Studia Politicae Universitatis Silesiensis 2018, T. 21, s. 185—203
ISSN 2353-9747 (wersja elektroniczna)
www.studiapoliticae.us.edu.pl

Nowe trendy w aktywności państw w przestrzeni teleinformatycznej w drugiej dekadzie XXI wieku

New trends in activities of states in cyberspace in the second decade of the 21st century

Miron Lakomy*

Abstrakt

Prezentowany artykuł stanowi próbę zidentyfikowania nowych tendencji w zakresie aktywności aktorów państwowych w cyberprzestrzeni w drugiej dekadzie XXI wieku. W tekście wskazano na cztery, w opinii autora najważniejsze, trendy. Przede wszystkim, doszło do zmiany podejścia Federacji Rosyjskiej do wykorzystania potencjału przestrzeni teleinformatycznej w warunkach konfliktu zbrojnego, czego dowiodły doświadczenia Ukrainy. Po drugie, stosunkowo nowym zjawiskiem są wysoce zorganizowane kampanie cyberszpiegowskie, których celem jest wywieranie wpływu na procesy demokratyczne w państwach rozwiniętych. Po trzecie, doszło także do istotnego złagodzenia kontrowersji w dziedzinie cyberbezpieczeństwa między Chinami a USA. Wreszcie, potwierdzono użyteczność kom-

Abstract

This article identifies and characterizes new tendencies in activities of states in cyberspace in the second decade of the 21st century. The paper argues that there are four major trends noticeable. Firstly, the Russian Federation has changed its approach to the use of cyberspace during military conflicts, which was visible during the conflict in Donbass. Secondly, advanced cyber espionage campaigns attempting to influence democratic processes in developed countries have been also a new phenomenon. Thirdly, previous controversies between China and the U.S. on cybersecurity problems have been toned down due to their recent agreement. And finally, the usability of military cyber-units in asymmetric conflict was also proven.

Key words: cybersecurity, cyber war, cyber espionage, international security

* Instytut Nauk Politycznych i Dziennikarstwa, Wydział Nauk Społecznych, Uniwersytet Śląski w Katowicach (miron.lakomy@us.edu.pl).

ponentu cyberprzestrzennego sił zbrojnych w warunkach konfliktu asymetrycznego.

Słowa kluczowe: cyberbezpieczeństwo, bezpieczeństwo międzynarodowe, cyberwojna, cyberszpiegostwo

Wstęp

Już na przełomie XX i XXI wieku stało się oczywiste, że cyberprzestrzeń została nowym wymiarem rywalizacji i konfrontacji państw. Rządy wielu z nich zaczęły bowiem dostrzegać, iż szkodliwa aktywność w tym środowisku może ułatwiać realizację wybranych interesów w środowisku międzynarodowym. Temu narastającemu przez lata trendowi sprzyjały specyficzne cechy cyberprzestrzeni, w tym jej „ageograficzność" i niematerialność, łatwa do osiągnięcia anonimowość czy brak wywiadu strategicznego i systemu wzajemnego odstraszania. Innym czynnikiem, który odegrał znaczną rolę w tym procesie, były także postępy rewolucji informatycznej, implikujące większe uzależnienie państw i społeczeństw (w tym obiektów o znaczeniu strategicznym) od niezawodności technologii informacyjno-komunikacyjnych (ICT). Oznaczało to zarazem, iż stały się one podatne na szkodliwe oddziaływanie w cyberprzestrzeni. Wreszcie, istotnymi powodami ich rosnącej aktywności w sieci były nieskuteczność klasycznych mechanizmów polityki bezpieczeństwa wobec incydentów teleinformatycznych oraz problemy z ich interpretacją na gruncie prawa międzynarodowego publicznego. Wszystkie wskazane kwestie, z jednej strony, przyczyniały się do powstawania nowych form zagrożeń dla bezpieczeństwa narodowego i międzynarodowego, a z drugiej — zachęcały służby specjalne i wojsko do korzystania z rosnącego potencjału cyberprzestrzeni[1].

Rywalizacja państw w przestrzeni teleinformatycznej manifestowała się w rozmaity sposób, począwszy od inspirowania grup haktywistów do atakowania potencjalnych lub rzeczywistych przeciwników przez ataki komputerowe o charakterze wywiadowczym, aż po naruszanie integralności infrastruktury krytycznej. Metody, do których odwoływały się rządy oraz powiązane z nimi grupy podlegały więc stałej ewolucji, generując coraz poważniejsze dylematy z punktu widzenia bezpieczeństwa międzynarodowego. Istniało bowiem coraz większe ryzyko przekształcenia się incydentów teleinformatycznych w inne, nawet zbrojne formy konfrontacji państw[2].

[1] M. Lakomy: *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Katowice 2015, s. 93—114.

[2] Szerzej na temat cyberwojny w: M. Libicki: *The Cyberwar Challenge to NATO*. W: *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*. Red.

W tym kontekście, celem podjętym w artykule jest omówienie kilku wybranych, nowych trendów w zakresie aktywności państw w cyberprzestrzeni w drugiej dekadzie XXI wieku oraz przedstawienie ich wpływu na bezpieczeństwo międzynarodowe. W ostatnich latach można bowiem zaobserwować jakościowo nowe zjawiska, które w pierwszej dekadzie XXI wieku nie występowały bądź też miały marginalne znaczenie.

Główne cechy rywalizacji państw w cyberprzestrzeni na przełomie XX i XXI wieku

Analiza najnowszych trendów w zakresie aktywności państw w środowisku teleinformatycznym powinna zostać poprzedzona krótkim przeglądem wcześniejszych tendencji w tej dziedzinie, które występowały w latach dziewięćdziesiątych XX wieku oraz w pierwszej dekadzie XXI wieku.

W największym uproszczeniu, można zauważyć, iż w tym okresie rządy wykorzystywały do realizowania swoich interesów w środowisku międzynarodowym głównie cztery rodzaje metod. Przede wszystkim, jednym ze zjawisk, które pojawiły się najwcześniej, jest cyberszpiegostwo. Do pierwszych tego typu incydentów, których celem było nielegalne pozyskanie informacji niejawnych poprzez sieć, dochodziło już w latach osiemdziesiątych XX wieku. Do pewnej popularyzacji i profesjonalizacji tego procederu doszło jednak dopiero na przełomie XX i XXI wieku, o czym świadczyły dwie serie poważnych ataków komputerowych, przeprowadzonych w tym okresie na instytucje amerykańskie. W drugiej połowie lat dziewięćdziesiątych XX wieku Stanami Zjednoczonymi wstrząsnęła informacja o długoletniej operacji wywiadowczej *online*, której ofiarami padły między innymi NASA, National Oceanic and Atmospheric Administration, amerykańskie uniwersytety, a także marynarka wojenna oraz lotnictwo. Amerykańskie służby nadały jej kryptonim Moonlight Maze. Większość dowodów wskazywała na odpowiedzialność rosyjskich służb specjalnych, choć nigdy nie zostało to potwierdzone[3]. W kilka lat później, od 2003 roku, chińskie służby przeprowadziły operację określaną mianem Titan Rain, skierowaną przede wszystkim przeciwko amerykańskim

A. Podraza, P. Potakowski, K. Wiak. Warszawa 2013; A. Podraza: *Cyberterroryzm jako wzrastające zagrożenie dla bezpieczeństwa międzynarodowego w XXI wieku*. W: *Cyberterroryzm zagrożeniem XXI wieku*…, s. 34—35.

[3] B. Buchanan, M. Sulmeyer: *Russia and Cyber Operations: Challenges and Opportunities for the Next U.S. Administration*. Carnegie Endowment for International Peace 2016, s. 1.

komputerom należącym między innymi do United States Army Space and Strategic Defense[4].

W tym okresie aktywność szpiegowska zaczęła stawać się nagminnym zjawiskiem w przestrzeni teleinformatycznej, o czym świadczyło wiele przykładów. Przede wszystkim, Chiny były wielokrotnie oskarżane o prowadzenie w sieci zmasowanej kampanii wywiadowczej, której celem stały się zarówno instytucje federalne i stanowe USA oraz korporacje, jak i elementy infrastruktury krytycznej. Przykładowo, miały być odpowiedzialne za kradzież technologii samolotu F-35, która później miała zostać wykorzystana do budowy jego chińskiego odpowiednika wykorzystującego technologię *stealth*. W 2009 roku ChRL była także zamieszana w operację Aurora, skierowaną przeciwko korporacji Google[5]. Skalę amerykańskiej działalności wywiadowczej *online* ujawnił z kolei Edward Snowden, który przekazał dziennikarzom między innymi dokumenty świadczące o tym, iż USA włamywały się do sieci chińskich operatorów sieci komórkowych w celu przechwytywania milionów wiadomości SMS[6]. Podobną aktywność prowadziła także Rosja, o czym świadczyło istnienie grupy cyberszpiegowskiej określanej mianem APT28, która zaatakowała między innymi gruzińskie Ministerstwo Obrony oraz Ministerstwo Spraw Wewnętrznych, dziennikarzy zajmujących się tematyką kaukaską, a także wschodnioeuropejskie instytucje państwowe i wojsko. W 2008 roku Federacja miała stać także za poważnym włamaniem do sieci amerykańskiego Departamentu Obrony[7]. Reasumując, w pierwszej dekadzie XXI wieku rywalizacja państw w cyberprzestrzeni, manifestująca się wzajemnymi włamaniami o podłożu szpiegowskim, stała się zjawiskiem powszechnym, szczególnie wśród mocarstw.

Innym fenomenem, który wykształcił się w tym samym okresie, była aktywność, której celem nie było wyprowadzenie wrażliwych danych, lecz doprowadzenie do możliwie najpoważniejszych szkód i zniszczeń ze względu na określone motywacje polityczne sprawców, co można określić mianem cyberterroryzmu. Jakkolwiek pojęcie to bywa odnoszone głównie do działalności organizacji terrorystycznych w środowisku teleinformatycznym, to jednak w pierwszej dekadzie XXI wieku można było zaobserwować przynajmniej jedną operację o takim charakterze przeprowadzoną przez służby specjalne. Słynny robak komputerowy Stuxnet, odkryty w 2010 roku, został bowiem sku-

[4] N. Thornburgh: *Inside the Chinese Hack Attack* — https://courses.cs.washington.edu/courses/csep590/05au/readings/Titan.Rain.pdf (dostęp: 11.09.2017).

[5] S.W. Harold, M.C. Libicki, A.S. Cevallos: *Getting to Yes with China in Cyberspace*. Santa Monica 2016, s. 39.

[6] B. Malkin: *Edward Snowden Claims US Hacks Chinese Phone Messages* — http://www.telegraph.co.uk/news/worldnews/asia/hongkong/10137215/Edward-Snowden-claims-US-hacks-Chinese-phone-messages.html (dostęp: 11.09.2017).

[7] Zob. *APT28. A Window into Russia's Cyber Espionage Operations?* "FireEye Special Report" 2014.

tecznie użyty przeciwko irańskiemu ośrodkowi wzbogacania uranu w Natanz. Był to pierwszy przypadek w historii, kiedy cyberatak doprowadził do fizycznych zniszczeń elementów należących do infrastruktury krytycznej (ok. 1000 wirówek typu IR-1). Prawdopodobnie ten złośliwy program komputerowy został stworzony przez Stany Zjednoczone i Izrael w celu spowolnienia programu atomowego reżimu ajatollahów[8].

Należałoby również wspomnieć o coraz szerszym wykorzystaniu cyberprzestrzeni w ramach konfliktów oraz operacji zbrojnych. Z jednej strony, we wrześniu 2007 roku Izrael zbombardował budowany syryjski reaktor atomowy w okolicach Deir ez-Zor. Sukces tego nalotu miał wynikać między innymi stąd, iż przed jego rozpoczęciem został sparaliżowany system obrony przeciwlotniczej Syryjskiej Armii Arabskiej, dzięki czemu samoloty IDF bez przeszkód dotarły do celu. Według wielu źródeł cel ten osiągnięto za pomocą cyberataku na syryjskie komputery wojskowe[9]. Był to *de facto* pierwszy przykład bezpośredniego użycia cyberprzestrzeni do wsparcia klasycznej operacji zbrojnej. Niedługo później, w sierpniu 2008 roku, środowisko teleinformatyczne odegrało również istotną rolę w wojnie na Kaukazie. Prorosyjskie grupy, prawdopodobnie powiązane z służbami specjalnymi Federacji, przeprowadziły wówczas masową kampanię cyberataków wymierzonych w instytucje sektora prywatnego i publicznego Gruzji. Co prawda, integralność kluczowych elementów infrastruktury krytycznej oraz serwerów wojskowych nie została wówczas naruszona, jednak zablokowano w ten sposób rządowi w Tbilisi możliwość prowadzenia skutecznej polityki informacyjnej *online* w trakcie tego konfliktu. *Casus* ten potwierdził więc, iż aktywność w przestrzeni teleinformatycznej podczas wojny ma zasadnicze znaczenie z punktu widzenia walki informacyjnej[10].

Wreszcie, należałoby wspomnieć o trendzie, który zarysował się przede wszystkim na obszarze poradzieckim. Federacja Rosyjska w pewnym sensie wyspecjalizowała się bowiem w pierwszej dekadzie XXI wieku w inspirowaniu mas użytkowników Internetu do przeprowadzania cyberataków przeciwko „wrogom ojczyzny". Oprócz wspomnianego przykładu wojny w Gruzji w 2008 roku, gdzie „haktywiści patriotyczni" również odegrali pewną rolę, zjawisko to

[8] Zob. R. Langner: *To Kill a Centrifuge*. The Langner Group. November, 2013 — https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf; C. Morton: *Stuxnet, Flame, and Duqu — the OLYMPIC GAMES*. In: *A Fierce Domain: Conflict in Cyber Space, 1986 to 2012*. Ed. J. Healy. Arlington 2013.

[9] T. Rid: *Cyber War Will Not Take Place*. "Journal of Strategic Studies" 2012, Vol. 35, No 1, s. 16. Warto jednak zauważyć, iż w obecnie odtajnionych informacjach IDF na temat tej operacji wątek cyberataku się nie pojawia. Zob. M. Kamassa: *Odtajnienie izraelskiego ataku na syryjski reaktor. Nieprzypadkowy moment* — http://www.defence24.pl/odtajnienie-izraelskiego-ataku-na-syryjski-reaktor-nieprzypadkowy-moment (dostęp: 25.03.2018).

[10] A. Kozłowski: *Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan*. "European Scientific Journal" 2014, Vol. 3, s. 239—240; A. Cohen, R.E. Hamilton: *The Russian Military and the Georgia War: Lessons and Implications*. Carlisle 2011, s. 44—49.

stało się wyraźne przy okazji eskalacji estońsko-rosyjskiego sporu historycznego w kwietniu i maju 2007 roku. W jego tle grupy haktywistów, działających na rzecz interesów Federacji, w tym jej interpretacji historii najnowszej, przeprowadziły zmasowane cyberataki przeciwko komputerom należącym zarówno do instytucji państwowych, jak i sektora prywatnego sąsiada[11]. Ta trwająca kilka tygodni kampania była pierwszym na tą skalę przykładem motywowanego politycznie cyberataku na jakiekolwiek państwo. Dowiodła, iż odpowiednio zainspirowani obywatele, którzy posiadają wystarczającą wiedzę i umiejętności informatyczne, mogą posłużyć jako instrument realizowania celów polityki zagranicznej w tym specyficznym środowisku, jakim jest cyberprzestrzeń.

Działalność w cyberprzestrzeni podczas konfliktu zbrojnego na Ukrainie

Zgodnie z omówionymi procesami, w pierwszej dekadzie XXI wieku udowodniono użyteczność działań w cyberprzestrzeni podczas konfliktów zbrojnych. Doświadczenia Gruzji wskazywały nie tylko na użyteczność ataków komputerowych w kontekście realizowania określonych interesów w środowisku międzynarodowym, ale także na rosnące zdolności służb Federacji Rosyjskiej w tej dziedzinie. Wraz z wybuchem wojny na wschodzie Ukrainy na początku 2014 roku wielu ekspertów oczekiwało więc powtórzenia scenariusza kaukaskiego, w postaci zmasowanych cyberataków na systemy i sieci teleinformatyczne tego państwa. Zamiast nich wystąpiły jednak incydenty na zdecydowanie mniejszą skalę, które polegały przede wszystkim na podmianie zawartości wybranych stron WWW (*website defacement*), a także prostych atakach typu DDoS (*Distributed Denial of Service*) przeciwko instytucjom państwowym oraz mediom ukraińskim. Za wieloma z nich stała grupa haktywistyczna o nazwie CyberBerkut, choć można przypuszczać, iż była ona w jakiś sposób powiązana z służbami specjalnymi Federacji Rosyjskiej, podobnie jak miało to miejsce w przypadku wojny gruzińskiej. W tym kontekście, jednym z najpoważniejszych naruszeń cyberbezpieczeństwa Ukrainy było zaatakowanie komputerów i sieci należących do Centralnej Komisji Wyborczej przed oraz w trakcie wyborów prezydenckich w maju 2014 roku. Ich przejawem było między innymi zamieszczenie na stronie Komisji przed samym zamknięciem urn do głosowania 25 maja 2014 roku fałszywej informacji o zwycięstwie w wyborach lidera radykalnego Prawego

[11] S. Herzog: *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*. "Journal of Strategic Security" 2011, Vol. 4, No 2; M. Lakomy: *Cyberprzestrzeń jako nowy wymiar…*, s. 184—228.

Sektora Dmitrija Jarosza. Do sieci tej instytucji wprowadzono także zaawansowane oprogramowanie szpiegowskie (Sofacy/Sednit), co mogło wskazywać na udział rosyjskich służb specjalnych[12]. Co ciekawe, incydenty teleinformatyczne na Ukrainie występowały jeszcze przed wojną, w trakcie rewolucji na „Euromajdanie". Z jednej strony, od grudnia 2013 roku, z wykorzystaniem sieci botnet Black-Energy i Dirt Jumper, zaatakowano za pomocą DDoS wiele stron internetowych opozycji. Do szczególnie intensywnych działań w tej dziedzinie doszło w trakcie strzelaniny na Placu Niepodległości w dniach 18—20 lutego 2014 roku, kiedy telefony komórkowe ukraińskich deputowanych wspierających protesty były „zalewane" (*flood*) wiadomościami tekstowymi (SMS) i połączeniami telefonicznymi w celu uniemożliwienia im skutecznej komunikacji oraz koordynacji działań. Jednocześnie, podobną aktywnością wykazywała się także opozycja, wykorzystująca głównie metodę DDoS[13].

Ofiarą rosyjskiej kampanii cyberataków padły także wspierające Ukrainę organizacje i instytucje zachodnie, w tym strony internetowe Sojuszu Północnoatlantyckiego. CyberBerkut zaatakował także Polskę. Grupa ta wzięła na cel stronę prezydent.pl oraz Giełdę Papierów Wartościowych. W opublikowanym oświadczeniu wyjaśniającym powody tych włamań CyberBerkut oskarżył Polskę o to, iż „jest sponsorem ukraińskiego faszyzmu" oraz miesza się w konflikt zbrojny w Donbasie[14].

Warto podkreślić, iż w ograniczonym stopniu na aktywność Rosjan odpowiadali Ukraińcy oraz wspierające ich grupy. Za przejaw takiego działania można uznać cyberatak na strony internetowe prorosyjskiej stacji telewizyjnej RT w marcu 2014 roku. W nagłówkach wiadomości wymieniono słowa „Russia", „Russians" oraz „military" na „Nazi", co miało uderzyć w rosyjską kampanię informacyjną wobec wydarzeń na Ukrainie. Występowały także ataki komputerowe przeciwko rosyjskim instytucjom rządowym, za czym stała grupa haktywistyczna Anonymous OpUkraine[15].

Niewielka w gruncie rzeczy skala „zauważalnych" i „medialnych" cyberataków w trakcie wojny na Ukrainie nie oznacza jednak, iż rola cyberprzestrzeni podczas tych wydarzeń była ograniczona. Bardziej „tradycyjne" metody dzia-

---

[12] S. Sakkov: *Foreword*. In: *Cyber War in Perspective: Russian Aggression Against Ukraine*. Ed. K. Geers. Tallin 2015, s. 8—9; *Key Events*. In: *Cyber War in Perspective*…, s. 10; N. Koval: *Revolution Hacking*. In: *Cyber War in Perspective*..., s. 55—58.

[13] G. Pakharenko: *Cyber Operations at Maidan: A First-Hand Account*. In: *Cyber War in Perspective*…, s. 60—63.

[14] *Cyber-Berkut atakuje polskie serwisy internetowe. Prezydent.pl padł. GPW także* — https://niebezpiecznik.pl/post/cyber-berkut-atakuje-polskie-serwisy-internetowe-prezydent-pl-padl-gwp-tez/ (dostęp: 15.09.2017).

[15] D. Storm: *Political Hackers Attack Russia, Nazi Defacement, Threaten US CENTCOM with Cyberattack* — https://www.computerworld.com/article/2476002/cybercrime-hacking/political-hackers-attack-russia--nazi-defacement--threaten-us-centcom-with-cybera.html (dostęp: 15.09.2017).

łania w tej domenie zastąpiła bowiem aktywność o charakterze cyberszpiegowskim oraz informacyjnym. Z jednej strony, grupy rosyjskie stały za serią włamań do komputerów w celu pozyskania informacji zastrzeżonych, które bywały przekazywane opinii publicznej. Prawdopodobnie działały one na zlecenie rosyjskich służb specjalnych (APT), na co wskazuje użycie zaawansowanego, złośliwego oprogramowania typu Turla/Uroburos/Snake, a także RedOctober, MiniDuke i NetTraveler. Przykładowo, w połowie 2015 roku wspomniany CyberBerkut opublikował w sieci tysiące dokumentów należących do ukraińskiego Ministerstwa Obrony. Wskazywały one między innymi na plany podniesienia wydatków zbrojeniowych. Z drugiej strony, w tle konfliktu zbrojnego na wschodzie Ukrainy doszło do bezprecedensowej kampanii propagandowej. Prowadzona na przykład w mediach społecznościowych oraz na popularnych portalach, zasadzała się przede wszystkim na zamieszczaniu komentarzy krytycznych wobec nowych władz ukraińskich, przedstawianiu ich wizerunku zgodnie z interesami rosyjskimi, a także uzasadnianiu stanowiska wspieranych przez Federację rebeliantów. Stała za nią działająca w Sankt Petersburgu tzw. fabryka trolli, odpowiedzialna za produkowanie i rozpowszechnianie prorosyjskiej propagandy w sieci. Jednym z powszechnej stosowanych przez nią zabiegów było przedstawianie nowych władz ukraińskich jako nielegalnych bądź „faszystowskich". Dokonywano także zamiany zawartości Wikipedii[16].

Reasumując ten wątek, wydarzenia na Ukrainie stały się kolejnym po Gruzji przykładem konfliktu zbrojnego, któremu towarzyszyła intensywna działalność w cyberprzestrzeni. Wszystkie zainteresowane strony wykorzystywały bowiem ataki komputerowe do realizacji swoich interesów krótko- i długoterminowych, co przejawiało się dążeniem do uzyskania przewagi informacyjnej oraz podniesienia skuteczności szeroko rozumianej propagandy wojennej. Naturalnie przewagę uzyskała Federacja Rosyjska, która dysponuje olbrzymim potencjałem w tej dziedzinie. Niemniej jednak, koncentrując się przede wszystkim na aktywności cyberszpiegowskiej oraz operacjach psychologicznych (PSYOPS) w środowisku teleinformatycznym, zaskoczyła część ekspertów, spodziewających się powtórzenia scenariusza kaukaskiego bądź estońskiego, polegającego na zmasowanych cyberatakach wymierzonych w kluczowe usługi i strony internetowe. W tym kontekście rację może mieć więc Sven Sakkov, który wskazał na kilka powodów takiego stanu rzeczy. Jego zdaniem, Ukraina przede wszystkim nie stanowiła interesującego obiektu cyberataku o charakterze destrukcyjnym. Była i jest ona bowiem na relatywnie wczesnym etapie rewolucji informatycznej. Ponadto, zdaniem dyrektora natowskiego CCD COE, strona rosyjska dys-

[16] G. Pakharenko: *Cyber Operations*…, s. 61—63; *Key Events*. In: *Cyber War in Perspective*…; S. Berger: *Hackers Leak Ukraine Military Documents Revealing Plan to Increase Spending on Armed Forces* — http://www.ibtimes.com/hackers-leak-ukraine-military-documents-revealing-plan-increase-spending-armed-forces-1989742 (dostęp: 15.09.2017).

ponowała dużymi możliwościami dokonania sabotażu środkami tradycyjnymi, przez co wykorzystywanie zaawansowanych środków cyberprzestrzennych nie było potrzebne. Wreszcie, w jego opinii, obie strony starały się nie dopuścić do eskalacji tego konfliktu, zarówno na teatrach tradycyjnych, jak i w sieci[17].

Nowe akcenty w stosunkach amerykańsko-chińskich w dziedzinie cyberbezpieczeństwa

Jednym z najistotniejszych dla bezpieczeństwa międzynarodowego przejawów rywalizacji państw w środowisku teleinformatycznym w pierwszej dekadzie XXI wieku były incydenty komputerowe występujące na linii Chiny — Stany Zjednoczone. W pierwszych latach drugiej dekady XXI wieku ten trend był nadal kontynuowany, o czym świadczyło kilka kwestii. Przede wszystkim, poważną krytykę w USA zrodziły wspomniane chińskie cyberataki wymierzone w korporację Google, a także 34 inne przedsiębiorstwa amerykańskie, w tym Adobe, Yahoo, Symantec, Northrop Grumman, Dow Chemical[18]. Kontrowersje wywołał także raport amerykańskiej korporacji Mandiant z 2013 roku, w którym poddano analizie wiele incydentów teleinformatycznych w Stanach Zjednoczonych, Wielkiej Brytanii, Belgii, Indiach czy Izraelu, za którymi stała grupa określana jako APT1. W USA jej ofiarami padło aż 115 instytucji i przedsiębiorstw. Za ich organizację, według raportu, odpowiadała wyspecjalizowana jednostka wojskowa nr 61398 Chińskiej Armii Ludowo-Wyzwoleńczej[19].

Wśród znanych opinii publicznej przykładów chińskiej aktywności cyberszpiegowskiej wymierzonej w Stany Zjednoczone na początku drugiej dekady XXI wieku można wymienić między innymi:

— włamanie do komputerów U.S. Chamber of Commerce w 2010 roku,
— ataki na skrzynki poczty elektronicznej przedstawicieli amerykańskich instytucji rządowych w 2011 roku,
— włamanie do serwerów korporacji Lockheed Martin w maju 2011 roku,
— utracenie przez amerykański sektor obronny 24 tys. plików w marcu 2011 roku,

[17] S. Sakkov: *Foreword…*, s. 8—9.

[18] A. Jacobs, M. Helft: *Google, Citing Attack, Threatens to Exit China* — http://www.nytimes.com/2010/01/13/world/asia/13beijing.html?_r=1 (dostęp: 15.09.2017); J. Schofield: *Google, Yahoo, Adobe and Who?* — https://www.theguardian.com/technology/2010/jan/14/google-yahoo-china-cyber-attack (dostęp: 15.09.2017).

[19] Zob. *APT1. Exposing One of China's Cyber Espionage Units*. Mandiant 2013 — http://cs.brown.edu/courses/csci1800/sources/2013_Mandiant_APT1_Report.pdf (dostęp: 15.09.2017).

— ujawnienie operacji Shady RAT w 2011 roku, w ramach której zaatakowano między innymi 6 instytucji amerykańskich na poziomie federalnym, 5 na poziomie stanowym i 3 na poziomie hrabstw,
— ujawnienie w 2012 roku kampanii cyberszpiegowskiej wymierzonej w amerykańską infrastrukturę krytyczną (system gazociągów)[20].

Na tym tle należy zauważyć, iż amplituda ataków teleinformatycznych wymierzonych w Stany Zjednoczone oraz w inne państwa będące obiektem zainteresowania ChRL na początku drugiej dekady XXI wieku nadal rosła. Warto dodać, iż USA były nie tylko ofiarą, ale także sprawcą cyberataków. Według doniesień Edwarda Snowdena, miały one organizować i prowadzić operacje w przestrzeni teleinformatycznej, których celami były między innymi Chiny oraz Rosja[21]. W tym kontekście można więc było mówić o narastającej rywalizacji obu państw w cyberprzestrzeni, która miała istotny wpływ na pogorszenie stosunków dwustronnych. Stany Zjednoczone w działalności informatyków Chińskiej Armii Ludowo-Wyzwoleńczej upatrywały poważne zagrożenie bezpieczeństwa narodowego. Oficjele amerykańscy wielokrotnie formułowali oficjalne oskarżenia o odpowiedzialność ChRL za działalność cyberszpiegowską wymierzoną w USA, co z reguły wywoływało nerwową reakcję jej władz[22].

Nie może dziwić więc fakt, iż kwestia ta stała się przedmiotem intensywnych rozmów na najwyższym szczeblu, które rozpoczęły się w 2013 roku[23]. Należy podkreślić, iż inicjatywa ta miała charakter bezprecedensowy. Nigdy wcześniej dwa państwa, poróżnione na tle wykorzystania sieci przez własne służby oraz organizacje przestępcze, nie podjęły takich rozmów, których celem było osiągnięcie konsensu w tej trudnej materii. Co ciekawe, na tle kolejnych oskarżeń strony amerykańskiej o udział chińskiej armii w cyberatakach na USA, negocjacje zostały już po roku zerwane przez ChRL[24]. Mimo to, we wrześniu 2015 roku ogłoszono osiągnięcie porozumienia w tej dziedzinie, co miało miejsce w trakcie wizyty prezydenta Xi Jinpinga w USA. W komunikacie Białego Domu stwierdzono między innymi, że „Stany Zjednoczone oraz Chiny zgadzają się, że rząd żadnego z państw nie będzie prowadził lub świadomie wspierał kradzieży cybernetycznej własności intelektualnej, w tym sekretów handlowych

[20] M. Lakomy: *Cyberprzestrzeń jako nowy wymiar…*, s. 318—325.

[21] Ibidem, s. 325.

[22] J. Kaiman: *China Reacts Furiously to US Cyber-espionage Charges* — https://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges (dostęp: 15.09.2017).

[23] E. Piklington: *US and China to Discuss Cybersecurity at High-level Diplomatic Meetings* — https://www.theguardian.com/world/2013/jun/02/us-china-cybersecurity-hacking-espionage-meetings (dostęp: 19.05.2017).

[24] S.W. Harold, M.C. Libicki, A.S. Cevallos: *Getting to Yes with China in Cyberspace*. Santa Monica 2016.

lub innych zastrzeżonych informacji biznesowych"[25]. W innych punktach porozumienia przewidywano:

— szybką reakcję obu rządów na prośby o udzielenie informacji lub reakcję na szkodliwą aktywność w cyberprzestrzeni,
— współpracę w zakresie identyfikacji oraz promocji właściwych norm zachowań państw w przestrzeni teleinformatycznej,
— utworzenie mechanizmu dialogu wysokiego szczebla w zakresie zwalczania cyberprzestępczości oraz związanych z nią zagadnień[26].

Co jednak najważniejsze, osiągnięcie konsensu wywarło wymierny wpływ na poziom bezpieczeństwa teleinformatycznego Stanów Zjednoczonych. Jak wykazał raport korporacji FireEye z czerwca 2016 roku, od momentu zawarcia porozumienia odnotowano zdecydowany spadek aktywności chińskich grup cyberszpiegowskich nie tylko w USA, ale także w 25 innych państwach[27].

Reasumując, przyjęte przez USA i Chiny we wrześniu 2015 roku rozwiązanie spornych kwestii dotyczących zachowania w cyberprzestrzeni miało charakter bezprecedensowy. Nigdy wcześniej nie doszło bowiem do porozumienia tej rangi między dwoma wielkimi mocarstwami, dotychczas posiadającymi zupełnie odmienne interesy w tej dziedzinie. Jest to istotne osiągnięcie z punktu widzenia bezpieczeństwa międzynarodowego z trzech powodów. Po pierwsze, daje ono nadzieję, iż podobne spory i kryzysy występujące w stosunkach innych państw (np. USA — Rosja, Indie — Pakistan) mogą zostać uregulowane za pomocą metod dyplomatycznych. Po drugie, uwagę zwraca wysoka skuteczność tego rozwiązania, w które początkowo wielu ekspertów wątpiło. Obniżenie skali cyberataków jest rzeczą niezwykle cenną nie tylko dla USA i Chin. Jak wspomniano wyżej, skorzystały na tym także państwa postronne. Wreszcie, mając na uwadze fakt, iż od lat społeczność międzynarodową dzieli kwestia interpretacji norm prawa międzynarodowego w zakresie zachowania państw w cyberprzestrzeni, uzgodnienia na linii Pekin — Waszyngton dają nadzieję na przełamanie tego impasu.

Cyberataki na procesy wyborcze państw zachodnich

Kolejnym zauważalnym trendem w zakresie aktywności państw w środowisku teleinformatycznym w drugiej dekadzie XXI wieku są ataki komputerowe,

[25] The White House, Office of the Press Secretary: *FACT SHEET*: *President Xi Jinping's State Visit to the United States* — https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (dostęp: 15.09.2017).

[26] Ibidem.

[27] *Red Line Drawn: China Recalculates Its Use of Cyber Espionage*. "FireEye iSIGHT Intelligence Special Report", June 2016, s. 4.

których celem jest wywarcie wpływu na wyniki wyborów w państwach rozwiniętych. Zjawisko to potwierdziło opinie sceptyków, którzy tonowali popularną na początku milenium koncepcję e-wyborów, polegającą w dużym uproszczeniu na uwzględnianiu technologii informacyjno-komunikacyjnych w systemie wyborczym, włącznie z możliwością oddania głosu przez Internet[28].

Za pierwszymi i najpoważniejszymi incydentami tego typu stać miała rosyjska grupa cyberszpiegowska określona przez amerykańskie służby i korporacje mianem APT28[29]. Była ona odpowiedzialna za serię ataków komputerowych skierowanych przeciwko wybranym instytucjom politycznym w trakcie prezydenckiej kampanii wyborczej w Stanach Zjednoczonych w 2016 roku. Pierwsze, nieoficjalne informacje na temat rosyjskiej aktywności wokół wyborów pojawiły się w czerwcu tego roku. Śledztwo amerykańskich służb wykazało, iż APT28 działające w ramach operacji określanej mianem Grizzly Steppe, miało uzyskać nielegalny dostęp do cyfrowych danych należących do: Democratic National Committee oraz U.S. Democratic Congressional Campaign Committee. Zdobyto także wiadomości e-mail Johna Podesty, przewodniczącego komitetu wyborczego Hillary Clinton, oraz innych współpracowników tej kandydatki. Innymi słowy, kampania rosyjska była wymierzona *stricte* w Partię Demokratyczną, zapewne z powodu wyraźnie antyrosyjskich wypowiedzi Clinton w trakcie kampanii wyborczej. Warto podkreślić, iż samo uzyskanie informacji niejawnych z komputerów należących do PD lub jej członków nie mogło mieć jeszcze wymiernego wpływu na procesy demokratyczne w USA. Rosyjscy specjaliści zdobyte dane, szczególnie te, które mogły wywoływać poważne kontrowersje, zamieszczali jednak w Internecie[30]. Te z kolei przyciągnęły olbrzymią uwagę amerykańskiej i międzynarodowej opinii publicznej, w tym wiodących mediów, które wielokrotnie przywoływały i powielały ujawnione informacje[31], co mogło wpłynąć na wyniki wyborów prezydenckich, w których zwyciężył kontrkandydat Hillary Clinton — Donald Trump.

Już po wyborach, na przełomie lat 2016 i 2017 amerykańskie instytucje ujawniły wiele interesujących informacji na temat przebiegu tej kampanii cyberszpiegowskiej. Według raportu wywiadu amerykańskiego (Intelligence Community Assessment) z 6 stycznia 2017 roku, decyzja o zaatakowaniu komputerów należących do struktur oraz członków Partii Demokratycznej zapadła na

[28] Zob. np. *Towards Trustworthy Elections. New Directions in Electronic Voting*. Eds. D. Chaum et al. Berlin 2010.

[29] Według raportu NCCIC oraz FBI, w atakach brała udział także grupa APT29. Zob. *Grizzly Steppe — Russian Malicious Cyber Activity*. Joint Analysis Report, Federal Bureau of Investigation, NCCIC — https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf (dostęp: 16.09.2017).

[30] C.A. Theohary, C. Welt: *Russia and the U.S. Presidential Elections*. "CRS Insight" 2017, January 17; *Senate Intelligence Committee: Russia and 2016 Election*. "FireEye" 2017.

[31] Zob. np. *18 Revelations from Wikileaks' Hacked Clinton Emails* — http://www.bbc.com/news/world-us-canada-37639370 (dostęp: 16.09.2017).

najwyższym szczeblu władz rosyjskich. Prawdopodobnie polecenie w tej sprawie wydał sam Władimir Putin, który dzięki zdyskredytowaniu Hillary Clinton chciał zwiększyć szanse wyborcze Trumpa. Ponadto, działania służb Federacji Rosyjskiej były wynikiem wcześniejszej działalności cyberszpiegowskiej, skierowanej przeciwko amerykańskim instytucjom, think-tankom oraz grupom lobbystycznym. Dostęp do komputerów Democratic National Committee APT28 (związane prawdopodobnie z GRU) uzyskało bowiem już w czerwcu 2015 roku. Natomiast w marcu 2016 roku rozpoczęto samą operację przeciwko Demokratom. Co ciekawe, już w 2014 roku zdobyto także nielegalny dostęp do komputerów systemu wyborczego USA (Electoral Boards), choć w ocenie Departamentu Bezpieczeństwa Krajowego, nie miało to wpływu na proces zliczania głosów. Wreszcie, warto zwrócić uwagę na sposób przekazywania zdobytych informacji opinii publicznej. Według wywiadu USA wykorzystywano do tego:

— rumuńskiego „niezależnego" hakera o pseudonimie Guccifer 2.0 — choć istnieją spore wątpliwości, co do jego tożsamości,
— portal DCLeaks.com,
— portal Wikileaks[32].

W tym kontekście, trudno określić, w jakim stopniu rosyjskie cyberataki miały wpływ na wyniki wyborów prezydenckich w Stanach Zjednoczonych. Nie ulega jednak wątpliwości, że był to pierwszy przykład kampanii cyberszpiegowskiej, która uzyskała tak widoczne sukcesy i mogła rzeczywiście wywrzeć określony skutek na preferencje wyborców. Stanowiło to więc jakościowo nowe zjawisko, jeśli chodzi o działalność państw w środowisku teleinformatycznym. Warto podkreślić, iż nie było to zdarzenie incydentalne, lecz sygnał trendu, który może mieć charakter powszechny w przyszłości. W pierwszej połowie 2017 roku ujawniono bowiem informacje, które wskazywały na podobną działalność rosyjskich służb w cyberprzestrzeni skierowanych przeciwko kandydatowi na prezydenta Francji — Emmanuelowi Macronowi[33]. Tym razem jednak ich skuteczność okazała się zdecydowanie mniejsza, o czym świadczyło jego zwycięstwo nad kontrkandydatką preferowaną przez Moskwę — Marine Le Pen.

Reasumując, wydaje się, iż nowy trend, jakim są cyberataki skierowane przeciwko systemowi wyborczemu, partiom i grupom politycznym, a także kandydatom w wyborach ma istotne znaczenie dla bezpieczeństwa narodowego i międzynarodowego. Potencjalnie może on bowiem zaburzyć procesy demokratyczne, korzystając z luk w technologiach informacyjno-komunikacyjnych,

[32] *Assessing Russian Activities and Intentions in Recent US Elections*. Intelligence Community Assessment, Office of the Director of National Intelligence, 6.01.2017 — https://www.dni.gov/files/documents/ICA_2017_01.pdf (dostęp: 11.09.2017).

[33] B. Henderson, C. Graham: *Russia Blamed as Macron Campaign Blasts 'massive hacking attack' ahead of French Presidential Election* — http://www.telegraph.co.uk/news/2017/05/05/macron-campaign-blasts-massive-hacking-attack-ahead-french-presidential/ (dostęp: 16.09.2017).

z których powszechnie korzystają zarówno instytucje państwowe, jak i sami politycy. To z kolei może wpłynąć na dobór interesów i celów realizowanych przez nowe elity władzy na arenie międzynarodowej. Wydaje się jednak, iż mimo wszystko skuteczności takich działań nie można przeceniać. Omówione uprzednio dwa przypadki wskazują bowiem, iż ujawnianie opinii publicznej zdobytych za pomocą włamań komputerowych informacji o kandydatach miałoby określony wpływ na kampanię wyborczą tylko w sytuacji, w której posiadają oni zbliżone szanse na uzyskanie pozytywnego wyniku wyborczego. Co więcej, zawsze istnieje ryzyko, iż polityk, który nie będzie w ten sposób poszkodowany, wzbudzi pewną nieufność wśród krajowej opinii publicznej.

Operacje zbrojne w cyberprzestrzeni: kazus Stanów Zjednoczonych i tzw. Państwa Islamskiego

Ostatni trend, jaki jest zauważalny w działalności państw w cyberprzestrzeni, wiąże się z procesami dalszej militaryzacji tej domeny[34]. Mimo wieloletniego i rosnącego zainteresowania wielu armii na świecie potencjałem środowiska teleinformatycznego, widoczne postępy w tej dziedzinie poczyniło niewiele z nich. Do końca pierwszej dekady XXI wieku można też było mówić tylko o jednym, wspomnianym już przykładzie akcji militarnej, w której prawdopodobnie wykorzystano komponent cyberprzestrzenny[35].

W tym kontekście, tendencję tę potwierdziła aktywność amerykańskiej armii w cyberprzestrzeni, która została wymierzona w infrastrukturę teleinformatyczną tzw. Państwa Islamskiego. Decyzja o wykorzystaniu cyberataków przeciwko tej organizacji terrorystycznej wynikała przede wszystkim z faktu, iż działania w Internecie odgrywały olbrzymią rolę w prowadzonej przez nią kampanii propagandowej. Członkowie ugrupowania Abu Bakra al-Baghdadiego stworzyli niezwykle skuteczną maszynę propagandową, składającą się z sieci wyspecjalizowanych komórek, które od przełomu 2013 i 2014 roku produkowały wysokiej jakości materiały promujące ideologię dżihadu. Magazyny internetowe („Dabiq", „Rumiyah"), nagrania egzekucji jeńców (m.in. Jamesa Foleya czy Stevena Sotloffa), nagrania starć zbrojnych, „reklamy" czy „reportaże" zyskały olbrzymi rozgłos, a co za tym idzie, trafiły do milionów użytkowników sieci

[34] Zob. M. Dunn Cavelty: *The Militarisation of Cyberspace: Why Less May be Better*. In: *2012 4th International Conference on Cyber Conflict*. Eds. C. Czosseck, R. Ottis, K. Ziolkowski. Tallin 2012.

[35] Zob. T. Rid: *Cyber War…*, s. 16.

na całym świecie[36]. Istniała więc paląca potrzeba obniżenia zdolności tej grupy do produkcji i dystrybucji materiałów cyberdżihadystycznych. W tym celu Stany Zjednoczone zdecydowały się wykorzystać budowany od dawna potencjał USCYBERCOM oraz NSA, co w lutym 2016 roku ogłosił Sekretarz Obrony USA Ashton Carter. Wśród celów tej operacji wymienił on ograniczenie zdolności komunikacyjnych oraz kontroli i dowodzenia (*command & control*) Daesz, a także prowadzenia przez nią operacji na poziomie taktycznym i lokalnym[37]. Co ciekawe, U.S. Cyber Command powołała liczącą 100 osób Joint Task Force Ares, której celem było opracowanie cyberbroni zdolnych dokonywać szkód lub zniszczeń w zaatakowanych przez amerykańską armię systemach i sieciach teleinformatycznych należących do tzw. Państwa Islamskiego. Wśród działań podejmowanych w ramach tej operacji media wymieniały między innymi:

— zakłócanie systemu wypłat dla bojowników Daesz,
— identyfikację i zakłócanie platform komunikacyjnych tej grupy,
— włamywanie na konta członków organizacji,
— kasowanie zamieszczanych przez nią materiałów propagandowych w sieci,
— blokowanie dostępu specjalistów PI do wybranych serwisów internetowych[38].

Co prawda, skuteczność tych działań wywoływała pewne kontrowersje[39], jednak wydają się one nieuzasadnione. W latach 2016—2017 można było bowiem rzeczywiście zauważyć skuteczne ograniczenie zasięgu oddziaływania propagandowego tzw. Państwa Islamskiego w środowisku teleinformatycznym[40], co wskazywałoby na przynajmniej częściowe osiągnięcie zakładanych przez Pentagon celów. Co za tym idzie, udowodniono w ten sposób przydatność wojskowych cyberjednostek nie tylko do walki z aktorami państwowymi, ale także z organizacjami terrorystycznymi.

---

[36] Zob. D. Gartenstein-Ross, N. Barr, B. Moreng: *The Islamic State's Global Propaganda Strategy*. ICCT Research Paper, March 2016.

[37] R. Scarborough: *U.S. Cyber Command Launches Hacking Offensive against Islamic State* — http://www.washingtontimes.com/news/2016/feb/29/us-launches-cyber-attacks-islamic-state/ (dostęp: 17.09.2017).

[38] E. Nakashima: *U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies* — https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.c91ece2fddf6 (dostęp: 17.09.2017); E. Nakashima, M. Ryan: *U.S. Military Has Launched a New Digital War against the Islamic State* — https://www.washingtonpost.com/world/national-security/us-militarys-digital-war-against-the-islamic-state-is-off-to-a-slow-start/2016/07/15/76a3fe82-3da3-11e6-a66f-aa6c1883b6b1_story.html?utm_term=.23b62580ea67 (dostęp: 17.09.2017).

[39] Zob. C. Bing: *Why the U.S. is Struggling with the Digital War on ISIS* — https://www.cyberscoop.com/us-cyber-command-digital-war-isis/ (dostęp: 17.09.2017).

[40] Zob. M. Lakomy: *Cracks in the Online "Caliphate": How the Islamic State is Losing Ground in the Battle for Cyberspace*. "Perspectives on Terrorism" 2017, Vol. 11, No 3.

Zakończenie

Należy podkreślić, że w porównaniu z pierwszą dekadą XXI wieku, w latach 2010—2017, można było zidentyfikować wiele nowych zjawisk i procesów dotyczących szeroko pojętej działalności państw w cyberprzestrzeni. Przede wszystkim, warto zwrócić uwagę na nowy model działania przyjęty przez Federację Rosyjską. Po pierwsze, zaskakująca była strategia obrana przez Kreml na Ukrainie, gdzie znaczna część specjalistów spodziewała się powtórzenia scenariusza znanego z Gruzji. Służby rosyjskie ograniczyły jednak skalę swojej aktywności, skupiając się nie na sabotażu, lecz na zbieraniu zastrzeżonych danych oraz szeroko pojętej walce informacyjnej *online*. Takie podejście mogło wynikać ze specyficznego charakteru tej wojny. Po drugie, nowym, choć niezbyt zaskakującym zjawiskiem okazały się zmasowane ataki cyberszpiegowskie na elementy systemów wyborczych oraz partie polityczne państw zachodnich w celu wywierania wpływu na procesy demokratyczne. Trudno ocenić, czy nadal wywołująca olbrzymie kontrowersje w USA operacja Grizzly Steppe miała rzeczywisty wpływ na zwycięstwo Trumpa w wyborach prezydenckich w 2016 roku. Nie ulega jednak wątpliwości, iż potencjalna skuteczność takich zabiegów jest uwarunkowana wieloma czynników, wśród których najistotniejszą rolę odgrywa popularność kandydatów oraz poziom nieufności wyborców wobec niesprawdzonych informacji pojawiających się w Internecie. Po trzecie, zaskakującym wydarzeniem było osiągnięcie porozumienia między Stanami Zjednoczonymi a Chinami co do *modus operandi* w cyberprzestrzeni. Dotychczas oba państwa należały do najbardziej skonfliktowanych w zakresie działań w tym środowisku. Jest to nie tylko dowód na to, iż takie rozwiązania zarówno bi-, jak i multilateralne mają sens. Kazus ten stanowi także szansę na osiągnięcie konsensu na arenie międzynarodowej co do uniwersalnych zasad zachowania państw w przestrzeni teleinformatycznej. Wreszcie, po raz kolejny udało się potwierdzić użyteczność nowego, cyberprzestrzennego komponentu sił zbrojnych.

Bibliografia

APT1. Exposing One of China's Cyber Espionage Units. Mandiant 2013 — https://cs.brown.edu/courses/csi1800/sources/2013_Mandiant_APT1_Report.pdf (dostęp: 11.09.2017).

APT28. A Window into Russia's Cyber Espionage Operations? "FireEye Special Report" 2014.

Assessing Russian Activities and Intentions in Recent US Elections. Intelligence Community Assessment, Office of the Director of National Intelligence,

6.01.2017 — https://www.dni.gov/files/documents/ICA_2017_01.pdf (dostęp: 11.09.2017).

Berger S.: *Hackers Leak Ukraine Military Documents Revealing Plan to Increase Spending on Armed Forces* — http://www.ibtimes.com/hackers-leak-ukraine-military-documents-revealing-plan-increase-spending-armed-forces-1989742 (dostęp: 15.09.2017).

Bing C.: *Why the U.S. is Struggling with the Digital War on ISIS* — https://www.cyberscoop.com/us-cyber-command-digital-war-isis/ (dostęp: 17.09.2017).

Buchanan B., Sulmeyer M.: *Russia and Cyber Operations: Challenges and Opportunities for the Next U.S. Administration*. Carnegie Endowment for International Peace 2016.

Cohen A., Hamilton R.E.: *The Russian Military and the Georgia War: Lessons and Implications*. Carlisle 2011.

Cyber-Berkut atakuje polskie serwisy internetowe. Prezydent.pl padł. GPW także — https://niebezpiecznik.pl/post/cyber-berkut-atakuje-polskie-serwisy-internetowe--prezydent-pl-padl-gwp-tez/ (dostęp: 15.09.2017).

Dunn Cavelty M.: *The Militarisation of Cyberspace: Why Less May be Better*. In: *2012 4th International Conference on Cyber Conflict*. Eds. C. Czosseck, R. Ottis, K. Ziolkowski. Tallin 2012.

18 Revelations from Wikileaks' Hacked Clinton Emails — http://www.bbc.com/news/world-us-canada-37639370 (dostęp: 16.09.2017).

Gartenstein-Ross D., Barr N., Moreng B.: *The Islamic State's Global Propaganda Strategy*. "ICCT Research Paper" 2016, No 1.

Grizzly Steppe — Russian Malicious Cyber Activity. Joint Analysis Report, Federal Bureau of Investigation, NCCIC — https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf (dostęp: 11.09.2017).

Harold S.W., Libicki M.C., Cevallos A.S.: *Getting to Yes with China in Cyberspace*. Santa Monica 2016.

Henderson B., Graham C.: *Russia Blamed as Macron Campaign Blasts 'massive hacking attack' ahead of French Presidential Election* — http://www.telegraph.co.uk/news/2017/05/05/macron-campaign-blasts-massive-hacking-attack-ahead-french-presidential/ (dostęp: 16.09.2017).

Herzog S.: *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*. "Journal of Strategic Security" 2011, Vol. 4, No 2.

Jacobs A., Helft M.: *Google, Citing Attack, Threatens to Exit China* — http://www.nytimes.com/2010/01/13/world/asia/13beijing.html?_r=1 (dostęp: 15.09.2017).

Kaiman J.: *China Reacts Furiously to US Cyber-espionage Charges* — https://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges (dostęp: 15.09.2017).

Kamassa M.: *Odtajnienie izraelskiego ataku na syryjski reaktor. Nieprzypadkowy moment* — http://www.defence24.pl/odtajnienie-izraelskiego-ataku-na-syryjski-reaktor-nieprzypadkowy-moment (dostęp: 25.03.2018).

Key Events. In: *Cyber War in Perspective: Russian Aggression Against Ukraine*. Ed. K. Geers. Tallin 2015.

Koval N.: *Revolution Hacking*. In: *Cyber War in Perspective: Russian Aggression Against Ukraine*. Ed. K. Geers. Tallin 2015.

Kozłowski A.: *Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan*. "European Scientific Journal" 2014, Vol. 3.

Lakomy M.: *Cracks in the Online "Caliphate": How the Islamic State is Losing Ground in the Battle for Cyberspace*. "Perspectives on Terrorism" 2017, Vol. 11, No 3.

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

Langner R.: *To Kill a Centrifuge*. The Langner Group. November 2013 — https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf (dostęp: 11.09.2017).

Libicki M.: *The Cyberwar Challenge to NATO*. W: *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*. Red. A. Podraza, P. Potakowski, K. Wiak. Warszawa 2013.

Malkin B.: *Edward Snowden Claims US Hacks Chinese Phone Messages* — http://www.telegraph.co.uk/news/worldnews/asia/hongkong/10137215/Edward-Snowden-claims-US-hacks-Chinese-phone-messages.html (dostęp: 11.09.2017).

Morton C.: *Stuxnet, Flame, and Duqu — the OLYMPIC GAMES*. In: *A Fierce Domain: Conflict in Cyber Space, 1986 to 2012*. Ed. J. Healy. Arlington 2013.

Nakashima E., Ryan M.: *U.S. Military Has Launched a New Digital War against the Islamic State* — https://www.washingtonpost.com/world/national-security/us-militarys-digital-war-against-the-islamic-state-is-off-to-a-slow-start/2016/07/15/76a3fe82-3da3-11e6-a66f-aa6c1883b6b1_story.html?utm_term=.23b62580ea67 (dostęp: 17.09.2017).

Nakashima E.: *U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies* — https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.c91ece2fddf6 (dostęp: 17.09.2017).

Pakharenko G.: *Cyber Operations at Maidan: A First-Hand Account*. In: *Cyber War in Perspective: Russian Aggression against Ukraine*. Ed. K. Geers. Tallin 2015.

Piklington E.: *US and China to Discuss Cybersecurity at High-level Diplomatic Meetings* — https://www.theguardian.com/world/2013/jun/02/us-china-cybersecurity-hacking-espionage-meetings (dostęp: 19.05.2017).

Podraza A.: *Cyberterroryzm jako wzrastające zagrożenie dla bezpieczeństwa międzynarodowego w XXI wieku*. W: *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*. Red. A. Podraza, P. Potakowski, K. Wiak. Warszawa 2013.

Red Line Drawn: China Recalculates Its Use of Cyber Espionage. "FireEye iSIGHT Intelligence Special Report", June 2016.

Rid T.: *Cyber War Will Not Take Place*. "Journal of Strategic Studies" 2012, Vol. 35, No 1.

Sakkov S.: *Foreword*. In: *Cyber War in Perspective: Russian Aggression Against Ukraine*. Ed. K. Geers. Tallin 2015.

Scarborough R.: *U.S. Cyber Command Launches Hacking Offensive against Islamic State* — http://www.washingtontimes.com/news/2016/feb/29/us-launches-cyber-attacks-islamic-state/ (dostęp: 17.09.2017).

Schofield J.: *Google, Yahoo, Adobe and Who?* — https://www.theguardian.com/technology/2010/jan/14/google-yahoo-china-cyber-attack (dostęp: 15.09.2017).

Senate Intelligence Committee: Russia and 2016 Election. "Fireye" 2017.

Storm D.: *Political Hackers Attack Russia, Nazi Defacement, Threaten US CENTCOM with Cyberattack* — https://www.computerworld.com/article/2476002/cybercrime-hacking/political-hackers-attack-russia--nazi-defacement--threaten-us-centcom-with-cybera.html (dostęp: 15.09.2017).

The White House, Office of the Press Secretary: *FACT SHEET*: *President Xi Jinping's State Visit to the United States* — https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (dostęp: 15.09.2017).

Theohary C.A., Welt C.: *Russia and the U.S. Presidential Elections*. "CRS Insight" 2017, January 17.

Thornburgh N.: *Inside the Chinese Hack Attack* — https://courses.cs.washington.edu/courses/csep590/05au/readings/Titan.Rain.pdf (dostęp: 11.09.2017).

Towards Trustworthy Elections. New Directions in Electronic Voting. Eds. D. Chaum et al. Berlin 2010.

Miron Lakomy, dr hab. nauk społecznych w zakresie nauk o polityce (specjalność: stosunki międzynarodowe, bezpieczeństwo międzynarodowe). Adiunkt w Zakładzie Stosunków Międzynarodowych Instytutu Nauk Politycznych i Dziennikarstwa Uniwersytetu Śląskiego. Jego zainteresowania badawcze obejmują problematykę cyberdżihadyzmu, cyberbezpieczeństwa, oraz konfliktów zbrojnych. Opublikował dotychczas 3 monografie i ok. 50 artykułów naukowych.