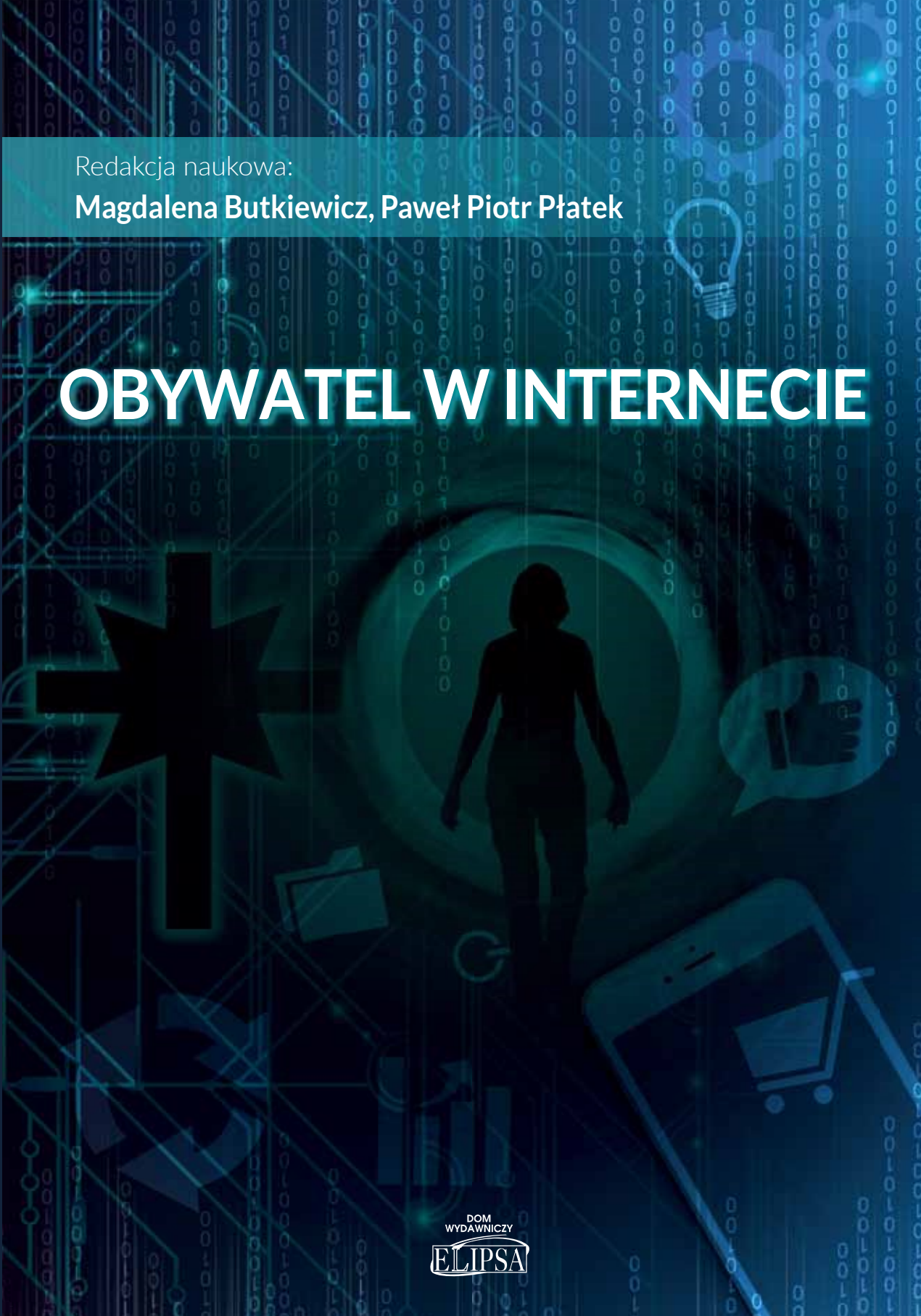
Redakcja naukowa:
Magdalena Butkiewicz, Paweł Piotr Płatek

OBYWATEL W INTERNECIE



DOM WYDAWNICZY
ELIPSA

OBYWATEL W INTERNECIE

OBYWATEL W INTERNECIE

Redakcja naukowa

dr Magdalena Butkiewicz
dr Paweł Piotr Płatek

Dom Wydawniczy ELIPSA

Warszawa 2017

Publikacja dofinansowana przez Uniwersytet Kardynała Stefana Wyszyńskiego
w Warszawie

Recenzenci
ks. dr hab. Andrzej Adamski, prof. WSIiZ
Wyższa Szkoła Informatyki i Zarządzania z siedzibą w Rzeszowie
ks. dr hab. Jarosław P. Woźniak
Katolicki Uniwersytet Lubelski Jana Pawła II

Projekt okładki
Agnieszka Miłaszewicz

Korekta
Paweł Płatek

ISBN 978-83-8017-158-9

DOM WYDAWNICZY ELIPSA
Dom Wydawniczy ELIPSA
ul. Inflancka 15/198, 00-189 Warszawa
tel./fax 22 635 03 01, 22 635 17 85
e-mail: elipsa@elipsa.pl, www.elipsa.pl

Spis treści

Wstęp 7

Część I. Obywatel i cyberwojna 9

mgr Mateusz Kofin
Atak cybernetyczny i awaria systemów informatycznych – paraliż państwa i życia obywateli na przykładzie Estonii, Gruzji, Litwy oraz Polski 11

dr Piotr Łuczuk
Internet jako nowoczesne pole bitwy. Cyberwojna i jej obszary – rys historyczny konfliktów w cyberprzestrzeni 24

Część II. Obywatel i cyberreligia 43

mgr Sergiusz Anoszko
Nowe ruchy religijne w przestrzeni on-line: Kościół Scjentologiczny a Internet .. 45

dr hab. Piotr Drzewiecki, prof. UKSW
Obywatel w nauczaniu Kościoła o środkach społecznego przekazu 63

Część III. Obywatel i cybermanipulacja 83

lic. Katarzyna Berta
Reklama internetowa w świadomości społeczeństwa na podstawie badania ilościowego 85

dr Magdalena Butkiewicz
Manipulacja i propaganda w Internecie a wolność obywateli 97

Część IV. Obywatel i cybertwórczość 117

lic. Magda Pasińska
Blog jako przestrzeń twórczej działalności internautów 119

lic. Mateusz Łysiak
Analiza aktywności w mediach społecznościowych Martyny Wojciechowskiej i Marka Kamińskiego 135

Biogramy 145

Wstęp

Człowiek nie może istnieć sam dla siebie. Arystoteles uważał ludzi za istoty społeczne. Tomasz Merton natomiast zapewniał, że nikt nie jest samotną wyspą i osoba potrzebuje innych do naturalnego rozwoju. Człowiek zatem potrzebuje zbiorowości. Jednak historia pokazała, że zbiór osób to niewystarczająca gwarancja przetrwania i poszanowania praw i przywilejów jednostki. Dlatego od najdawniejszych czasów ludzie łączą się w rodziny, klany, grupy. Ta hierarchia doprowadziła do powstania państw, u podstaw których jest obywatel.

Kim jest obywatel? W sensie prawnym jest to osoba fizyczna, która na mocy przynależności do danego państwa posiada prawa i wypełnia określone przez to państwo powinności. Prawa natomiast przedstawiają wzajemny poziom relacji między obywatelem a państwem. Konstytucja i pozostałe akty prawne stoją na straży obywatela. Są gwarantami jego swobód, wolności obywatelskiej, czyli przestrzeni, w którą nie wolno ingerować. Konstytucja Rzeczpospolitej Polskiej w rozdziale II. wspomina w sposób szczególny o obywatelu. Określa jego przywileje, tłumaczy zagadnienia związane z nabywaniem obywatelstwa, wyjaśnia zagadnienia ochrony, praw i wolności w przestrzeni, w której dany obywatel może się poruszać.

Z terminem „obywatel" związane są również inne zagadnienia. Choćby „obywatelskość", a więc: „zespół postaw poznawczych i normatywnych oraz odpowiadających im wzorów działania, preferencji wartości i celów, które są podstawą emocjonalnego i intelektualnego zaangażowania jednostek – członków określonej wspólnoty politycznej (państwowej), w sprawy publiczne, ich poczucia identyfikacji i akceptacji tradycji oraz systemu wartości własnej wspólnoty polityczno-kulturowej"[1]. Zatem bycie obywatelem, to również uczestnictwo w przestrzeni kulturowej oraz poszanowanie dla tradycji historycznej własnego narodu.

Czemu zatem *Obywatel w Internecie*? To metamedium – Internet – jest niewątpliwie najpopularniejszym środkiem komunikacji oraz wymiany wiedzy i informacji o świecie. Codziennie dokonuje się w jego przestrzeni milionów operacji bankowych, transakcji handlowych itd. Działanie w sieci objęte jest prawem w granicach świata rzeczywistego i w związku z tym dotyczy każdego obywatela danego państwa. Jest zatem konieczne, by ciągle analizować to, co

[1] *Obywatelskość*, w: *Leksykon politologii*, A. Antoszewski, R. Herbut (red.), Wrocław 2002, s. 265.

dzieje się w przestrzeni cyfrowej, ponieważ wpływa ona na działanie danego obywatela w rzeczywistości codziennej jego narodu. Dlatego też przedstawiona Państwu publikacja porusza szeroki zakres zagadnień związanych z tą materią.

Ostatnimi czasy oczywistym stało się, że nie tylko na świecie, ale również w cyberprzestrzeni człowiek nie może czuć się już dłużej bezpiecznie, niezależnie od przynależności do konkretnego narodu. W tej perspektywie dotyka nas problem cyberwojny, wojny informacyjnej, która może destabilizować funkcjonowanie jednostek administracyjnych w przestrzeni życia codziennego. Internet staje się również polem rozwoju dla wielu ruchów religijnych, ale także sekt. Nie tylko chrześcijaństwo buduje w tej przestrzeni platformę porozumienia i szerzenia Ewangelii. Obok niego spotkać można również szeroko zakrojone działania na rzecz popularyzacji islamu, judaizmu, ale również sekt, dla przykładu takich jak kościół scjentologiczny.

Internet to także przestrzeń, w której przedsiębiorcy – na różne sposoby – próbują zwiększać własne zyski, nie tylko rozbudowują więc oferty swoich sklepów internetowych, ale także promują swoje usługi i produkty uciekając się niekiedy do wykorzystania pewnych form manipulacji opinią konsumentów. Pod tym względem sieć stała się przestrzenią rozwoju dla nowych form reklamy. Jak pokazują przedstawione w publikacji wyniki badań, stanowi ona dynamicznie rozwijającą się gałąź handlu.

Nie można pominąć zagadnienia manipulacji w świecie wirtualnym. To metamedium nie służy dziś wyłącznie normalnym kontaktom interpersonalnym. Stało się przestrzenią wynaturzenia osoby, tworzenia fałszywych tożsamości i manipulacji umysłami tych obywateli, których określić można mianem internautów. Ważne jest jednak, aby nie zapominać o pozytywnych aspektach sieci, która buduje kulturę i rozwija twórczość w obrębie danego narodu. Cyberprzestrzeń stała się miejscem wymiany myśli np. poprzez blogi. Dała możliwość wypromowania swojej osoby i podzielenia się z innymi swoimi przemyśleniami oraz stylem życia.

Niniejsza publikacja jest kolejną, która powstała z inicjatywy pracowników Instytutu Edukacji Medialnej i Dziennikarstwa na Wydziale Teologicznym Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Stanowi ona następną „cegiełkę" w procesie ewolucji naszego sposobu postrzegania świata realnego i wirtualnego, ale tym razem w przestrzeni obywatelskiej. W imieniu Zespołu Redakcyjnego pragnę więc podziękować Autorom poszczególnych artykułów oraz wszystkim tym osobom, które przyczyniły się do powstania publikacji, jaką serdecznie polecamy Państwu do lektury.

Paweł Płatek

Część 1
Obywatel i cyberwojna

mgr Mateusz Kofin

Atak cybernetyczny i awaria systemów informatycznych – paraliż państwa i życia obywateli na przykładzie Estonii, Gruzji, Litwy oraz Polski

Streszczenie

Artykuł przedstawia zagrożenia prowadzące do paraliżu państwa i życia obywateli, jakie niesie za sobą rozwój cyberprzestrzeni w XXI wieku, na przykładzie: po pierwsze, ataków cybernetycznych inspirowanych przez Federację Rosyjską w Estonii w 2007 r., Gruzji i Litwie w 2008 r., oraz – po drugie – awarii systemów bankowych i rządowych w Polsce w I. połowie 2010 r., poprzedzających katastrofę pod Smoleńskiem.

Słowa kluczowe

cyberwojna, atak cybernetyczny, wojna informacyjna

Cyberwojna – nowy wymiar wojny informacyjnej

Wojny dzieli się zazwyczaj na dwie kategorie: wojnę energetyczną prowadzoną przy użyciu armii oraz informacyjną, której podstawowym celem jest wzbudzenie poczucia powszechnego strachu[1], nazywaną nieraz propagandową lub psychologiczną[2]. Do dzisiaj najbardziej wpływowymi strategami i teoretykami wojny pozostają: chiński generał Sun Tsu (VI w. p.n.e.), prekursor wojny psychologicznej, oraz pruski generał Carl von Clausewitz (1780-1831) – zwolennik klasycznych siłowych rozwiązań. Sun Tsu, nie był zwolennikiem rozwiązań

1 R. Brzeski, *Wojna Informacyjna*, „Fronda" (nr 60), 3/2011, s. 77.
2 P.M.A. Linebarger, *Wojna psychologiczna*, Waszyngton 1954, s. 5.

militarnych. Uważał on, że „sto zwycięstw w stu bitwach nie jest szczytem osiągnięć. Prawdziwym szczytem osiągnięć jest podbicie armii wroga bez walki”[3] oraz że „mądrzy władcy i przebiegli dowódcy pokonują przeciwników i dokonują wybitnych czynów, ponieważ z wyprzedzeniem zdobywają wiedzę o wrogu”[4]. Clausewitz z kolei jest autorem najbardziej znanej definicji wojny, odnoszącej się do relacji pomiędzy głównymi aktorami polityki międzynarodowej, jakim są państwa. W dziele *O Wojnie* pisał, że wojna jest: „prawdziwym narzędziem polityki, dalszym ciągiem stosunków politycznych, przeprowadzeniem ich innymi środkami. (…) aktem przemocy, mającym na celu zmuszenie przeciwnika do spełnienia naszej woli”[5].

W wieku XX, po II wojnie światowej, w dwubiegunowym układzie międzynarodowym opartym na rywalizacji dwóch mocarstw – USA oraz ZSRR – przy możliwości użycia przez każdą ze stron broni ostatecznej – atomowej, klasyczna wojna prowadzona przy użyciu konwencjonalnych metod stała się głównie konfliktem informacyjnym, w którym podstawowym narzędziem była dezinformacja[6]. W latach 70. XX wieku, wraz z rozwojem technologicznym, będącym według A. Tofflera *trzecią falą* po agrarnej i przemysłowej[7], z kształtującym się społeczeństwem informacyjnym[8], gdzie rywalizacja zaczęła wkraczać w obszar kosmosu i zaczęto powszechnie używać komputerów tworząc sieci komputerowe, doszło – według amerykańskiego pułkownika US Air Force, Johna Ashelya Wardena III – do wykształcenia się kolejnego obszaru toczenia wojny, którym po morzu, lądzie, powietrzu i przestrzeni kosmicznej stawała się cyberprzestrzeń[9]. Pojęcie cyberprzestrzeni po raz pierwszy pojawiło się w literaturze *science fiction* w powieści *Neuromancer* Williama Gibsona w 1984 roku. Gibson definiował ją jako metaforę: „która pozwala nam ogarnąć miejsce, gdzie, mniej więcej od czasu drugiej wojny światowej, tworzyliśmy stopniowo coraz większą ilość rzeczy określanych przez nas jako cywilizacja. To w cyberprzestrzeni przeprowadzane są operacje bankowe, również rozmowy telefoniczne”[10].

---

[3] Sun Tzu, Sun Pin, *Sztuka wojny*, Gliwice 2004, s. 32.

[4] Tamże, s. 134.

[5] C. von Clausewitz, *O wojnie*, Warszawa 2006, s. 15, 29.

[6] A. Golicyn, *Nowe kłamstwa w miejsce starych. Komunistyczna strategia podstępu i dezinformacji*, Warszawa 2007; V. Volkoff, *Dezinformacja – oręż wojny*, Warszawa 1991; V. Volkoff, *Montaż*, Poznań 2005.

[7] A. Toffler, *Trzecia fala*, Warszawa 1986.

[8] D. Bell, *The End of Ideology*, 1960.

[9] S. Czeszejko, *Działania w środowisku elektronicznym, a świadomość sytuacyjna pola walki*, „Journal of KONBiN” (18) 2/2011, s. 16.

[10] Cyt. za: A. Majdan, *William Gibson*, (brak daty publ.), http://www.iik.pl/biografie.php/37 (dostęp: 25.01.2018).

John Arquilla i David Ronfeldt, eksperci z RAND Corporation, którzy na początku lat 90. XX wieku alarmowali o nadejściu cyberwojen[11], zaproponowali w ramach wojny informacyjnej rozróżnienie między *netwojną* (ang. *netwar*) a *cyberwojną* (ang. *cyberwar*)[12]. *Netwar* jest konfliktem prowadzonym na wysokim szczeblu między narodami bądź grupami społecznymi, którego celem jest wpływanie na to, co populacja, która jest celem ataku, wie o swojej tożsamości, bądź o otaczającym ją świecie. *Netwojna* skupia się na opinii publicznej, na elitach rządzących lub obu tych celach, wykorzystując takie narzędzia jak: dyplomacja, propaganda, kampanie psychologiczne, dezinformacja bądź manipulowanie lokalnymi mediami, infiltracja sieci komputerowych i baz danych. *Cyberwojna* są to działania mające zakłócić lub zniszczyć systemy informatyczne i komunikacyjne wroga, które mogą być realizowane na kilka sposobów:

a) uderzenie mechaniczne – poprzez zrzucenie bomb czy wystrzelenie rakiet w kierunku budynków, w których umieszczone są serwery komputerowe,
b) atak impulsem elektromagnetycznym,
c) atak cyfrowy[13].

Wraz z rewolucją techniczną i informacyjną oraz pojawieniem się nowego wymiaru wojny, jakim jest cyberprzestrzeń, dochodzi wśród ekspertów do poszerzenia zakresu wojny informacyjnej. W dokumencie amerykańskiego Połączonego Komitetu Szefów Sztabów „Joint Doctrine for Command and Control Warfare" (C2W) współczesna wojna informacyjna została zdefiniowana jako: „działania zmierzające do osiągnięcia przewagi informacyjnej poprzez wpływanie na informacje posiadane przez przeciwnika, jego systemy informatyczne oraz sieci komputerowe, przy jednoczesnej ochronie własnych informacji i systemów oraz sieci informatycznych"[14]. Pojęcie cyberprzestrzeni, współcześnie zdefiniować można za Departamentem Obrony Stanów Zjednoczonych jako: „współzależną, powiązaną ze sobą sieć infrastrukturalną technologii informatycznej, obejmującą Internet, sieci telekomunikacyjne, systemy komputerowe oraz systemy kierujące procesami produkcji i kontroli w sektorach strategicznych dla bezpieczeństwa narodowego"[15].

---

[11] J. Arquilla, D. Ronfeldt, *Cyberwar is Coming!*, „Comparative Strategy", 12 (2)/1993, s. 141-165.

[12] K. Liedel, P. Piasecka, *Wojna cybernetyczna– wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe", 2011, nr 1, s. 22.

[13] Tamże, s. 22-23.

[14] Cyt. za: M. Lekowski, *Współczesna rewolucja w dziedzinie wojskowości. Analiza wybranych aspektów i cech charakterystycznych*, „Bezpieczeństwo Narodowe", 2011 nr 19, s. 270.

[15] Cyt. za: M. Ciecierski, *Szpiegostwo przemysłowe opanowało cyberprzestrzeń*, z 2.08.2016, http://www.wywiad-gospodarczy.pl/cyberprzestrzen.html (dostęp: 25.01.2017).

Cyberwojna od początku XX wieku stała się szczególnym przedmiotem zainteresowania badaczy i ekspertów z zakresu bezpieczeństwa[16], którzy wskazywali potencjalne zagrożenie. W kwietniu 2007 roku Sami Saydjari, szef organizacji Professionals for Cyber Defense, w przemówieniu przed Amerykańską Komisją Bezpieczeństwa Wewnętrznego przedstawił scenariusz niczym z literatury *science fiction*: „Gaśnie światło, Internet nie działa. Banki są zamknięte, nie można skorzystać z bankomatu. Radio i telewizja milczą. Lotniska i dworce kolejowe puste. Za to ulice – zupełnie zakorkowane. Po długiej nocy pojawiają się szabrownicy – policja nie jest w stanie przywrócić porządku. Nikt nie ma dostępu do pieniędzy, jedyne, co się teraz liczy to paliwo, jedzenie i woda. Zaczyna się panika…"[17], który – jak się okazało – spełnił się szybciej niż można było sobie wyobrazić.

Estonia, Gruzja, Litwa

Estonia jest przykładem jednego z najbardziej zinformatyzowanych państw w Europie, przez co nazywaną jest często E-Stonią. W Estonii ponad 90% transakcji bankowych dokonuje się *on-line*, istnieje możliwość składania deklaracji podatkowych w formie elektronicznej, każdy obywatel posiada Digital ID, umożliwiający głosowanie przez Internet[18]. Gdy w kwietniu 2007 roku estoński rząd zdecydował się na przeniesienie pomnika przedstawiającego żołnierza Armii Czerwonej z centrum Tallina na miejscowy cmentarz wojskowy, przez dwie noce – z 26 na 27 oraz z 27 na 28 kwietnia – estońską stolicą wstrząsały potężne zamieszki, prowokowane przez rosyjską młodzież. W tym samym czasie w Moskwie prokremlowska organizacja młodzieżowa zablokowała estońską ambasadę[19]. Najważniejszym obszarem konfliktu stał się jednak estoński Internet. 27 kwietnia o godzinie 22.30 strony estońskiego rządu zbombardowane zostały przez tzw. ataki DDoS (Distributed Denial of Service), polegające na zalewaniu upatrzonych serwerów gigantyczną ilością danych, co powoduje ich przeciążenie, a w efekcie doprowadza do blokady[20]. Apogeum ataków miało

---

16 S. Wierzbicki, *Wojny cybernetyczne jako element niekonwencjonalnej konfrontacji międzypaństwowej. Pragmatyczna rzeczywistość, nieunikniona przyszłość*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności", 2015, nr 2, s. 134-148.

17 Cyt. za: A. Nowak, *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe AON", nr 3(92) 2013, s. 10.

18 Tamże.

19 J. Jalonen, *Dni, które wstrząsnęły Estonią*, z 12.05.2009, http://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html (dostęp: 25.01.2017), M. Lakomy, *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*, „Stosunki Międzynarodowe – International Relations", tom 42, Warszawa 2010, s. 62.

20 J. Jalonen, dz. cyt.

miejsce 9 maja (w Rosji jest to Dzień Zwycięstwa), ruch na estońskich stronach WWW wzrósł ponad dwudziestokrotnie. 10 największych ataków miało siłę ponad 90 Mb/s, trwały one nieprzerwanie ponad 10 godzin[21]. W wyniku ataków zablokowane zostały strony rządowe, kancelarii prezydenta i głównych gazet, padły systemy bankowe oraz wewnętrzna sieć estońskiej policji. Estończycy zostali odcięci od informacji w Internecie oraz od dostępu do kont bankowych i ulokowanych na nich pieniędzy. Sytuacja zaczęła przypominać powieść *science fiction*: dwa największe banki, Hansapank i SEB Ühispank, musiały zawiesić usługi *on-line* i wstrzymać transakcje zagraniczne. Zamarła też strona największego dziennika „Postimees"[22]. Ataki cybernetyczne były tak dolegliwe dla funkcjonowania państwa, że estoński minister obrony Jaaka Aaviksoo stwierdził, że: „pierwszy raz zdarzyło się, żeby cyberataki stanowiły poważne zagrożenie dla bezpieczeństwa całego narodu"[23], rozważając nawet odwołanie się do artykułu 5 Traktatu Waszyngtońskiego. Władze Estońskie o atak obwiniły Federację Rosyjską, a premier Estonii Andrus Ansie pytany o przyczyny zdarzenia stwierdził: „komputery, które wykorzystano w ataku, miały adres administracji prezydenta Putina. Akcja przeciwko Estonii była doskonale zsynchronizowana – w tym samym czasie demonstranci atakowali naszą ambasadę w Moskwie i przedstawicielstwo linii lotniczych. A oficjalna delegacja rosyjska, która odwiedziła Tallin, stwierdziła, że rząd Estonii powinien się podać do dymisji"[24]. Prowadzone przez 5 lat śledztwo umorzone zostało w lipcu 2012 roku. Chociaż ustalono dane dużej liczby komputerów związanych z atakiem, to prokurator, Heili Sepp, stwierdziła, że: „większość z nich znajdowała się poza granicami Estonii, prośby o pomoc prawną przy dochodzeniu wysłane do rządów Federacji Rosyjskiej oraz Litwy okazały się bezskuteczne, nie było możliwości ustalenia czy hakerzy działali na zlecenie Kremla"[25]. Pomimo iż dla zwykłych obywateli atak cybernetyczny był raczej frustrujący niż niebezpieczny oraz zastosowano w nim prymitywne metody, jak DDoS, które nie wystarczyłyby do zniszczenia infrastruktury informatycznej, to osiągnięty został jednak efekt psychologiczny – wywołano poczucie niepewności i strachu, a zatem osiągnięto odwieczny cel wojny informacyjnej. Atak cybernetyczny na Estonię, wzmógł w konsekwencji dyskusję o tym, czy artykuł 5 Traktatu Waszyngtońskiego dotyczy także cyberwojny i cyberterroryzmu. W 2008 roku Tallin został siedzibą nowej NATO-wskiej

[21] A. Nowak, s. 11.
[22] Zob. J. Jalonen.
[23] Cyt. za: A. Nowak, s. 11.
[24] Tamże.
[25] Tamże.

instytucji: Cooperative Cyber Defence Centre of Excellence, czyli ośrodka koordynującego obronę NATO-wskiej cyberprzestrzeni[26].

Atak cybernetyczny na Estonię z 2007 roku nie był jedynym takim przypadkiem w ostatniej dekadzie w Europie. W 2008 roku doszło do dwóch podobnych incydentów, ale tym razem w Gruzji oraz na Litwie. Gdy w 2008 roku wojska rosyjskie wkroczyły na teren Abchazji i Osetii Południowej i zbliżyły się na kilkadziesiąt kilometrów do Tbilisi, to zaatakowana została gruzińska infrastruktura IT. 20 lipca niektóre rządowe strony WWW zostały podmienione. Później nastąpiły ataki DDoS, pojawiły się też sfałszowane komunikaty BBC i CNN, które w rzeczywistości infekowały komputery. Podobnie jak w przypadku Estonii, tak i tu atakowane były strony internetowe administracji rządowej (na których umieszczono zdjęcia porównujące gruzińskiego prezydenta Micheila Saakaszwiliego do Hitlera) oraz strony banków i ambasad państw wspierających Gruzję[27]. Za atakiem, według specjalistów, stać miała rosyjska organizacja Russian Business Network[28], a rosyjscy hakerzy atakować mieli w szczególności serwery internetowe z domeną o końcówce .ge, które na kilkanaście godzin przestały działać. Aby przywrócić ich funkcjonowanie, domenę dla gruzińskiego rządu udostępniła m.in. Kancelaria Prezydenta RP[29]. Jak wskazuje A. Kozłowski, „konflikt z 2008 roku był pierwszym w dziejach świata, który toczył się w czterech wymiarach, poza tradycyjnym: lądem, morzem i powietrzem, doszła do tego jeszcze cyberprzestrzeń. Działania w niej były zaplanowane i skoordynowane z wkroczeniem konwencjonalnych sił rosyjskich do Gruzji. Głównym celem hakerów w tej wojnie była dezinformacja przeciwnika oraz odcięcie rządu Saakaszwiliego od świata. Rosja, blokując strony administracji państwowej oraz główne serwisy informacyjne, chciała przedstawiać światu Gruzję i jej prezydenta jako niebezpiecznego podżegacza i ludobójcę, zabierając możliwość obrony. Był to przykład zastosowania propagandy przy użyciu środków z XXI wieku oraz przejaw wojny informacyjnej, która coraz częściej toczyć się będzie w cyberprzestrzeni. Paraliż stron rządowych miał też pokazać, że rząd Saakaszwiliego nie funkcjonuje i nie jest w stanie sprawować władzy nad własnym krajem. Rosjanie w ataku wymierzonym przeciwko Gruzji wyciągnęli wnioski z 2007 z Estonii, jednak po raz kolejny ich akcja nie spotkała się z całkowitym sukcesem. W osiągnięciu

---

[26] J. Jalonen.

[27] *Gruzja – Rosja – konflikt w cyberprzestrzeni*, z 14.11.2011, https://www.cybsecurity.org/gruzja-rosja-konflikt-w-cyberprzestrzeni/ (dostęp: 25.01.2017).

[28] S. Górski, D. Błaszczykiewicz, *Gruzja zaatakowana przez Rosję – również w Internecie*, z 11.08.2008, http://www.pcworld.pl/news/Gruzja.zaatakowana.przez.Rosje.rowniez.w.Internecie,162227.html (dostęp: 25.01.2017).

[29] R. Grodzki, *Wojna Gruzińsko-Rosyjska 2008. Przyczyny – przebieg – skutki*, Zakrzewo 2009, s. 108.