosci/, 8 XI 2022.

90 *Tamże*.

91 *Avaliku teabe seadus*, Riigi Teataja, 15 XI 2000, [online] https://www.riigiteataja.ee/akt/12203 2011010, 8 XI 2022.

92 J. Rzucidło, *Prawo dostępu do Internetu jako podstawowe prawo człowieka. Część I*, „Kwartalnik Naukowy Prawo Mediów Elektronicznych" 2010, no. 2, [online] http://www.bibliotekacyfrowa.pl/Content/38666/PDF/009.pdf, 9 XI 2022.

93 *Yesterday, Estonia Was Subject to the Most Extensive Cyber Attacks It Has Faced Since 2007. Attempted DDoS Attacks Targeted Both Public Institutions and the Private Sector*. Zob. L. Ilves, wpis na Twitterze, 18 VIII 2022, [online] https://twitter.com/luukasilves/status/1560105663933587458, 20 XI 2022.

94 N. Bochyńska, *Estonia pod presją ataków DDoS. To może być dopiero początek*, CyberDefence24, 23 VIII 2022, [online] https://cyberdefence24.pl/cyberbezpieczenstwo/estonia-pod-presja-atakow-ddos-to-moze-byc-dopiero-poczatek, 22 XI 2022.

wzięła na siebie prorosyjska grupa KillNet. Podobne zdarzenia zarejestrowano podczas ćwiczeń cybernetycznych Locked Shields na początku 2022 roku[95]. Warto wspomnieć, że po cyberatakach z 2007 roku ataki DDoS są codziennością w estońskiej cyberprzestrzeni, lecz ich skuteczność jest znikoma ze względu na rozbudowany i sprawnie działający system ochrony cyberprzestrzeni.

Artykuł dotyczy konsekwencji, jakie przyniósł Estonii cyberatak będący jedną z odsłon konfliktu politycznego na linii Tallinn–Moskwa w 2007 roku. Istotą konfliktu nie była tzw. wojna pomników[96], ale sprzeciw mniejszości rosyjskiej wobec estońskiej polityki pamięci i próba wykorzystania przeniesienia pomnika Brązowego Żołnierza w walce o własne interesy. Strona rosyjska po raz kolejny sięgnęła po argumenty dotyczące ochrony praw rodaków w Estonii w kontekście krytykowanej polityki narodowościowej, manifestując swój sprzeciw wobec redukcji wpływów na obszarze posowieckim.

Skutki konfliktu są dostrzegane zarówno w budowie państwowego *soft*, jak i *hard power* w zakresie cyberbezpieczeństwa. Estonia zwiększyła swoją rolę we współpracy międzynarodowej na rzecz budowy bezpieczeństwa informacyjnego poprzez uświadamianie, ćwiczenia, badania i rozwój. Stanowi również przykład tego, jak sektory publiczny i prywatny powinny współpracować, aby zapewnić bezpieczeństwo wszystkim zaangażowanym stronom. Bez wątpienia szeroki wachlarz e-usług, inwestycje w nowoczesne technologie i społeczeństwo cyfrowe powodują, że Estonia przyciąga zagranicznych inwestorów, a jej sektor usług cyfrowych dla klientów firm oraz obywateli nadal szybko się rozwija. To wszystko sprawia, że Estonia wyznacza kierunki rozwoju innym podmiotom, zarówno państwowym, jak i międzynarodowym, innymi słowy – jest państwem przyszłości, a działania w zakresie bezpieczeństwa cybernetycznego obejmują zasięg i partnerstwa wykraczające poza tradycyjne umowy europejskie i transatlantyckie[97]. Estonia, nazywana Nadbałtycką Doliną Krzemową, to strona licznych dwustronnych umów o współpracy w obszarze cyberbezpieczeństwa[98]. Posiada najszerszy zakres instytucjonalnych polityk dotyczących bezpieczeństwa w cyberprzestrzeni w krajach bałtyckich[99] i słynie z innowacji, nowoczesnych technologii oraz rozwiązań cyfrowych.

Działania naprawcze po cyberatakach prowadzono zarówno w sferze publicznej, jak i prywatnej, a zabiegi rządu zmierzające do powrotu do stanu sprzed ataku mocno wspierał sektor komercyjny. Zrozumienie powiązań obu sfer w zakresie zapewnienia cyberbezpieczeństwa państwu jako całości jest kluczem do sukcesu przy szybkim wyjściu z sytuacji kryzysowej. Podobnie wyglądają działania związane z utrzymaniem

95 *Tamże*.

96 Przeniesienie pomnika Brązowego Żołnierza w 2007 roku w mniej eksponowane miejsce w Tallinnie było pokłosiem wydarzeń z 2006 roku, kiedy doszło do incydentu znieważenia flagi państwowej oraz zamieszek pomiędzy zwolennikami a przeciwnikami obchodów Dnia Zwycięstwa przy pomniku Ofiar II Wojny Światowej. Ataki na pomniki upamiętniające żołnierzy sowieckich zdarzały się już wcześniej, problem dotyczący kwestii sowieckich symboli nie był zatem niczym nowym. Zob. A. Szabaciuk, *Polityka etniczna...*, s. 226-228.

97 *Estonia's National Cybersecurity and Cyberdefense Posture...*

98 P. Szymański, *Nowe pomysły na obronę totalną...*, s. 40.

99 D. Tomic, E. Saljic, D. Cupic, *Cybersecurity Policies...*, s. 5-6.

pozycji państwa odpornego na cyberataki – tu też potrzeba koordynacji starań różnych sektorów państwa, w tym zaangażowania społeczeństwa, które stanowi fundament cybernetycznej odporności.

I chociaż cyberagresja na Estonię nie stanowi typu idealnego cyberwojny, a nawet zdaniem części badaczy z cyberwojną nie ma wiele wspólnego, to do dziś wskazywana jest w podręcznikach, artykułach prasowych czy komentarzach ekspertów jako przykład pierwszych ataków w cyberprzestrzeni wymierzonych w struktury państwowe przez inne państwo w celu realizacji celów politycznych. Jak wskazuje Rid, cyberwojna jeszcze się nie zdarzyła, a żaden dotychczasowy incydent nie spełnił trzech kryteriów właściwych samej wojnie: śmiercionośności, instrumentalności i politycznej motywacji[100]. Mimo to Estonia nadal pozostaje krajem-ofiarą, który na cyberataku sprzed lat zbudował cyfrową popularność i stał się wzorem dla innych w kwestii budowy państwowej odporności na incydenty komputerowe. Bez wątpienia rok 2007 ma obecnie wymiar symboliczny: atak na Estonię zwrócił międzynarodową uwagę na problem cyberbezpieczeństwa.

BIBLIOGRAFIA

Avaliku teabe seadus, Riigi Teataja, 15 XI 2000, [online] https://www.riigiteataja.ee/akt/122032011010.

Babraj R., *NATO Locked Shields*, NASK, 23 IV 2018, [online] https://cyberpolicy.nask.pl/nato-locked-shields/.

Baltrusaits D.F., *Cyber War: Do We Have the Right Mindset?*, [w:] *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, red. E.G. Carayannis, D.F.J. Campbell, M.P. Efthymiopoulos, Cham 2018, https://doi.org/10.1007/978-3-319-09069-6_24.

Bochyńska N., *Estonia pod presją ataków DDoS. To może być dopiero początek*, CyberDefence24, 23 VIII 2022, [online] https://cyberdefence24.pl/cyberbezpieczenstwo/estonia-pod-presja-atakow-ddos-to-moze-byc-dopiero-poczatek.

Bright A., *Estonia Accuses Russia of „Cyberattack"*, The Christian Science Monitor, 17 V 2007, [online] https://www.csmonitor.com/2007/0517/p99s01-duts.html.

Bryant C.C., *Cybersecurity 2020: What Estonia Knows about Thwarting Russians*, The Christian Science Monitor, 4 II 2020, [online] https://www.csmonitor.com/World/Europe/2020/0204/Cybersecurity-2020-What-Estonia-knows-about-thwarting-Russians.

Building Sustainable Peaces: Timing and Sequencing of Post-Conflict Reconstruction and Peacebuilding, red. A. Langer, G.K. Brown, Oxford 2016.

Collier J., *Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom*, [w:] *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative*, red. M. Taddeo, L. Glorioso, Cham 2017, https://doi.org/10.1007/978-3-319-45300-2_11.

[100] Rid wskazuje, że cyberwojna nigdy nie wystąpiła w przeszłości, nie trwa w teraźniejszości i jest bardzo mało prawdopodobne, że zakłóci przyszłość. T. Rid, *Cyberwar and Peace: Hacking Can Reduce Real-World Violence*, „Foreign Affairs" 2013, vol. 92, no. 6, [online] https://www.foreignaffairs.com/cyberwar-and-peace, 27 XI 2022.

Cyber Security Strategy 2008, Ministry of Economic Affairs and Communication, 2014, [online] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en.

Czosseck C., Ottis R., Talihä A.M., *Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security,* „Journal of Cyber Warfare and Terrorism" 2011, vol. 1, no. 1, https://doi.org/10.4018/ijcwt.2011010103.

Data Embassies: Sovereignty, Security, and Continuity for Nation-States, Complex Discovery, 9 II 2022, [online] https://complexdiscovery.com/data-embassies-sovereignty-security-and-continuity-for-nation-states/.

Davies P., *Cyberattacks Likely to Rise in Wake of Ukraine War: This Is What Estonia Learnt from Web War One*, Euronews, 1 VII 2022, [online] https://www.euronews.com/next/2022/05/26/cyberattacks-likely-to-rise-in-wake-of-ukraine-war-this-is-what-estonia-learnt-from-web-wa.

Davies P., *Estonia Hit by „Most Extensive" Cyberattack since 2007 Amid Tensions with Russia over Ukraine War*, Euronews, 19 VIII 2022, [online] https://www.euronews.com/next/2022/08/18/estonia-hit-by-most-extensive-cyberattack-since-2007-amid-tensions-with-russia-over-ukrain.

Dereń J., Rabiak A., *NATO a aspekty bezpieczeństwa w cyberprzestrzeni*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Warszawa 2014.

Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015, Warszawa 2015, [online] http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf.

Electronic Communications Act, Riigi Teataja, 8 XII 2004, [online] https://www.riigiteataja.ee/en/eli/501042015003/consolide.

Establishing the First Data Embassy in the World, Observatory of Public Sector Innovation, 7 II 2017, [online] https://oecd-opsi.org/innovations/establishing-the-first-data-embassy-in-the-world/.

Estonia – ikona e-możliwości, Thompson&Stein, [online] https://www.thompsonstein.com/estonia-ikona-e-mozliwosci/.

Estonia Faces Its Most Extensive Cyberattacks since 2007 after Soviet Monument Removal, Baltic News Network, 18 VIII 2022, [online] https://bnn-news.com/estonia-faces-its-most-extensive-cyberattacks-since-2007-after-soviet-monument-removal-237275.

Estonia Presses Bush for Cyber-Attack Research Center, The Wall Streat Journal, 25 VI 2007, [online] https://www.wsj.com/articles/BL-WB-2739.

Estonia's National Cybersecurity and Cyberdefense Posture: Policy and Organizations, Cyberdefense Report, Zürich, IX 2020, [online] https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Estonia.pdf.

Estonian Defence League's Cyber Unit, Kaitseliit, [online] http://www.kaitseliit.ee/en/cyber-unit.

Fraser M., *Prezydentka Estonii: brak ulg dla cyfrowych gigantów pozwolił na wzrost lokalnych startupów*, CyberDefence24, 21 IX 2021, [online] https://cyberdefence24.pl/polityka-i-prawo/prezydentka-estonii-brak-ulg-dla-cyfrowych-gigantow-pozwolil-na-wzrost-lokalnych-startupow.

Ghildiyal M., *How Did Estonia Prepare for a Secure Cyber Security Achitecture?*, CeSCube, 11 III 2022, [online] https://www.cescube.com/vp-how-did-estonia-prepare-for-a-secure-cyber-security-architecture.

Global Cybersecurity Index 2020, ITU, 2023, [online] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

Herzog S., *Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity*, „Georgetown Journal of International Affairs" 2017, vol. 18, no. 3, https://doi.org/10.1353/gia.2017.0038.

How Estonia Became a Global Heavyweight in Cyber Security, e-Estonia, 14 VI 2017, [online] https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.

ICMP Flood, Fundacja Instytut Cyberbezpieczeństwa, 27 X 2022, [online] https://instytutcyber.pl/artykuly/icmp-flood/.

Ilves L., wpis na Twitterze, 18 VIII 2022, [online] https://twitter.com/luukasilves/status/1560105663933587458.

Information and Communication Technologies: Statistics Estonia, [online] https://www.stat.ee/en/find-statistics/statistics-theme/technology-innovation-and-rd/information-and-communication.

Internet jako nowoczesne pole bitwy, [w:] *Obywatel w internecie*, red. M. Butkiewicz, P.P. Płatek, Warszawa 2017.

Jalonen J., *Dni, które wstrząsnęły Estonią*, przeł. P. Bukalska, Tygodnik Powszechny, 12 V 2019, [online] http://www.eesti.pl/index.php?dzial=panstwo&strona=cyberataki.

Juurvee I., Mattiisen M., *Report the Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict*, VIII 2020, [online] https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf.

Kofin M., *Atak cybernetyczny i awaria systemów informatycznych – paraliż państwa i życia obywateli na przykładzie Estonii, Gruzji, Litwy oraz Polski*, [w:] *Obywatel w internecie*, red. M. Butkiewicz, P.P. Płatek, Warszawa 2017.

Korzystanie z Internetu w 2022 roku, komunikat z badań CBOS, Centrum Badań Opinii Społecznej, 2022, nr 77, [online] https://www.cbos.pl/SPISKOM.POL/2022/K_077_22.PDF.

Kozłowski A., *Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan*, „European Scientific Journal" 2020, vol. 3, https://10.19044/esj.2014.v10n7p%25p.

Küberväejuhatus, Eesti Kaitsevägi, [online] https://mil.ee/uksused/kubervaejuhatus/.

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

Landler M., Markoff J., *In Estonia, What May Be the First War in Cyberspace*, The New York Times, 28 V 2007, [online] https://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html.

Lee S., *Ethics of Cyberattack*, [w:] *The Ethics of Information Warfare*, red. K.W. Miller, M. Taddeo, Oxford 2014, https://doi.org/10.1007/978-3-319-04135-3_7.

Leksykon politologii, red. A. Antoszewski, R. Herbut, Wrocław 2004.

Lewis J.A., *Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States*, Institutions for Development Sector, VII 2016, [online] https://publications.iadb.org/publications/english/document/Advanced-Experiences-in-Cybersecurity-Policies-and-Practices-An-Overview-of-Estonia-Israel-South-Korea-and-the-United-States.pdf.

Locked Shields 2022, Wojsko Polskie, [online] https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/locked-shields-2022/.

Majkowski W., *Koniec śledztwa w sprawie cyberataku na Estonię*, Polityka Globalna, 21 VIII 2012, [online] http://www.politykaglobalna.pl/2012/08/koniec-sledztwa-w-sprawie-cyberataku-na-estonie/.

Myers S.L., *Russia Rebukes Estonia for Moving Soviet Statue*, The New York Times, 27 IV 2007, [online] https://www.nytimes.com/2007/04/27/world/europe/27cnd-estonia.html.

National Security Concept of Estonia, Kaitseministeerium, 12 V 2010, [online] https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia.pdf.

Nolte-Laird R., *Peacebuilding Online: Dialogue and Enabling Positive Peace*, Dunedin 2021, https://doi.org/10.1007/978-981-16-6013-9.

Nordic Baltic Cooperation (NB8), Republic of Estonia. Ministry of Foreign Affairs, [online] https://www.vm.ee/en/international-relations-estonian-diaspora/regional-cooperation/nordic-baltic-cooperation-nb8.

Nowak A., *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe AON" 2013, no. 3.

Olejnik Ł., Kurasiński A., *Filozofia cyberbezpieczeństwa. Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny*, Warszawa 2022.

Penal Code, Riigi Teataja, 6 VI 2001, [online] https://www.riigiteataja.ee/en/eli/522012015002/consolide.

Pernik P., Maldre P., *Rising Challenges: Cybersecurity in the Baltic Sea Region*, [w:] *Baltic Visions: European Cooperation, Regional Stability*, red. K. Redłowska, Warszawa 2015.

Polacy z ABW, SKW, MON-u, WAT-u oraz CERT.PL zwyciężyli w ćwiczeniach NATO symulujących ataki internetowe, Niebezpiecznik, 24 V 2022, [online] https://niebezpiecznik.pl/post/polacy-z-abw-skw-mon-u-oraz-cert-pl-zwyciezyli-w-cwiczeniach-nato-dot-atakow-internetowych/.

Pomerantsev P., *To nie jest propaganda. Przygody na wojnie z rzeczywistością*, przeł. A. Paszkowska, Warszawa 2020.

Public Information Act, Riigi Teataja, 15 XI 2000, [online] https://www.riigiteataja.ee/en/eli/514112013001/consolide.

Regional Activities, Republic of Estonia. Ministry of Foreign Affairs, [online] https://vm.ee/en/international-law-cyber-diplomacy/cyber-diplomacy/regional-activities.

Renteria S., *Nadbałtycka Dolina Krzemowa*, PFR, 31 XII 2019, [online] https://pfr.pl/blog/nadbaltycka-dolina-krzemowa.html.

Rid T., *Cyberwar and Peace: Hacking Can Reduce Real-World Violence*, „Foreign Affairs" 2013, vol. 92, no. 6, [online] https://www.foreignaffairs.com/cyberwar-and-peace.

Rid T., *Wojna informacyjna*, przeł. F. Tryl, Warszawa 2022.

Riigi küberturvalisuse tagamine, Majandus-ja Kommunikatsiooniministeerium, [online] https://www.mkm.ee/digiriik-ja-uhenduvus/kuberturvalisus/riigi-kuberturvalisuse-tagamine.

Ruus K., *Cyber War I: Estonia Attacked from Russia*, The European Institute, [online] https://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia.

Rzucidło J., *Prawo dostępu do Internetu jako podstawowe prawo człowieka. Część I*, „Kwartalnik Naukowy Prawo Mediów Elektronicznych" 2010, no. 2, [online] http://www.biblioteka cyfrowa.pl/Content/38666/PDF/009.pdf.

Setting Up Government 3.0 Solutions Based on Open Source Software: The Case of X-Road, [w:] *Electronic Government: 18th IFIP WG 8.5 International Conference, EGOV 2019, San Benedetto Del Tronto, Italy, September 2–4, 2019. Proceedings*, red. I. Lindgren i in., Cham 2019.

Socor V., *Estonian President's U.S. Visit Reflects a Special Relationship*, The Jamestown Foundation, 28 VI 2007, [online] https://jamestown.org/program/estonian-presidents-u-s-visit-reflects-a-special-relationship/.

Strona FIRST, [online] http://www.first.org/.

Strona GEANT, [online] https://geant.org/.

Strona Kaitseministeerium, [online] https://kaitseministeerium.ee/et.

Strona NATO Cooperative Cyber Defence Centre of Excellence, [online] https://ccdcoe.org/about-us/.

Strona X-Road, [online] https://x-road.global/.

Szabaciuk A., *Polityka etniczna Republiki Estońskiej*, „Wschodnioznawstwo" 2016, no. 10.

Szymański P., *Nowe pomysły na obronę totalną. Bezpieczeństwo całościowe w Finlandii i Estonii*, Warszawa 2020.

The Tallinn Manual, CCDCOE, [online] https://ccdcoe.org/research/tallinn-manual/.

TCP SYN Flood, Imperva, [online] https://www.imperva.com/learn/ddos/syn-flood/.

Tiido A., *Wpływ kwestii mniejszości rosyjskiej na stosunki pomiędzy Republiką Estońską a Federacją Rosyjską*, [online] https://depotuw.ceon.pl/bitstream/handle/item/2197/streszczenie.pdf?sequence=3.

Tomic D., Saljic E., Cupic D., *Cybersecurity Policies of East European Countries*, Dubai 2018, https://doi.org/10.1007/978-3-319-06091-0_59-1.

Venemaa sõda Ukrainas läbi küberdomeeni prisma, Riigi Infosüsteemi Amet, 1 III 2022, [online] https://www.ria.ee/kuberturvalisus/kuberruumi-analuus-ja-ennetus/ohuhinnangud?view_instance=1&current_page=1.

Agnieszka WARCHOŁ – politolog i administratywista, doktor w dziedzinie nauk społecznych, w dyscyplinie nauki o polityce, specjalność – polityka bezpieczeństwa. Adiunkt w Katedrze Bezpieczeństwa Wewnętrznego Instytutu Bezpieczeństwa i Informatyki w Wydziale Nauk Społecznych Uniwersytetu Komisji Edukacji Narodowej w Krakowie. Autorka monografii naukowej pt. *Zagrożenia dla bezpieczeństwa informacyjnego państwa u progu XXI wieku* (2016), współautorka kilku monografii, m.in. *Współczesne zagrożenia bezpieczeństwa państwa* (2018), współredaktorka monografii *Uwarunkowania bezpieczeństwa międzynarodowego i narodowego na początku XXI wieku* (2019), autorka licznych artykułów naukowych dotyczących cyberbezpieczeństwa, bezpieczeństwa informacyjnego państwa, systemu bezpieczeństwa państwa. Prelegentka na konferencjach krajowych i międzynarodowych.