mgr Jolanta Cichosz
mytutorial72@gmail.com

ZAGROŻENIA ASYMETRYCZNE W KONTEKŚCIE NOWYCH TECHNOLOGII. UNIA EUROPEJSKA, STANY ZJEDNOCZONE – STUDIUM PRZYPADKU

ASYMMETRIC THREATS IN THE CONTEXT OF NEW TECHNOLOGIES. EUROPEAN UNION, UNITED STATES – CASE STUDY

Streszczenie: Autor przedstawia aktualnie asymetryczne zagrożenia, które wpływają na globalne bezpieczeństwo. Celem artykułu jest analiza źródeł i zagrożeń asymetrycznych w kontekście nowych technologii. Cel zostanie osiągnięty zarówno poprzez analizę uwarunkowań bezpieczeństwa w cyberprzestrzeni wobec wyzwań i zagrożeń asymetrycznych dla państwa, jak również poprzez analizę stanu bezpieczeństwa. Teza przedstawiona w artykule brzmi następująco: nowe technologie w rękach nieuprawnionych podmiotów powodują asymetryczne zagrożenia w zakresie bezpieczeństwa państwa w wymiarze lokalnym i globalnym. Autor dokona analizy danych w zakresie źródeł i zagrożeń asymetrycznych w cyberprzestrzeni w kontekście nowych technologii, które są istotne dla bezpieczeństwa narodowego i międzynarodowego. Na podstawie analizy literatury w zakresie asymetrycznych zagrożeń autor przedstawia istotne wnioski dla bezpieczeństwa państwa.

Słowa kluczowe: zagrożenia asymetryczne, cyberprzestrzeń, nowe technologie.

Summary: The author presents current asymmetric threats that affect global security. The aim of this article is to analyze asymmetrical sources and threats in the context of new technologies. The goal will be achieved both by analyzing the conditions of security in cyberspace against challenges and asymmetric threats for the state, as well as by analyzing the state of security. The thesis presented in this article is: the new technologies in the hands of unauthorized entities cause asymmetric threats in the field of national security in the local and global dimension. The author will analyze data on asymmetrical sources and threats in cyberspace in the context of new technologies that are important for national and international security. Based on the analysis of literature in the field of asymmetrical threats, the author presents important conclusions for the security of the state.

Keywords: asymmetric threats, cyberspace, new technologies,

Wstęp

W ostatnich latach nasilają się trudności w utrzymaniu globalnego bezpieczeństwa wobec licznie pojawiających się asymetrycznych źródeł i zagrożeń. Według raportu Europolu z 2017 r. aż 85% użytkowników Internetu odczuwało obawy przed zagrożeniem

w cyberprzestrzeni (European, 2017, s. 12-30). Obecnie szybki rozwój nowych technologii powoduje powstanie licznych zmiennych od siebie zależnych, które wpływają na funkcjonowanie państwa. Identyfikacja potencjalnych źródeł zagrożeń jest trudna i często niemożliwa w zakresie wskazania podmiotów zagrożenia. Z kolei asymetria potencjałów pomiędzy licznymi podmiotami państwowymi i prywatnymi powoduje, iż szanse, ryzyka, wyzwania i zagrożenia pochodzące z cyberprzestrzeni mają rzeczywisty wpływ na globalne bezpieczeństwo. Państwa współuczestniczą w zmieniającym się cyber-środowisku i są odpowiedzialne za ochronę swojej cyberprzestrzeni. Zagrożenia środowisk mogą wynikać z nasilających się ataków na infrastrukturę państw oraz ich obywateli (użycie konwencjonalnej i niekonwencjonalnej broni), nielegalnej i szkodliwej ekonomicznie działalności, nieprzychylnych akcji propagandowych pogorszających wizerunek państwa na płaszczyźnie międzynarodowej. (Szubrycht, 2006, s. 141). Wobec powyższych zagrożeń celem artykułu jest dokonanie analizy i oceny kształtującego się paradygmatu zapewniania bezpieczeństwa przez państwa w obliczu nowych technologii. Jego treści są rezultatem rozwiązania następującego problemu badawczego: Jakie zmiany w ostatnich latach nastąpiły w wyniku masowo pojawiających się zagrożeń asymetrycznych w kontekście nowych technologii?

Współczesne zagrożenia

Po atakach terrorystycznych z 11 września 2001 r., które miały miejsce w Stanach Zjednoczonych, w których zginęło kilka tysięcy osób, zagrożenia niekonwencjonalne uznano w państwach transatlantyckich za jeden z najważniejszych problemów polityki bezpieczeństwa i największą groźbę dla ich stabilności. Zaliczono do nich: terroryzm międzynarodowy, transnarodową przestępczość zorganizowaną, użycie broni masowego rażenia i technologii informatycznych (Szubrycht, 2006, s. 141).

Biorąc pod uwagę rozważania, dotyczące zdefiniowania zagadnienia zagrożenia asymetrycznego, zasadne jest odwołanie się do koncepcji Robert D. Steele. Według autora wyłania się obecnie nowy paradygmat zagrożeń cechujący się dynamiką i nieliniowością, brakiem jakichkolwiek ograniczeń i reguł działania (Steele, 2002, s. 56). Wyjątkowo duża skala współzależności systemów teleinformatycznych powoduje poważne zagrożenia dla życia i zdrowia jednostek, funkcjonowania gospodarki państw i systemów międzynarodowych (Castells, 2010, s. 493-498). W wyniku analizy tematyki, zasadne są stwierdzenia autorów: Marka Madeja i Krystiana Piątkowskiego, że zagrożenie asymetryczne najczęściej stwarza strona, która dążąc do konfrontacji, nie jest zdolna przeciwstawić się przeciwnikowi w sposób symetryczny, z użyciem tych samych lub podobnych środków walki (Madej, 2005, s. 486-518) (Piątkowski, 2002, s. 23-24).

Zagrożenia asymetryczne w ujęciu politologicznym oznaczają odmienność metod działania i sposobów prowadzenia konfliktu oraz dysproporcje potencjałów (zwłaszcza militarnych) stron układu, którzy należą do różnych kategorii uczestników stosunków międzynarodowych, wśród których wyróżniono podmioty pozapaństwowe, trans- lub subnarodowe (Carte, 2001, s. 23-27). Z kolei według Roberta Steel, autora publikacji

New craft of the intelligence: achieving asymmetric advantage in the face of nontraditional threats zagrożenia asymetryczne są dokonywane przez podmioty, które można zaklasyfikować jako: siły zbrojne dysponujące zaawansowanymi technologicznie systemami uzbrojenia w danym państwie (*high-tech brutes the violent state threat)*, pozapaństwowe grupy kryminalne i terrorystyczne (*low-tech brutes, the violent nonstate threat)*, nieuzbrojone podmioty pozapaństwowe – wyznawcy ideologii, religii *(low-tech seers, the nonviolent nonstate threat)*, podmioty wykorzystujące zaawansowane technologie do nieautoryzowanego działania, grupy szpiegów gospodarczych *(high-tech seers, the volatile mixed threat)* (Steele, 2002, s. 9-14)

W strategiach militarnych analizowane są zagrożenia asymetryczne w różnych wymiarach, takich jak: ląd, morze, powietrze, przestrzeń kosmiczna, cyberprzestrzeń (Tabela 1). W Stanach Zjednoczonych wydzielono dodatkowo działania dokonywane poza morzem w obrębie pozostałych wód terytorialnych (Blank, 2003, s. 31),

Ocena środowiska zagrożeń jest kluczowym elementem dla sformułowania strategii każdego państwa i doktryny obronnej. Od września 2001 r. czynione są postępy w zakresie ochrony państwa, lecz większość działów operacyjnych nie wykorzystało konsekwentnie swoich planów strategicznych w zakresie priorytetowych zagrożeń i alokacji zasobów. Plany te wydają się być strategiami zarządzania bardziej niż dokumentami planowania strategicznego. Wnioski takie sformułowano na przykładzie oceny planów strategicznych Stanów Zjednoczonych odnoszących się do asymetrycznych zagrożeń. Skala nierozwiązanych zadań obronnych ujętych w strategicznych planach jest duża. Świadczy o tym przyznana ocena – niesatysfakcjonujący, w zakresie realizacji zadań typu „przydzielone zasoby" dla Wydziału antyterrorystycznego, Oddziału Cybernetycznego, Wydziału ds. Broni Masowego Zniszczenia oraz Wydziału Wywiadu FBI oraz zadania typu „zagrożenia pojawiające się" dla Wydziału Wywiadu sdla w roku 2015 (Tabela 2) (Hoffman, Meese, Roemer, 2015, s. 70).

Tabela 1. Ocena Komisji planów strategicznych FBI w zakresie zagrożeń asymetrycznych

Rodzaj sektora obronnego	Zagrożenia pojawiające się	Przydzielone zasoby	Strategia zarządzania
Wydział antyterrorystyczny Plan strategiczny	+	¾	+
Oddział Cybernetyczny Plan strategiczny	∞	¾	+
Wydział Broni Masowego Zniszczenia Plan strategiczny	+	¾	+
Zarządzanie wywiadem Plan strategiczny	¾	¾	+

Klucz: + satysfakcjonujący, ∞ rozwój, ¾ niesatysfakcjonujący

Źródło: Opracowanie własne: Report of the Congressionally-directed, 9/11 Revie-w Commission To The Director of the FBI by Commissioners Bruce Hoffman Edwin Meese, Timothy J. Roemer, (2015), s. 70.

Zagrożenia w cyberprzestrzeni

Zakres asymetrycznych zagrożeń w wymiarze globalnym wzrósł w ostatnich latach z powodu powszechnej dostępności do nowoczesnych technologii, które mogą ukrywać identyfikację użytkownika w czasie nieautoryzowanych działań. Przykładem powyższych działań są (The use, 2012, s. 68-133; Cloud, 2017, Dark, 2017, Ballagas, Borchers, Sheridan, Jennifer, 2006, s. 70-77; Sarga, Roman, 2013, s. 243-252, Yoongu, Jeremie, Hye, Donghyuk, Onur, 2014. s. 12, Cai, Onur, Ken, 2012. s. 4; Jiang, Khera, Wood, 2003, s. 2-4):

- wykorzystanie technologii chmurowej (technologia pozwala na zdalne przechowywanie informacji), która zmniejsza zdolność dowodową dotyczącą działań terrorystycznych przy udziale Internetu (ilość danych przechowywanych lokalnie na poszczególnych urządzeniach może być niewystarczająca do szybkiej weryfikacji atakujących – którzy wykupili czas obliczeniowy w chmurze na przykład tytułem działań typu botnet) (Cloud, 2017). Udostępnianie plików na platformach internetowych (np.: Rapidshare, Dropbox lub Fileshare) zapewnia stronom możliwość łatwego udostępniania baz danych, wyszukiwania plików multimedialnych za pośrednictwem Internetu,
- stosowanie anonimizujących serwerów pośredniczących – Proxy, protokołu bezpołączeniowego UDP/IP (protokół nie potwierdza przeprowadzenia transmisji), dynamicznie zmieniającego się adresu IP hosta oraz maskujących aplikacji np.: przeglądarki internetowej Tor (Dark, 2017),
- wykorzystanie technik anonimowości w komunikacji poczty elektronicznej przez ukrycie adresu IP poprzez usunięcie informacji identyfikującej użytkownika z nagłówka ramki (jednostka danych) przed przekazaniem jej do następnego serwera pocztowego,
- wykorzystywanie Chat rooms online (dedykowane kanały internetowe) chronionych hasłem może służyć organizacjom terrorystycznym i sympatykom do promowania poczucia wspólnoty w globalnym środowisku, gdyż informacje udostępniane podczas sesji online nie są zwykle rejestrowane przez usługodawcę, a zatem powyższe informacje mogą być niedostępne do pobrania po zakończeniu sesji online oraz do analizy sądowej twardego dysku,
- posługiwanie się smartfonami, tabletami stanowi potężną fizyczną infrastrukturę, która może być źródłem interakcji z infrastrukturą w określonym miejscu (Ballagas, Borchers, Sheridan, Jennifer, 2006, s. 70-77; Sarga, Roman, 2013, s. 243--252),
- stosowanie oprogramowania – radiowego o wysokiej częstotliwości transmisji HF zapewnia wymianę informacji za pośrednictwem serwera bez tworzenia danych czy loginów, co sprawia trudność w przechwyceniu wiadomości przesyłanych za pomocą tej metody w odniesieniu do znalezienia lokalizacji nadajników jak również do przewidywania częstotliwości w czasie rzeczywistym z jakim te komunikaty są przekazywane,

- korzystanie z usług internetowych działanie w ramach wspólnej sieci Wi-Fi znacznie komplikuje proces identyfikowania użytkownika, na przykład aplikacja Fon umożliwia zarejestrowanym użytkownikom dzielenie się częścią „rezydenta" sieci Wi-Fi wraz z innymi subskrybentami na całym świecie. Anonimowy dostęp do zabezpieczonych lub niezabezpieczonych sieci Wi-Fi może umożliwić użytkownikom maskowanie powiązań w czasie działalności internetowej z identyfikacją informacji,
- szyfrowanie danych w plikach JPEG i GIF za pomocą oprogramowania np.: WinZip, a następnie przesyłanie informacji, jako, plików-załączonych do wiadomości e-mail (utrudniona weryfikacja diagnostyki twardego dysku w zakresie brakującej objętości danych może wynikać z wielokrotnego szyfrowania informacji kilkoma kluczami),
- posługiwanie się podatnym na sterowanie oprogramowaniem lub sprzętem (IoT – *Internet of Things)*, pamięciami DRAM (Yoongu, Jeremie, Hye, Donghyuk, Onur, 2014. s. 12), NAND Flash (Cai, Onur, Ken, 2012. s. 4; Jiang, Khera, Wood, 2003, s. 2-4). Przejęcie sterowania sprzętu może nastąpić w wyniku zainfekowanie sprzętu podłączonego do Internetu, np.: złośliwym oprogramowaniem,
- budowanie nieautoryzowanych masztów przekaźnikowych transmisjii bezprzewodowej, pozwala na przechwytywanie informacji.

Jak wynika z powyższego, ogrom pojawiających się asymetrycznych zagrożeń jest wyzwaniem dla zapewnienia cyberbezpieczeństwa w obszarze infrastruktury krytycznej. Świadczenie usług przez serwery danych znajdujące się fizycznie w innej jurysdykcji może utrudniać uzyskanie kluczowych dowodów dotyczących postępowania sądowego, a tym samym stanowi wyzwanie w zakresie ścisłej koordynacji z miejscowymi organami ścigania.

Cyberzagrożenia i cyberataki stają się obecnie coraz bardziej powszechne, skomplikowane i szkodliwe. Wśród istotnych asymetrycznych zagrożeń dotyczących infrastruktury krytycznej wyróżnia się działania wywiadowczo-destrukcyjne nakierowane na urządzenia i sieci inteligentne *Smart Grids* (zbiór niezależnych mikro-sieci połączonych z monitorującym systemem SCADA) W obszarze działań penetracyjnych i destrukcyjnych, zidentyfikowano stosowanie różnych technik. Pozwalały one na przełamanie słabości zabezpieczeń systemów komputerowych, oprogramowania, ustawień sieciowych, takich jak: podatności w zabezpieczeniach systemu *typu Backdoors*, podatności protokołów sieciowych (np.: MODBUS, DNP3 i IEC 61850), brak uaktualnienia luk oprogramowania komputerowego, niewłaściwa polityka bezpieczeństwa, nieskuteczna wykrywalność nieautoryzowanych działań w cyberprzestrzeni, nieskuteczne strategie łagodzenia skutków działań inwigilacyjno-destrukcyjnych. Również w kampaniach, których celem było niszczenie informacji, w sieci Internet wykorzystywano wektory ataków, które złożone były z sekwencyjnych ataków na urządzenia zdalne, ataków na bazę danych, przechwytywania i modyfikowania informacji między nadawcą i odbiorcą typu *Man in The Middle Attack* (Saadawi, Colwell, 2017, s. 213; Remote, 2017).

W raportach dotyczących naruszeń danych cyfrowych Unii Europejskiej, Stanach Zjednoczonych, przekazywane są specyfikacje cyberzagrożeń, które nie mają jednoli-

tego nazewnictwa na obszarze UE i USA, co stwarza ryzyko nieprecyzyjnego szacowania zagrożeń w cyberprzestrzeni w wymiarze globalnym. I tak, Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji – ENISA, w 2016 r. zweryfikowała cyberzagrożenia typu (uzyskane od jednostek państwowych i prywatnych): *Malware*, *Web based attacks*, *Web application attacks*, *Denial of service*, *Botnets*, *Phishing*, *Spam, Ransomware*, *Insider threat* (*malicious, accidental*), *Physical manipulation/damage/theft/loss*, *Exploit kits*, *Data breaches*, *Identity theft*, *Information leakage, Cyber espionage* (*ENISA,* 2017).).

Z kolei w tym samym roku (2016) jednostka FBI Complaint Center (IC3) przekazała na podstawie zgłoszeń 280 000 poszkodowanych obywateli Stanów Zjednoczonych listę cyberzagrożeń podając rozbudowaną specyfikację. I tak, na liście zidentyfikowanych cyberzagrożeń wyróżniono: *Non-Payment/Non-Delivery* – 17 029, *419/Overpayment* – 25 716, *Personal Data Breach* – 27 573, *Employment* – 17 387, *Extortion* – 17 146, *Phishing/Vishing/Smishing/Pharming* – 19 465, *Identify Theft* – 16 878, *Harassment/Threats of Violence* – 16 385, *Credit Card Fraud* – 15 895, *Advanced Fee* – 15 075, *Confidence Fraud/Romance* – 14 546, *No Lead Value* – 13 794, *Other* – 12 619, *Real Estate/Rental* – 12 574, *Government Impersonation* – 12 344, *Business Email Compromise* – 12 005, *Tech support* – 10 850, *Misrepresentation* – 5436, *Lottery/Sweepstakes* – 4231, *Malware/ Scareware* – 2783, *Corporate Data Breach* – 3403, *Ransomware* – 2673, *IPR/Copyright and Counterfeit* – 2572, *Investment* – 2197, *Virus* – 1498, *Crimes Against Children* – 1230, *Civil Matter* – 1070, *Denial of Service* – 979, *Re-shipping* – 893, *Charity* – 437, *Health Care Related* – 369, *Terrorism* – 295, *Gambling* – 137, *Hacktivist* – 113, *Social Media* – 18 712, *Virtual Currency* – 1904 (2016 Internet, 2015, s. 19, 25-28).

Należy dodać, że naruszenia danych są również wykorzystywane jako element ataków hybrydowych w bardziej złożonym scenariuszu (The Real, 2017), na który mogą składać się wycieki danych, dezinformacja, ataki typu odmowa usługi, skoordynowane kampanie społecznościowe połączone z zastosowaniem metod socjotechnicznych lub innych działań (Ducaru, 2016, s. 2, 3) tytułem przejęcia funduszy, wpływów politycznych. Przykładem przeprowadzonych hybrydowych ataków była kampania prezydencka w USA (A new era*,* 2017) oraz kryzys ukraiński (Ukrainian, 2016).

Skala globalnych asymetrycznych zagrożeń w cyberprzestrzeni intensywnie zwiększa się począwszy od początku XXI wieku. Wysokość strat finansowych, spowodowanych przez przestępstwa w cyberprzestrzeni w Stanach Zjednoczonych w 2016 r. wynosiła ponad 1 miliard dolarów (Opracowane, 2017). Według Global Terrorism Index 2016 w ciągu ostatnich 15 lat nastąpiło istotne przesunięcie paradygmatu – terroryści (np.: ISIL – *the Terrorist Organisation Islamic State in Iraq and the Levant* a także al-Qaida) jako poważne zagrożenie (ataki przeciwko rządom) w otwartej sieci Internet. Do asymetrycznych działań, grupy terrorystyczne wykorzystują nowoczesne technologie działające online, należą do nich szyfrujące komunikatory oraz internetowe platformy, takie jak: Twitter, Telegram, Zello, Tumbir, Snapchat, Silent Circle, WhatApp, Kik, Last.fm. Instagram, Alrawi, Archie.org, Google Drive, Dating Websites, ISISsinglers.com, Quora, Skype, Threema, WordPress, YouTube, JustPaste.it (Gambhir, 2016, s. 21-33). Obecnie ISIL zjednoczyło pięć różnych grup hakerskich w *United Cyber Caliphat*, których celem jest budowanie cyber armii do obsługi forów internetowych, które umożliwią zwolenni-

kom przeprowadzenie kampanii cyber-terrorystycznych *Electronic Jihad*, polegających na włamaniu się do sieci energetycznych – co wynika z zasad działania ich organizacji – *The 39 Principles of Jihad*. Powyższe działania wspierają grupy hakerów np.: A Kosovan, Ardit Ferizi, którzy przejęli m. in.: 1350 danych osobowych amerykańskich żołnierzy i pracowników rządu, celem dalszego nieautoryzowanego wykorzystania pozyskanej identyfikacji (Global, 2016, s. 88). ISIL Aby uniknąć wykrycia swoich działań trenuje swoich zwolenników w zakresie korzystania z anonimowych przeglądarek, technologii sieci ZeroNet, konfigurowania ustawień witryn ISIL, aby uniemożliwić ich usunięcie z globalnej sieci Internet. Grupy terrorystyczne takie jak ISIL dokonują przemocy zarówno w rzeczywistym, jak i wirtualnym świecie. Badania przeprowadzone przez niezależną agendę bezpieczeństwa RAND (mającą siedzibę w UE i USA) wykazały, że zwolennicy ISIL wysłali ponad sześć milionów komunikatów – *tweetów,* od lipca 2014 r. do maja 2015 r. (Bodine-Baron, Helmus, Magnuson, Winkelman, 2015, s. 5-8). Internet umożliwiał im dokonywanie zakupu usług hakerskich *as-aService,* narzędzia typu *cyber weapons* za pomocą których dokonywano transmisji ogromnych ilości danych celem sparaliżowania sieci komputerowych bądź konkretnych komputerów (np.: poprzez zaprogramowane *zombie computers* lub złośliwe oprogramowanie – *sophisticated cyber malwa re*) (Enormous, 2017; Gilbert, 2014). Przykładem może być zidentyfikowane ~~oprogramowanie przeznaczone~~ do zaawansowanych zadań wywiadowczo-destrukcyjnych w cyberprzestrzeni Japonii, Południowej Korei był *Ice Fog*, który oferowano w kwocie 10 000$ (Blake, 2015, s. 5-6).

Cyberprzestrzeń zaczęła pełnić funkcję obszaru do przeprowadzania cyberprzestępczości: przejmowania funduszy, planowania zabójstw, rekrutacji oraz propagandy (Schori, 2015, s. 5-7). To oferowano w internetowych magazynach, takich jak: *Vice Jihad, Dbiq, Istok, Dar al. Islam, Fethi*, *Roumiay* (Seth, Libicki, 2008, s. 130-134; Gambhir, 2016, s. 21-33;Voice, 2017). Aplikacje sieciowe *dark Web* stanowiły narzędzie do planowania ataków, zakupu broni dla komórek grup terrorystycznych i „samotnych wilków" w Europie. O skali problemu w zakresie cyberprzestępczości świadczą ujawniane fakty. I tak, w 2015 r. po realizacji zakupu broni palnej przez Internet we Francji zostało aresztowanych 57 osób (Freeman, 2015). Obecnie identyfikacja cyberzagrożeń wymaga zespołowej pracy dobrze wykwalifikowanej kadry posługującej się nowymi technologiami w zakresie rozpoznania problemu w cyberprzestrzeni. Rozwiązywanie problemów jest utrudnione, choćby ze względu na fakt, że wielu przywódców al-Qaidy w obawie przed śledzeniem telefonów komórkowych, poczty elektronicznej i innych form komunikacji, uruchomia sieć kurierską prowadzoną przez członków rodzin *al-Qaidy* celem przekazywania instrukcji operacyjnych w formie płyt CD, wideo lub ulotek do sieci telewizyjnych, na przykład do *al Jazeera* (Musharraf, 2006, s. 2-5).

Jednocześnie należy dodać, że rozpoczął się wyścig produkcji nowych technologii cyfrowych połączonej z bronią laserową i wysokoenergetyczną, z przeznaczeniem do walki we wszystkich wymiarach (producenci: *Leonardo, Rheinmetall Defense, APC, Lockheed*

Martin) (Czulda, 2017, s. 20-21)[1]. Stanowią one potencjalne zagrożenie w sytuacji użycia jej przez nieuprawnione podmioty (np.: w czasie walki asymetrycznej). Tym bardziej pojawiają się obawy gdyby nowa technologia podobnie jak inne rodzaje najnowszej technologii była do dyspozycji podmiotów nieuprawnionych.

W obliczu ogromnych wyzwań, państwa oraz jednostki wyspecjalizowane, takie jak: ENISA, Narodowy System Cyber Awareness US-CERT, Europol opracowują różne formy wsparcia w zakresie zapewnienia bezpieczeństwa w cyberprzestrzeni. Obecnie prowadzone są liczne badania oraz wdrożenia dotyczące doskonalenia identyfikacji zagrożeń asymetrycznych w cyberprzestrzeni. Do tego celu włącza się maszyny samouczące się *machine deep learning* oraz sztuczną inteligencję *artificial intelligence* (Plmgr, 2017). Rządy państw, aby zapewnić stabilność w cyberprzestrzeni ponoszą olbrzymie wydatki na cyberbezpieczeństwo. Według raportów w latach od 2017 do 2021 r. globalne wydatki przeznaczone na zapewnienie bezpieczeństwa cybernetycznego określono na wartość ponad 1 biliona $ USD (Cybersecurity, 2017). W okresie 2007-2013 Unia Europejska zainwestowała 334 miliony euro w projekty dotyczące cyberbezpieczeństwa i prywatności online. W kolejnych latach 2014-2020 Unia Europejska ma przeznaczyć 450 mln EUR na badania dotyczące cyberbezpieczeństwa i innowacji w ramach kontraktowego partnerstwa publiczno-prywatnego Horyzont 2020 (EU, 2017). Z kolei Stany Zjednoczone na walkę z cyberprzestępczością przeznaczają roczne 17 milionów $ USD. Pomimo wysiłków globalne straty związane z cyberprzestępczością oszacowano na około 6 bilionów $ USA w każdym roku (szacunki dotyczą okresu od 2017 do 2021 r.). Pojawiają się dysproporcje między metodami i narzędziami jakie udaje się wypracować w UE i USA w ramach badań w zakresie zwalczania cyberprzestępczości a rozwojem przestępczych – *modeli biznesowych* typu *ransomware-as-a-service* (dzięki którym mogą skalować cyberprzestępczość na całym świecie (Cyber, 2017).

Wobec nasilających się cyberzagrożeń Komisja Europejska w 2017 r. zainicjowała program na rzecz wzmocnienia społeczeństwa obywatelskiego, w ramach którego 15 mln euro przeznaczone zostało na wzmocnienie skutecznych przesłań przeciwdziałających terroryzmowi w internecie, do których należy program „Prawo, równość i obywatelstwo", którego realizacja służy zapobieganiu nawoływania do nienawiści w Internecie (Report, 2017).

Zakończenie

Innowacje i zakłócenia stały się powszechnymi zagadnieniami dzisiejszego świata, które powinny być omawiane na wszystkich szczeblach państw w wymiarze lokalnym i globalnym. Dynamika zmian w środowisku międzynarodowym będąca konsekwencją

[1] Przykładem producentów nowej technologii cyfrowo-laserowej jest Leonardo, który od 2015 r. na włoskich helikopterach NH90 instaluje systemy laserowe LOAM zapobiegające kolizjom z niebezpiecznymi przeszkodami (są tak precyzyjne w działaniu, że identyfikują kable elektryczne). W 2017 r. Lockheed Martin US Navy ogłosił włączenie broni cyfrowo-laserowej 60kW – określanej jako SEASABER, z dalszą adaptacją jej do 150 kW (Czulda, 2017, s. 20-21).

procesów globalizacji powoduje, że bezpieczeństwo państw jest w coraz większym stopniu uzależnione od wielu nieprzewidywalnych sytuacji. Myślenie o bezpieczeństwie państwa jako procesie postrzeganym wielopłaszczyznowo stało się nowym paradygmatem i dotyczy również nauk politycznych i społecznych. Potencjał nowej płaszczyzny bezpieczeństwa państwa w cyberprzestrzeni generuje wiele wyzwań, dotyczy wielu zagrożeń obejmujących: jednostki, struktury państwowe, podmioty prywatne będące użytkownikami nowoczesnych technologii informatycznych. Przekłada się to z kolei na konieczność realizacji działań na rzecz zapewniania bezpieczeństwa użytkowników korzystających z nowych technologii, w tym sieci teleinformatycznych. Nasilające się zjawisko zagrożeń asymetrycznych w globalnej cyberprzestrzeni to kolejne wyzwania dla bezpieczeństwa i stabilności sytuacji gospodarczej (Szubrycht, 2006, s. 141). Według Tim Maurer z the Open Technology Institute and the New America Foundation, cyberbroń[2] stale i szybko się zmienia, co powoduje, że nie istnieje jedna zwycięska strategia przeciwko zagrożeniom cybernetycznym (Cyber, 2017). Stąd ranga tego typu zagrożeń znacząco wzrasta.

O skali problemu wypowiadają się przedstawiciele państw. Według prezydenta Barack Obamy walka z terroryzmem będzie trwać przez pokolenia (Obama, 2017). Zagrożenie asymetryczne są niebezpieczne, ponieważ cechuje je: nieprzewidywalność, szybki zwrot działań w nieznanym kierunku. Asymetria jest dziś narzędziem i siłą terrorystów, źródłem ich sukcesów. Wykorzystanie asymetrii pozytywnej oraz przeciwdziałanie asymetrii negatywnej powinno stanowić podstawę formułowania strategii każdego państwa i doktryny obronnej, a także plan każdego działania. Asymetria musi zacząć służyć nam, a nie terrorystom. Musimy ją odwrócić i nauczyć się tworzyć ją celowo oraz efektywnie wykorzystywać. To sprawa zasadnicza (Rutkowski, 2006, s. 17).

Rzeczywistość współczesnych konfliktów asymetrycznych, a zwłaszcza ich globalny zasięg i względna intensywność wskazują na zasadę, wedle której zagrożeniu asymetrycznemu nie mogą w sposób efektywny przeciwdziałać państwa, które będą działać unilateralnie.

Wyeliminowanie licznych źródeł i zagrożeń asymetrycznych w różnych wymiarach może dokonać się, dzięki współpracy wspólnot międzynarodowych, rządów, sektora prywatnego, społeczeństw obywatelskich, a także dzięki wdrażaniu, egzekwowaniu globalnych mechanizmów zwalczających sieci przestępcze (Financial 2015, s. 11). Przygotowanie państwa na zagrożenia typu cyber wojny i związane z nimi nowe wyzwania powinno uwzględniać: zwiększenie odporności cybernetycznej w skali globalnej, stosowanie prawa międzynarodowego do działań cybernetycznych, wspieranie środków budowy zaufania między państwami w kontekście dużej niepewności w kwestiach takich jak atrybucja (wyjaśnienie przyczyn) cyberataków (Cyber, 2017).

[2] Cyberbroń jest zmienną koncepcją w zależności od celu i kontekstu, w jakim może być użyta

BIBLIOGRAFIA

2016 Internet Crime Report, U.S. (2017). Department of Justice Federal Bureau of Investigation, Internet Crime Complaint Center, USA.

A new era: our elections now will be decided by hackers and leaked data. Pobrano 9 sierpnia 2017, https://www.theguardian.com/technology/2016/nov/16/wikileaks-elections-hackers-surveillance-technology.

Ballagas R., Borchers J., Sheridan J. (2006). *The Smart Phone: A Ubiquitous Input Device*, IEEE Pervasive Computing, Vol. 5, No. 1.

Blake M. (2015). *U.K. Ramps up Cyber Plans amid Post-Paris Attack Panic*, Washington Times.

Blank S. (2003). *Rethinking asymmetric threats*, Strategic Studies Institute, USA.

Bodine-Baron E., Helmus T., Magnuson M., Winkelman Z. (2015). *Examining ISIS Support and Opposition Networks on Twitter*', RAND U.S. Department, USA,

Cai Yu, Onur M., Ken M. (2012). *Error Patterns in MLC NAND Flash Memory: Measurement Characterization, and Analysis*, In DATE, Carnegie Mellon University, USA.

Carte D. (2001).*Asymmetric Warfare and the Use of Special Operation Forces in North American Law Enforcement*, Canadian Military Journal, t. 2, nr 4.

Castells M., *Społeczeństwo sieciowe*, PWN, Warszawa 2010.

Cloud Security: Don't Throw Caution to the Wind, Mark Wood, Dell Secure Works and JD Sherry, Global Director, Technology and Solutions, Trend Micro. Pobrano 9 września 2017 z: https://www.brighttalk.com/webcast/9463/72123?utm_medium=web&utm_source=brighttalk-portal&utm_campaign=player-page-feed.

Cyber Crime Study 2017 Insights on the Security Investments that make a difference. (2017). Pobrano 9 września 2017 z: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Cybersecurity market report. (2017). Pobrano 8 stycznia 2018 z: https://cybersecurityventures.com/cybersecurity-market-report/

Czulda R. (2017). *Welcome to Hel, Development of High-energy Laser Weapons*, Military technology, Vol.XLI. Issue7-8, Germany.

Dark Web and Cybercrime. Pobrano 9 września 2017 z: https://www.deepdotweb.com.

Ducaru S. D. (2016). *The cyber dimension of modern hybrid warfare and its relevance for NATO*, Continuity and Change in European Governance, Europolity, vol. 10, no. 1, Belgium.

ENISA Threat Landscape 2016, European Union Agency For Network And Information Security. Pobrano 19 września 2017 z: https://www.enisa.europa.eu/+&cd=8&hl=pl&ct=clnk&gl=pl&client=opera.

Enormous Malware as a Service Infrastructure Fuels Ransomware Epidemic. Pobrano 12 września 2017 z: http://www.infosecurity-magazine.com/news/enormous-malware-as-a-service.

EU cybersecurity initiatives working towards a more secure online environment. (2017). Pobrane 07 listopada 2017, z: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

European Union Serious and Organised Crime Threat Assessment 2017, Report Organised Crime (SOCTA/OCTA). Pobrano 9 listopada 2017 z: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

Financial Action Task Force Report, *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISI)*, Financial Action Task Force Report, Paris 2015. Pobrane 07 listopada 2017, z: http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf.

Freeman C. (2015) *Inside the 'Ant Trade' – How Europe's Terrorists Get Their Guns*, The Telegraph. Pobrano 9 września 2017 z: http://www.telegraph.co.uk/news/worldnews/europe/12010458/Inside-the-Ant-Trade-how-Europes-terrorists-get-their-guns.html.

Gambhir H. (2016). *The Virtual Caliphate: ISIS's Information Warfare*, ISW, Waszyngton, USA.

Gilbert D. (2014). *Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog*, IBTimes. Pobrano 9 września 2017 z: http://www.ibtimes.co.uk/cost-developing-cyber-weapons-drops-100m-stuxnet-10k-icefrog-1435451.

Global Terrorism Index 2016. (2016). Institute for Economics& Peace, USA.

Hoffman B., Meese E., Roemer T. J. (2015). *Report of the Congressionally-directed, 9/11 Review Commission To The Director of the FBI*, Commissioners. Pobrane 17 listopada 2017, z: https://www.fbi.gov/file-repository/stats-services-publications-protecting-the-homeland-in-the-21st-century.

Jiang W., Khera G., Wood R. (2003). *Cross-Track Noise Profile Measurement for Adjacent-Track Interference Study and Write-Current Optimization in Perpendicular Recording,* Journal of Applied Physics, 93(10).

Madej M. (2005). Terroryzm i inne zagrożenia asymetryczne w świetle współczesnego pojmowania bezpieczeństwa narodowego i międzynarodowego – próba teoretycznej konceptualizacji, [w:] R. Kuźniar (red.), *Porządek międzynarodowy u progu XXI wieku* (s. 486-518), Wydawnictwo Uniwersytetu Warszawskiego, Warszawa.

Musharraf P. (2006). *In the Line of Fire: A Memoir*, New York: Free Press, USA.

NATO Summit Guide, Warsaw, 8-9 July. (2016), NATO Communications and Information Agency. Pobrano 16 listopada 2017 z: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607--Warsaw-Summit-Guide_2016_ENG.pdf

Obama: walka z terroryzmem potrwa pokolenia, ale nie zagraża on USA. (2016) Pobrano 9 września 2017 z: https://pl.sputniknews.com/swiat/201612074373111-obama-przemowienie-terroryzm-guantanamo-tortury.

Opracowane na podstawie danych FBI, IC3 i Departamentu Sprawiedliwości USA. Pobrano 9 września 2017 z: https://www.statista.com/statistics/267132/total-damage--caused-by-by-cyber-crime-in-the-us/.

Piątkowski K. (2002).Wojna nowego typu? „Polska w Europie", nr 1.

Plmgr, Pobrano 9 września 2017 z: https://www.jpmorgan.com/global/cib/research/investment-decisions-using-machine-learning-ai?source=car_di_cr_div090817.

Ransomware As A Service Being Offered For $39 On The Dark Net. Pobrano 2 września 2017 z: http://www.forbes.com/sites/kevinmurnane/2016/07/15/ransomware-as-a-ser, vice-being-offered-for-39-on-the-dark-net/#43fa4f0c302d.

Remote File Inclusion. Pobrano 7 września 2017 z: http://projects.webappsec.org/w/page/13246955/Remote%20File%20Inclusion.

Report from the Commission to the European Parliament, the European Council and the Council. (2017). COM(2017) 203 final.

Rutkowski C. (2006). Terroryzm – patologia społeczna XXI wieku. Nowe wyzwania dla międzynarodowego bezpieczeństwa, [w:] J. Gotowała (red.) *Terroryzm – rola sił zbrojnych w zwalczaniu zjawiska* (s. 17), AON, Warszawa.

Saadawi T., Colwell J., Jr Editors. (2017). *Cyber infrastructure protection,* Army War College, Strategic Studies Institute, Vol. III, USA.

Sarga L., Roman J. (2013). *Mobile Cyberwarfare Threats and Mitigations: An Overview*, 12th European Conference on Cyber Warfare and Security (ECCWS-2013), Jyväskylä, Finland.

Schori L. C. (2015). *Cyber-Jihad: Understanding and Countering Islamic State Propagand*', GCSP Policy Paper 2015/2.

Seth G. J., Libicki M. C. (2008). *How Terrorist Groups End, Lessons for Countering al Qa'ida*, RAND, Santa Monica, California. Pobrane 17 listopada 2017, z: https://www.rand.org/pubs/monographs/MG741-1.html.

Steele R. (2002). *New craft of the intelligence: achieving asymmetric advantage in the face of nontraditional threats*, US Army War College, Carlisle.

Szubrycht T. (2006). *Analiza podobieństw operacji militarnych innych niż wojna oraz działań pozwalających zminimalizowana zagrożenia asymetryczne*, „Zeszyty Naukowe Akademii Marynarki Wojennej" nr 1 (164).

The real hacker threat to election day? Data deception and denial. Pobrano 4 września 2017 z: https://www.wired.com/2016/11/real-hacker-threat-election-day-data-deception-denial/.

The use of the Internet for terrorist purposes. (2012). United Nations, New York,

Ukrainian Activists Leak Personal Information of Thousands of War Reporters in the Donbas. Pobrano 9 września 2017 z: https://advox.globalvoices.org/2016/05/11/ukrainian-activists-leak-personal-information-of-thousands-of-war-reporters-in-the-donbas/.

Urbanek A. (2016). *Cyberwojna – zagrożenie asymetryczne współczesnej przestrzeni bezpieczeństwa,* Akademia Pomorska, Słupsk.

Urbanek A. (2016). *Zagrożenia asymetryczne czy asymetryczność zagrożeń,* [w:] *Wyzwania i zagrożenia w XXI wieku. Aspekty militarne i niemilitarne*, (red.) Borkowski M., Stańczyk-Minkiewicz M., Ziemkiewicz-Gawlik I., Poznań 2013. Studia nad bezpieczeństwem, nr 1, s. 5-32.

Yoongu K., Jeremie K., Hye L. Ji, Donghyuk L., Onur M. (2014). *Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors,* ACM/IEEE 41st International Symposium on Computer Architecture (ISCA), Minneapolis, USA.