Miron Lakomy

ZAGROŻENIA DLA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO PAŃSTW – PRZYCZYNEK DO TYPOLOGII

Słowa kluczowe:
bezpieczeństwo teleinformatyczne, cyberzagrożenia, zagrożenia dla bezpieczeństwa teleinformatycznego, bezpieczeństwo państwa

Wprowadzenie

Digitalizacja niemal wszystkich dziedzin życia ludzkiego w ciągu ostatnich trzech dekad ma nie wątpliwie doniosłe konsekwencje dla bezpieczeństwa narodowego i międzynarodowego. Coraz powszechniejsze zastosowanie komputerów, sieci oraz szeroko pojętych technologii teleinformatycznych, tak w sferze publicznej, jak i prywatnej, wiąże się bowiem nie tylko z korzyściami, ale także z rosnącą wrażliwością na ich szkodliwe wykorzystanie. Od lat 80. XX wieku cyberprzestrzeń[1] stopniowo staje się w coraz większym stopniu obszarem działań stanowiących zagrożenie dla bezpieczeństwa państw, ciesząc się tym samym rosnącym zainteresowaniem środowiska naukowego. Świadczyły o tym w szczególności wydarzenia z drugiej połowy pierwszej dekady XXI wieku, kiedy to doszło do szeregu poważnych incydentów teleinformatycznych. Należy tu wskazać przede wszystkim na *casus* Estonii z kwietnia 2007 roku, kiedy po raz pierwszy

[1] W literaturze specjalistycznej funkcjonuje wiele definicji cyberprzestrzeni. Według Pierre'a Delvy jest to *przestrzeń otwartego komunikowania za pośrednictwem połączonych komputerów i pamięci informatycznych, pracujących na całym świecie*. Natomiast według amerykańskiego Departamentu Obrony jest to *globalna domena w środowisku informacyjnym, składająca się ze współzależnych sieci infrastruktur teleinformatycznych, w tym Internetu, sieci telekomunikacyjnych, systemów komputerowych oraz wbudowanych procesorów i kontrolerów*. W tym kontekście przedmiotem zainteresowania bezpieczeństwa teleinformacyjnego są wszelkie działania, które mogą zakłócić właściwe funkcjonowanie cyberprzestrzeni, w tym jej elementów o fundamentalnym znaczeniu dla funkcjonowania państw, np. teleinformatycznej infrastruktury krytycznej czy sieci wojskowych. Zob. *DoD Dictionary of Military Terms*, Joint Staff, Joint Doctrine Division, J-7, Washington D.C., 17.10.2008; M. Lakomy, *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*, „Stosunki Międzynarodowe – International Relations", 2010, nr 3-4, s. 56.

w historii ataki w cyberprzestrzeni doprowadziły na tak dużą skalę do zablokowania stron internetowych należących do instytucji rządowych, mediów, banków czy największych przedsiębiorstw komunikacyjnych i transportowych. W konsekwencji wiązały się one nie tylko z pewnymi stratami ekonomicznymi i wizerunkowymi, ale przede wszystkim dowiodły, jak poważne reperkusje mogą mieć zaniedbania na obszarze cyberbezpieczeństwa państwa[2]. Tym samym potwierdziły się opinie formułowane jeszcze w latach 80. i 90., iż przestrzeń teleinformatyczna może zostać skutecznie wykorzystana jako narzędzie rywalizacji w środowisku międzynarodowym. Niedługo później, we wrześniu 2007 roku, doszło do kolejnego wydarzenia potwierdzającego te tendencje. 6 września siły zbroje Izraela przeprowadziły naloty na syryjski ośrodek wojskowy, w którym prowadzono prace nad rozwojem technologii nuklearnych. Ciekawostką był fakt, iż system obrony przeciwlotniczej Syrii nie był w stanie wykryć nadlatujących samolotów IDF[3], bowiem został wcześniej zainfekowany wirusem komputerowym. W niespełna rok później, w sierpniu 2008 roku, w trakcie rosyjsko-gruzińskiego konfliktu zbrojnego o Osetię Południową, ponownie doszło do masowych ataków teleinformatycznych. W ich wyniku zablokowano strony internetowe gruzińskich instytucji państwowych, naukowych oraz największych przedsiębiorstw komercyjnych[4]. W 2010 roku świat obiegła informacja o zainfekowaniu komputerów kontrolujących prace irańskich elektrowni atomowych wirusem *Stuxnet*, który prawdopodobnie został stworzony przez wywiady Izraela i Stanów Zjednoczonych. W tym samym czasie pojawiły się także informacje o niezwykle zaawansowanych operacjach cyberszpiegowskich, prowadzonych przede

[2] W.C. Ashmore, *Impact of Alleged Russian CyberAttacks*, „Baltic Security &Defense Review", vol. 11, 2009; E. Lichocki, *Cyberterrorystyczne zagrożenie dla bezpieczeństwa teleinformatycznego państwa polskiego*, Warszawa 2008, s. 179; E. Lichocki, *Cyberterroryzm jako nowa forma zagrożeń dla bezpieczeństwa*, [w:] K. Liedel (red.), *Transsektorowe obszary bezpieczeństwa narodowego*, Warszawa 2011, s. 63.

[3] *Israeli Defense Forces*.

[4] Szerzej: D. Hollis, *Cyberwar Case Study: Georgia 2008*, „Small Wars Journal", 06.01.2011; F.S. Gady, G. Austin, *Russia, The United States, and Cyber Diplomacy. Opening the Doors*, EastWestInstitute, New York 2010, s. 17; M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm*, [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009, s. 108-109; M. Lakomy, *Cyberwojna jako rzeczywistość XXI wieku*, „Stosunki Międzynarodowe – International Relations", 2011, nr 3-4, s. 147.

wszystkim z terytorium Chin[5]. Wszystkie te wydarzenia stanowiły więc potwierdzenie opinii, wskazujących na zasadniczy wzrost teleinformatycznych zagrożeń dla bezpieczeństwa państw[6].

Problemy terminologiczne

Przytoczone powyżej przykłady stanowiły na przełomie pierwszej i drugiej dekady XXI wieku jedynie niewielki promil wszystkich poważnych incydentów komputerowych w tym okresie. Należy mieć bowiem na uwadze, iż szkodliwa działalność w cyberprzestrzeni charakteryzuje się niezwykłym bogactwem nie tylko form i technik, ale także szeroko rozumianą wieloaspektowością i wielopłaszczyznowością[7]. Technologie teleinformatyczne są bowiem współcześnie wykorzystywane na masową skalę, do rozmaitych celów, przez podmioty o różnym stopniu zorganizowania, odmiennych motywacjach i statusie prawno-politycznym. Sytuację dodatkowo komplikuje specyfika funkcjonowania cyberprzestrzeni, wiążąca się m.in. z brakiem tradycyjnych granic czy łatwą do osiągnięcia anonimowością. W tym kontekście rzeczą niezwykle istotną jest więc odpowiednia identyfikacja, a co za tym idzie, również zdefiniowanie najpoważniejszych zagrożeń dla bezpieczeństwa teleinformatycznego państw. Jest to jednak zadanie niezwykle trudne. Jak bowiem słusznie zauważyli Marek Madej i Marcin Terlikowski, *w kontekście każdego z tych wydarzeń mówiono o bezpieczeństwie teleinformatycznym (informatycznym), posługując się jednak czasem odmiennymi terminami. Również w stosunku do ich sprawców stosowano, zamiennie i niekonsekwentnie, różnorodne, a ponadto z reguły*

[5] Warto tu wspomnieć o odkrytej przez kanadyjskich naukowców, z Ronem Diebertem na czele, chińskiej siatce *GhostNet* lub operacji *Shady Rat*, której celem stało się ponad 70 państw, koncernów oraz organizacji pozarządowych. Zob. *Tracking GhostNet. Investigating a Cyber Espionage Network*, „Information Warfare Monitor", 29.03.2009; D. Alperovitch, *Revealed: Operation Shady Rat*, „McAfee White Paper", ver. 1.1.

[6] Zagrożenia dla bezpieczeństwa można zdefiniować jako *taki splot zdarzeń wewnętrznych lub w stosunkach międzynarodowych, w których z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do nie zakłócanego bytu i rozwoju wewnętrznego bądź naruszenie lub utrata suwerenności państwa oraz jego partnerskiego traktowania w stosunkach międzynarodowych – w wyniku zastosowania przemocy politycznej, psychologicznej, ekonomicznej, militarnej itp.*. Za E. Nowak, M. Nowak*, Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011, s. 40-44.

[7] Trzeba mieć bowiem na uwadze, iż na analizę tego zagadnienia składają się aspekty właściwe tak naukom ścisłym i technicznym (informatyka, elektronika, telekomunikacja), jak i społecznym (nauki polityczne, nauki o bezpieczeństwie, nauki o obronności, nauki prawne).

nieprecyzyjne określenia. Podejmowano także próby klasyfikowania tych zdarzeń, umieszczenia ich na mapie zagrożeń związanych z wykorzystaniem technologii teleinformatycznych. Wysiłki te dawały jednak zazwyczaj obraz nadmiernie uproszczony, uwypuklający jedynie wybrane aspekty poruszanych problemów, a całkowicie pomijający inne[8]. Z jednej strony należy zwrócić uwagę na fakt, iż media masowe, które od kilku lat coraz więcej miejsca poświęcają tej problematyce, częstokroć niepotrzebnie upraszczają zjawiska i procesy właściwe dla cyberprzestrzeni, stosując nieraz przy tym błędną lub niejasną terminologię. Szczególnie nadużywanym terminem wydaje się być „cyberterroryzm", który jest z reguły wykorzystywany do charakterystyki zarówno zwykłych aktów o charakterze kryminalnym, jak i incydentów mających wymiar międzypaństwowy[9]. Z drugiej strony nie ma jednak zgody samego środowiska akademickiego co do jednoznacznego zdefiniowania najpoważniejszych zagrożeń teleinformatycznych. W literaturze rodzimej oraz zagranicznej w ostatnich kilkunastu latach pojawiło się wiele typologii, klasyfikacji i definicji wyzwań na tym obszarze, które często wzajemnie się wykluczały lub skupiały na odmiennego rodzaju zagadnieniach. Najlepiej świadczyła o tym znaczna swoboda terminologiczna w określaniu tego stosunkowo nowego wymiaru bezpieczeństwa z punktu widzenia kryterium przedmiotowego[10]. Określa się go bowiem m.in. jako bezpieczeństwo teleinformatyczne, informacyjne, cybernetyczne, cyberprzestrzenne, komputerowe, informatyczne czy cyberbezpieczeństwo[11]. Trwa

[8] M. Madej, M. Terlikowski, *Wprowadzenie*, [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009, s. 9.

[9] M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm*, [w:] M. Madej, M. Terlikowski (red.), dz. cyt, .s. 120.

[10] Zob. B. Balcerowicz, *Procesy międzynarodowe. Tendencje i megatrendy*, [w:] R. Kuźniar, B. Balcerowicz, A. Bieńczyk-Missala, P. Grzebyk, M. Madej, K. Pronińska, M. Sułek, M. Tabor, A. Wojciuk, *Bezpieczeńswo międzynarodowe*, Warszawa 2012, s. 66-70.

[11] Rozmaici uznani autorzy w odmienny sposób definiują ten obszar badań. Zob. np. M.C. Libicki, *Conquest in Cyberspace*, Cambridge 2007; P. Hess (red.), *Cyberterrorism and information war*, New Delhi 2001; A. Bendiek, *European Cyber Security Policy*, "SWP Research Paper", October 2012; J.Carr, *Inside CyberWarfare*, Sebastopol 2010; J.V. Blane (red.), *Cyberwarfare: Terror at a click*, Huntington 2001; K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012; K. Liedel, *Bezpieczeństwo informacyjne państwa*, [w:] K. Liedel (red.), *Transsektorowe obszary bezpieczeństwa narodowego*, Warszawa 2011; M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009; M. Lakomy, *Cyberzagrożenia na początku XXI wieku*, „Przegląd Zachodni", 2012, nr 4; S. Moćkun, *Terroryzm cybernetyczny – zagrożenia dla bezpieczeństwa narodowego i działania amerykańskiej administracji*, „Raport Biura Bezpieczeństwa Narodowego", lipiec 2009.

również dyskusja co do zasadności niektórych, coraz powszechniej stosowanych określeń (np. cyberwojny), zwracających uwagę na kontekst międzypaństwowy działań w sieci[12]. Co więcej, każda z dyscyplin naukowych zajmujących się tą problematyką stosuje częstokroć własny, unikalny aparat pojęciowy, zwracając tym samym uwagę głównie na właściwe danemu obszarowi wiedzy aspekty[13]. Takie rozwiązanie może jednak prowadzić do zawężenia pola rozważań naukowych, a w konsekwencji do jednowymiarowego postrzegania zagadnień interdyscyplinarnych.

Warto więc podjąć próbę opracowania typologii uwzględniającej, choćby w sposób bardzo uproszczony, najpoważniejsze zagrożenia teleinformatyczne z perspektywy politycznych i prawnych aspektów bezpieczeństwa państw[14]. Wydaje się, iż jest to niezbędne z trzech powodów. Przede wszystkim precyzyjne zdefiniowanie tych niezwykle skomplikowanych, wielowymiarowych zjawisk jest rzeczą niezwykle istotną dla samego procesu ich naukowego badania. Dzięki niemu można bowiem uniknąć błędów wynikających między innymi z wieloznaczności stosowanych terminów. Po drugie, kwestia ta odgrywa zasadniczą rolę z punktu

[12] R.A. Clarke, R. Knake, *Cyberwar: The Next Threat to National Security and What to Do About It*, Ecco, 2010; T. Rid, *Cyber War Will Not Take Place*, „Journal of Strategic Studies", 2012, nr 1; A. Bautzmann, *Le cyberespace, nouveau champ de bataille?*, „Diplomatie. Affaires Stratégiques et Relations Internationales", luty-marzec 2012; A. Bufalini, *Les cyber-guerres a la lumière des regles internationales sur l'interdiction du recours à la force*, [w:] M. Arcari, L. Balmond (red.), *La gouvernance globale face aux défis de la sécurité collective*, Napoli 2012; T. Shimeall, *Countering cyber war*, „NATO Review", 2001, nr4, vol. 49, s. 16-18; *War in the fifth domain*, „The Economist", 01.07.2010; P. Sienkiewicz, *Wizje I modele wojny informacyjnej*, [w:] L.H. Haber (red.), *Społeczeństwo informacyjne – wizja czy rzeczywistość?*, Kraków 2003; P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*, [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009; K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe", 2011, nr 1; M. Lakomy, *Cyberwojna jako rzeczywistość XXI wieku*, [w:] „Stosunki Międzynarodowe – International Relations", 2011, nr 3-4.

[13] Świetnym przykładem tych tendencji są różnice w postrzeganiu wyzwań dla bezpieczeństwa teleinformatycznego przez nauki techniczne i nauki społeczne. Zob. K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 60-65.

[14] Za Ryszardem Ziębą można przyjąć, iż na bezpieczeństwo państwa (narodowe) składają się cztery rodzaje wartości: przetrwanie, integralność terytorialna, niezależność polityczna oraz jakość życia. Jednocześnie warto mieć na uwadze, iż w ostatnich dekadach zakres problemowy bezpieczeństwa narodowego został znacząco poszerzony. Bezpieczeństwo międzynarodowe można natomiast uznać za *brak zagrożeń dla norm, reguł i instytucji, które służą zapewnianiu bezpieczeństwa państw i pozostałych uczestników stosunków międzynarodowych*. Za. R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego*, Warszawa 1999, s. 41-42; R. Kuźniar, *Wstęp*, [w:] R. Kuźniar, B. Balcerowicz, A. Bieńczyk-Missala, P. Grzebyk, M. Madej, K. Pronińska, M. Sułek, M. Tabor, A. Wojciuk, *Bezpieczeństwo międzynarodowe*, Warszawa 2012, s. 15. E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011.

widzenia wypracowania skutecznych rozwiązań systemowych, obejmujących przygotowanie odpowiednich mechanizmów politycznych, aktów prawnych czy adekwatnych modeli współpracy poszczególnych instytucji rządowych i pozarządowych. Warto tu przytoczyć słowa Krzysztofa Silickiego, zdaniem którego: *do zaplanowania kształtu kultury bezpieczeństwa teleinformatycznego konieczne wydaje się opracowanie mapy drogowej, tzn. etapowego dojścia do założonego poziomu bezpieczeństwa. W tym celu należałoby najpierw dokonać opisu aktualnej sytuacji, tj. zidentyfikować i zebrać najważniejsze przeszkody hamujące postęp w bezpieczeństwie teleinformatycznym oraz ograniczenia i problemy wskazywane przez poszczególnych uczestników komunikacji elektronicznej*[15].

Jeszcze istotniejszy wydaje się trzeci powód. Zagrożenia teleinformatyczne, jak już wskazano wyżej, nie są właściwe jedynie poszczególnym państwom. Choćby ze względu na model funkcjonowania sieci mają one charakter transnarodowy, globalny[16]. Tym samym skuteczne im przeciwdziałanie nie zależy wyłącznie od rozwiązań na poziomie jednostkowym, lokalnym czy państwowym, lecz także od skutecznych mechanizmów współpracy w wymiarze międzynarodowym. Brak jednolitego aparatu pojęciowego wydaje się być jednym z czynników, które w zasadniczym stopniu utrudniają wypracowanie wspólnych mechanizmów walki z zagrożeniami teleinformatycznymi w środowisku międzynarodowym. Trzeba mieć bowiem na uwadze, iż optyka poszczególnych wyzwań uwarunkowana jest często określonymi interesami narodowymi. Stało się to szczególnie widoczne w trakcie wieloletniej debaty poświęconej tym zagadnieniom w ramach Organizacji Narodów Zjednoczonych czy Rady Europy. Ze względu na zasadnicze różnice pomiędzy Stanami Zjednoczonymi, Federacją Rosyjską oraz Chińską Republiką Ludową, wypracowanie spójnych rozwiązań nawet w stosunkowo prostych kwestiach okazało się dotychczas niezwykle trudne. Przykładem tych tendencji może być diametralnie odmienne stanowisko tych państw wobec ratyfikacji Konwencji Rady Europy

[15] K. Silicki, *Unia Europejska a bezpieczeństwo teleinformatyczne – inicjatywy i wyzwania*, [w:] M. Madej, M. Terlikowski (red.), dz. cyt., s. 203.
[16] Zob. K. Liedel, *Bezpieczeństwo informacyjne państwa*, [w:] K. Liedel (red.), *Transsektorowe obszary bezpieczeństwa narodowego*, Warszawa 2011, s. 45-62.

o Cyberprzestępczości z 2001 roku, globalnego traktatu poświęconego szkodliwemu wykorzystaniu cyberprzestrzeni, czy aktualizacji Międzynarodowych Regulacji Telekomunikacyjnych ITU[17]. W tej patowej sytuacji każde z państw, organizacji międzynarodowych czy nawet transnarodowych korporacji wypracowało własne *modus operandi* w zakresie bezpieczeństwa teleinformatycznego. Stosowana nomenklatura, typologia oraz definicje cyberzagrożeń w dużym stopniu wpływają na optykę tych zagadnień, a więc pośrednio także na procesy formułowania strategii i regulacji w tej dziedzinie, tak w wymiarze wewnętrznym, jaki międzynarodowym.

Typologie zagrożeń teleinformatycznych

W tym kontekście warto więc podjąć próbę opracowania podstawowej typologii najpoważniejszych zagrożeń teleinformatycznych z perspektywy politologicznej. Mając na uwadze wieloaspektowy i wielopłaszczyznowy charakter szkodliwej działalności w cyberprzestrzeni, jako podstawowe kryterium podziału należy wskazać odmienne motywacje i skonkretyzowane cele, które sprawiają, że podobne techniki cyberataków, z punktu widzenia nauk politycznych, mają jakościowo odmienny charakter. Przez motywacje można rozumieć *względnie trwałą tendencję (dążenie) do podejmowania czynności ukierunkowanych na określony cel*[18]. Mogą one mieć więc, np. charakter indywidualny, polityczny, ekonomiczny, społeczny, ideologiczny. Ponadto należy wziąć pod uwagę jeszcze kilka innych czynników:

- źródła zagrożeń, co jest sprawą fundamentalną dla oceny prawno-politycznych reperkusji incydentów teleinformatycznych,

[17] F.S. Gady, G. Austin, *Russia, The United States, and Cyber Diplomacy. Opening the Doors*, EastWest Institute, New York 2010; T. Maurer, *Cyber Norm Emergence at the United Nations – an Analysis of the Activities at the UN Regarding Cyber-Security*, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011; C. Arthur, *Internet remains unregulated after UN treaty blocked*, The Guardian, 14.12.2012, http://www.guardian.co.uk/technology/2012/dec/14/telecoms-treaty-internet-unregulated, 12.01.2012;
B. Harley, *A Global Convention on Cybercrime?*, „The Columbia Science and Technology Law Review", 23.03.2010, http://www.stlr.org/2010/03/a-global-convention-on-cybercrime, 09.01.2013; *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, United Nations General Assembly A/66/359, 14.09.2011.

[18] *Motywacja*, Encyklopedia PWN, http://encyklopedia.pwn.pl/haslo.php?id=3943894, 17.06.2013.

- stopień ich zorganizowania,
- stosowane techniki i narzędzia,
- oraz reperkusje dla bezpieczeństwa narodowego i międzynarodowego.

Uwzględnienie tych kryteriów wydaje się być istotne, gdyż cyberataki mogą wiązać się ze zgoła różnymi konsekwencjami m.in. w kontekście bieżących procesów politycznych w kraju, współpracy i sporów międzynarodowych bądź interpretacji prawa międzynarodowego publicznego. Jednocześnie nie można się zgodzić z pojawiającymi się czasami sugestiami, iż wszystkie incydenty teleinformatyczne mają podobny charakter, a co za tym idzie, należy je postrzegać w jednakowy sposób z punktu widzenia bezpieczeństwa narodowego i międzynarodowego[19]. Należy bowiem zauważyć, iż istnieje wiele form szkodliwej działalności w cyberprzestrzeni, posiadających diametralnie odmienne cechy, a co za tym idzie, mających odmienne skutki z perspektywy funkcjonowania państwa. Przykładowo, zupełnie inne były motywacje, cele, techniki oraz konsekwencje wykorzystane w trakcie ataków na Estonię w 2007 r., a czymś zupełnie innym była działalność chińskiej siatki szpiegowskiej *GhostNet*. Odmienny charakter, z punktu widzenia działalności służb państwowych czy prawa międzynarodowego, ma cyberprzestępczość, a czymś innym jest zjawisko cyberterroryzmu[20].

W oficjalnych dokumentach państwowych oraz literaturze specjalistycznej najczęściej wyróżnia się następujące zagrożenia teleinformatyczne: cyberprzestępczość, cyberterroryzm, haktywizm, haking[21], cyberszpiegostwo oraz wykorzystanie cyberprzestrzeni do działań zbrojnych (*cyberwarfare*)[22].Ten ostatni

[19] Z perspektywy nauk technicznych i ścisłych rzeczywiście narzędzia i techniki włamań komputerowych wydają się być najistotniejsze. Jednak w analizie politologicznej powinno być wzięte pod uwagę zdecydowanie szersze spektrum kryteriów mających konsekwencje polityczne lub prawne.

[20] M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm*, [w:] M. Madej, M. Terlikowski (red.), dz. cyt., s. 120.

[21] Pisali o nich m.in.: E. Lichocki, *Cyberterrorystyczne zagrożenie dla bezpieczeństwa teleinformatycznego państwa polskiego*, Warszawa 2008; K. Liedel (red.), *Transsektorowe obszary bezpieczeństwa narodowego*, Warszawa 2011; T. Jemioło, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Warszawa 2009; T. Jordan, *Hakerstwo*, Warszawa 2011; Y.-M. Peyry, *Menaces Cýbérnetiques : Le manuel du combattant*, Paris 2013.

[22]Zob. M. Arpagian, *La Cyberguerre*, Paris 2009; A. Bufalini, *Les cyber-guerres a la lumiere des regles internationales sur l'interdiction du recours a la force*, [w :] M. Arcari, L. Balmond (red.), *La gouvernance globale face aux defis de la securité collective*, Napoli 2012; P. Hess (red.), *Cyberterrorism and information war*, New

punkt często, choć nie do końca trafnie, bywa utożsamiany z pojęciem cyberwojny (*cyberwar*), określanej też mianem wojny informacyjnej czy wojny cybernetycznej[23].

W tym kontekście, aby osiągnąć wskazany wyżej cel, rozważania należałoby rozpocząć od odpowiedzi na pytanie, jakie podmioty w rzeczywistości działają w cyberprzestrzeni? Warto w tym miejscu odwołać się do zaproponowanego przez Piotra Sienkiewicza i Halinę Świebodę podziału na zagrożenia ustrukturalizowane i nieustrukturalizowane. Do tych pierwszych zaliczyli oni: państwa (ich agendy i wyspecjalizowane jednostki), terrorystów oraz jednostki transnarodowe (np. międzynarodowe grupy przestępcze). Do tej drugiej natomiast: przestępców, hakerów, krakerów, wandali i frustratów. Słusznie przy tym uznali, iż zdecydowanie inne konsekwencje będzie miał atak przeprowadzony przez pojedynczego przestępcę komputerowego, a zupełnie inne włamanie przygotowane przez obce państwo[24]. Zaproponowany podział wydaje się być przydatny do analizy prawno-politycznych konsekwencji cyberataków. Opierając się na tych rozważaniach, można by jednak dokonać pewnej modyfikacji tej typologii, tak aby pełniej oddawała charakter wyzwań teleinformatycznych. Do źródeł zagrożeń o charakterze systemowym (ustrukturalizowanym) można by więc zaliczyć:

- państwa i ich grupy[25],
- oraz wysoce zorganizowane podmioty pozapaństwowe (organizacje terrorystyczne).

Nie jest wykluczone, iż w przyszłości, do tej grupy należałoby zaliczyć także transnarodowe korporacje, które w wielu przypadkach już obecnie dysponują

Delhi 2001; T. Rid, *Cyber War Will Not Take Place*, London 2013; M.C. Libicki, *Cyberdeterrence and Cyberwar, Cambridge 2009.*

[23] Należy mieć jednak na uwadze, iż terminy te są wykorzystywane bardzo szeroko i niekoniecznie muszą się wiązać jedynie z wykorzystaniem cyberprzestrzeni do działań zbrojnych. Zob. np. K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe", 2011, nr 1; M. Lakomy, *Cyberwojna jako rzeczywistość XXI wieku*, „Stosunki Międzynarodowe – International Relations", 2011, nr 3-4.

[24] P. Sienkiewicz, H. Świeboda, *Analiza systemowa zjawiska cyberterroryzmu*, „Zeszyty Naukowe AON", 2006, nr 2, t. 63, s. 10.

[25] Nie ulega bowiem wątpliwości, iż cyberprzestrzeń staje się stopniowo wymiarem nie tylko rywalizacji, ale także współpracy poszczególnych państw, o czym świadczy m.in. kooperacja amerykańsko-izraelska w tej dziedzinie. Zob. *United States-Israel Enhanced Security Cooperation Act of 2012*, House of Representatives, United States 2012.

porównywalnym z niektórymi państwami potencjałem eksperckim i technologicznym w cyberprzestrzeni. Jest on jednak wykorzystywany głównie do ochrony poufnych danych i technologii przed aktami szpiegostwa komputerowego, np. pochodzenia chińskiego[26].

Warto również zaproponować nieco inną klasyfikację niesystemowych (nieustrukturalizowanych) źródeł zagrożeń teleinformatycznych. Można do nich zaliczyć:

- hakerów,
- haktywistów,
- „cyberwojowników"[27],
- przestępców,
- pozostałych, czyli posiadających różną motywację amatorów (np. *scripts kiddies*).

Na tej podstawie warto jednak zbudować szerszą typologię podstawowych form zagrożeń teleinformatycznych, która uwzględniłaby, z jednej strony, przytoczoną wyżej klasyfikację, z drugiej natomiast różnorodność motywacji i celów, stosowanych narzędzi i technik ataków oraz ich konsekwencji dla bezpieczeństwa państw. Innymi słowy, miałaby na uwadze wielopłaszczyznowy i wieloaspektowy charakter tych wyzwań, dostrzegając ich odmienne znaczenie z punktu widzenia nie tylko funkcjonowania infrastruktury krytycznej[28], ale także, np. wykładni prawa wewnętrznego i międzynarodowego oraz efektywności mechanizmów współpracy politycznej w środowisku międzynarodowym. Na podstawie powyższych rozważań

[26] Przestrzeń teleinformatyczna może być w przyszłości wykorzystana przez korporacje, np. do szpiegostwa przemysłowego lub rywalizacji na rynkach zbytu. Tego typu poważne incydenty pojawiały się, choć jeszcze nie w cyberprzestrzeni, np. w połowie lat 90. XX wieku między Francją a Stanami Zjednoczonymi. Zob. J. Fitchett, *French Report Accuses U.S. of Industrial Sabotage Campaign*, „The New York Times", 19.07.1995.

[27] Termin ten zaproponował François Paget, określając w ten sposób haktywistów, których działalność ma przede wszystkim kontekst międzypaństwowy i wynika często z motywacji patriotycznych. Jest to forma szkodliwej działalności, która stosunkowo rzadko bywa omawiana w kontekście najpoważniejszych zagrożeń teleinformatycznych dla bezpieczeństwa państw. Zob. F. Paget, *Hacktivism. Cyberspace has become the new medium for political voices*, „McAfee Labs White Paper", s. 4.

[28] Jako infrastrukturę krytyczną, za ustawą o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 roku, rozumie się m.in. systemy zaopatrywania w wodę, żywność, surowce energetyczne, energię, łączności, sieci teleinformatyczne, finansowe, transportowe, ratownicze czy zapewniające ciągłość administracji publicznej. Zob. Ustawa o zarządzaniu kryzysowym, 26.04.2007, Dz.U. z 2007 r. Nr 89, poz. 590.

oraz praktyki dotychczasowych cyberataków można więc pokusić się o wskazanie następujących zagrożeń:

- haking,
- haktywizm,
- „haktywizm patriotyczny”,
- wąsko rozumiana cyberprzestępczość,
- cyberterroryzm,
- cyberszpiegostwo,
- militarne wykorzystanie cyberprzestrzeni.

Analizując każdą z nich, warto mieć na uwadze dwie kwestie. Po pierwsze, należy pamiętać, iż szkodliwa działalność w cyberprzestrzeni częstokroć posiada także szeroki kontekst psychologiczno-propagandowy. Jest to szczególnie widoczne w przypadku takich zjawisk jak haktywizm czy cyberterroryzm, gdzie poza samym aktem włamania komputerowego liczy się także pożądana reakcja społeczeństwa, władz czy środowiska międzynarodowego[29]. Po drugie natomiast, nie można zapomnieć o toczącej się niejako równolegle dyskusji wokół, wspomnianego już, pojęcia cyberwojny. Kwestia ta jest o tyle ciekawa, iż nie tylko nie ma zgody co do zakresu tego fenomenu oraz jego definicji, ale także co do samego sensu jego wykorzystania.

Haking

Haking jest historycznie najstarszą formą wykorzystania luk w zabezpieczeniach komputerowych, stąd jest też pojęciem bardzo pojemnym i popularnym. Według Marcina Terlikowskiego, haker pierwotnie był uważany za osobę, która dzięki *dogłębnej wiedzy informatycznej i indywidualnym zdolnościom potrafiła przełamać zabezpieczenia elektroniczne systemów komputerowych*

[29] Szeroko o tym pisali m.in. Martin C. Libicki czy Piotr Sienkiewicz i Halina Świeboda. Zob. M.C. Libicki, *What is information warfare*, Washington 1995; P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*, [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009.

i zdobywać nieuprawniony dostęp do danych w nich przechowywanych[30]. Źródeł tego procederu można się dopatrywać już w połowie lat 60. XX wieku, kiedy również do użycia weszło samo słowo *hack*, mające wówczas pozytywne konotacje. Oznaczało bowiem wysoką specjalizację, pozwalającą skrócić lub obejść określone operacje w systemie. Z reguły uznaje się, iż zarówno sam termin, jak i zjawisko narodziły się w laboratoriach badawczych największych uniwersytetów, w tym przede wszystkim Massachussetts Institute of Technology. Na początku lat 70. haking został poszerzony o tzw. *phreaking*, polegający na wykorzystywaniu luk w systemach telekomunikacyjnych. Pierwszy *phreaker*, John Draper, mógł dzięki temu wykonywać darmowe połączenia telefoniczne, za co zresztą był wielokrotnie aresztowany. Na początku lat 80. XX wieku, wraz ze stopniowym rozpowszechnianiem się komputerów osobistych i rozwojem technologii ICT, haking zaczął ewoluować, przybierając bardziej dojrzałą, współczesną formę. Samo zjawisko pojawiło się wówczas po raz pierwszy w szeroko pojętym dyskursie publicznym. W 1983 roku temat ten poruszył amerykański film „War Games". Rok później pojawiły się także dwie publikacje książkowe, które przyczyniły się do popularyzacji kultury hakerskiej. Pierwszą była „cyberpunkowa" powieść Williama Gibsona *Neuromancer*, w której po raz pierwszy zresztą pojawił się termin „cyberprzestrzeń". Druga pozycja autorstwa Stevena Levy, *Hackers: Heroes of the Computer Revolution*, przedstawiła krótką jeszcze historię oraz najważniejsze aspekty ideologiczne tego ruchu, skupione wokół postulatu „wolności technologii". Tak więc to w latach 80. XX wieku doszło do wykształcenia się tradycyjnej formy hakingu[31]. Wówczas też zaczęły pojawiać się różnice w motywacjach, dotychczas raczej etycznych, tego wciąż niewielkiego środowiska. W tym okresie pojawiły się bowiem pierwsze poważniejsze przejawy wykorzystania tego typu umiejętności do działalności o charakterze *stricte* kryminalnym. Przykładowo, w 1987 roku grupa niemieckich hakerów VAXBusters włamała się do

[30] M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm*, [w:] M. Madej, M. Terlikowski (red.), dz. cyt., s. 98-99.

[31] Z. Clarke, J. Clawson, M. Cordell, *A brief history of hacking…*, „Historical Approaches to Digital Media", November 2003; R. Trigaux, *A History of Hacking*, „St. Petersburg Times Online", http://www.sptimes.com/Hackers/history.hacking.html, 13.02.2013.

serwerów NASA, komputerów w bazie wojskowej w Rammstein oraz do serwerów wielu instytucji badawczych, w tym, np. CERN (*European Organization for Nuclear Research*) czy University British Columbia. Pojawiły się także pierwsze przypadki hakerów opłacanych przez służby państwowe lub działających z pobudek politycznych. Symboliczna była tu sprawa Markusa Hessa, specjalisty wynajętego przez radzieckie KGB. Słynna stała się także historia Kevina Mitnicka, który stał się na wiele lat najsławniejszym hakerem na świecie. Co naturalne, w tym samym okresie problem zagrożeń hakingiem został dostrzeżony przez poszczególne państwa, w tym przede wszystkim Stany Zjednoczone, które nie tylko zaczęły aktualizować swój system prawny pod tym kątem, ale także utworzyły pierwszy na świecie zespół CERT (*Computer Emergency Response Team*). Co więcej, od przełomu lat 80. i 90. XX wieku coraz częściej zaczęły się pojawiać zorganizowane grupy hakerów, które w dużym stopniu odeszły od pierwotnych idei. Powszechniejsze stały się incydenty, których celem było nie tylko sprawdzenie stanu zabezpieczeń, ale także wykorzystanie odnalezionych luk w celach kryminalnych bądź politycznych[32]. W tym okresie z tradycyjnie pojętego środowiska hakerów wyodrębniły się zatem pierwsze poważne grupy cyberprzestępców oraz haktywistów.

Haking nadal pozostał jednak kategorią rozumianą bardzo szeroko. W tym kontekście na przełomie XX i XXI wieku doszło do wyodrębnienia się trzech rdzennych grup hakerów: białych, szarych oraz czarnych „kapeluszy" (tzw. *whitehats*, *greyhats, blackhats*). Różnią się one przede wszystkim stosunkiem do prawa, motywacjami oraz sposobem wykorzystania zdobytych danych. Programiści określający się jako „białe kapelusze" najczęściej są utożsamiani z pierwotną, tradycyjną i zarazem najbardziej etyczną formą hakingu. Tego typu specjaliści z reguły działają w granicach prawa, a ich celem jest głównie sprawdzenie swoich umiejętności. Często działają oni także na rzecz poprawy jakości pokonanych zabezpieczeń systemów i sieci. „Czarne kapelusze" obejmują natomiast tę grupę specjalistów, która działa z reguły poza granicami prawa, odnalezione luki w zabezpieczeniach udostępniając innym lub

[32] M. Lakomy, *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw*, s. 51-52; R. Trigaux, *A History of Hacking*, „St. Petersburg Times Online", http://www.sptimes.com/Hackers/history.hacking.html, 13.02.2013.

czyniąc nieuzasadnione szkody w zaatakowanych systemach i sieciach. W tym przypadku stosuje się termin „kraker". Co prawda „czarne kapelusze" swoją aktywnością łamią prawo, jednak jest to kategoria jakościowo nieco inna od głównego nurtu cyberprzestępczości. Krakerzy z reguły nie wykorzystują bowiem swoich umiejętności do uzyskania określonych korzyści osobistych. Wreszcie na początku XXI wieku wykształciła się również grupa tzw. „szarych kapeluszy". Ich działalność może wykraczać poza granice wyznaczone przez prawo, jednak czyni się tak głównie w imię wyższych przesłanek, czyli z reguły podniesienia jakości zabezpieczeń komputerowych. Są oni więc grupą stosującą metody zarówno „białych", jaki „czarnych kapeluszy"[33].

Na tej podstawie należy stwierdzić, iż haking jest zjawiskiem obejmującym łamanie szeroko pojętych zabezpieczeń komputerowych oraz uzyskanie nieuprawnionego dostępu do danych w formie elektronicznej. Co ważne, główną motywacją hakingu jest przede wszystkim sprawdzenie własnych umiejętności, czyli zakończone z sukcesem włamanie. Haker działa więc z pobudek pozapolitycznych, nie dokonując z reguły nieodwracalnych zniszczeń w zaatakowanych systemach i sieciach. Stanowi zatem marginalne zagrożenie z perspektywy bezpieczeństwa narodowego i międzynarodowego, tym bardziej, iż jak stwierdził Marcin Terlikowski, skala *tak rozumianego hakingu jest w praktyce bardzo mała*[34].

Haktywizm

Jak wspomniano wyżej, stosunkowo wcześnie, bo już w latach 80. XX wieku, środowisko hakerów zaczęło ulegać stopniowemu podziałowi. Oprócz tradycyjnie rozumianego hakingu pojawiły się nowe formy niezinstytucjonalizowanych zagrożeń teleinformatycznych. Niektórzy programiści postanowili wykorzystać własne umiejętności do nielegalnego osiągnięcia osobistych korzyści. Druga grupa natomiast

[33] S. Harris, A. Harper, C. Eagle, J. Ness, *Grey Hat Hacking. The Ethical Hacker's Handbook*, New York, Chicago 2008; B. Gottlieb, *HacK, CouNterHacK*, „The New York Times", 03.10.1999.

[34]Zob. M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm* [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*…, s. 98-99; Prezentacja: M. Terlikowski, *Haking, haktywizm, cyberterroryzm*, Polski Instytut Spraw Międzynarodowych, 23.04.2008, www.pism.pl, 13.02.2013.

zaczęła wykorzystywać potencjał cyberprzestrzeni do promowania określonych idei politycznych. W 1996 roku ukuto w tym kontekście termin haktywizm, który powstał z połączenia słów haking i aktywizm. Został on po raz pierwszy użyty przez grupę *Cult of the DeadCow*. Według nich, haktywistą miała być osoba wykorzystująca swoje umiejętności komputerowe do promocji określonych postulatów politycznych. W odróżnieniu od hakingu łamanie zabezpieczeń komputerowych, w tym rozumieniu, nie powinno prowadzić jedynie do rozwoju własnych umiejętności, lecz przede wszystkim do propagowania określonych postaw czy wartości w przestrzeni publicznej. Warto zarazem pamiętać, iż mimo pojawienia się tego terminu dopiero w 1996 roku, pierwsze głośne, motywowane politycznie cyberataki miały miejsce już na przełomie lat 80. i 90. XX wieku. Przykładowo, w 1989 roku cyberprzestrzeń została wykorzystana w protestach przeciwko próbnym wybuchom jądrowym[35]. Natomiast w 1994 roku wykorzystano technikę DDoS[36] jako formę politycznego protestu w Wielkiej Brytanii. Haktywizm w pełni rozwinął się jednak dopiero na początku XXI wieku, przede wszystkim za sprawą grup Anonymous oraz Lulzsec. Obie dokonały w ostatnich latach szeregu głośnych włamań i akcji w Internecie, które przyczyniły się do dostrzeżenia ich postulatów przez światową opinię publiczną. W Polsce symbolem rosnącego potencjału haktywizmu stały się protesty wokół umowy ACTA. Włączyła się w nie grupa Anonymous, dokonując serii ataków na witryny internetowe polskich instytucji rządowych[37]. W środowisku międzynarodowym możliwości haktywizmu potwierdziła natomiast arabska wiosna,

[35] Zob. A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa teleinformatycznego we współczesnym świecie*, Warszawa 2003, s. 60-61.

[36] *Distributed Denial of Service* – rodzaj ataku, polegający na zablokowaniu funkcjonowania systemu lub usługi sieciowej poprzez przeciążenie jej danymi. W odróżnieniu od DoS (*Denial of Service*), DDoS ma charakter rozproszony, czyli jest przeprowadzany z wielu komputerów naraz. Zob. E. Zuckerman, H. Roberts, R. McGrady, J. York, J. Palfrey, *Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites*, „The Berkman Center for Internet & Society", Harvard 2010.

[37] *Polskie strony rządowe przestały działać. Protest przeciwko ACTA?*, Wirtualna Polska, 21.01.2012, http://wiadomosci.wp.pl/kat,1329,title,Polskie-strony-rzadowe-przestaly-dzialac-Protest-przeciwko-ACTA,wid,14187932,wiadomosc.html?ticaid=1100ef&_ticrsn=5, 13.02.2013; M. Casserly, *What is Hacktivism? A short history of Anonymous, Lulzsec and the Arab Spring*, PC Advisor, 03.12.2012, http://www.pcadvisor.co.uk/features/internet/3414409/what-is-hacktivism-short-history-anonymous-lulzsec-arab-spring/, 13.02.2013; *WikileaksInfowar was not the first online protest action*, „Media Alternatives", http://medialternatives.blogetery.com/2010/12/15/intervasion-supports-anonymous/,13.02.2013.

w którą zaangażowali się nie tylko regionalni specjaliści, ale także międzynarodowe zespoły politycznie motywowanych hakerów. Co ważne, ich aktywność, nie stanowiąc poważnego zagrożenia dla funkcjonowania Internetu czy infrastruktury krytycznej, przyczyniła się do wybuchu masowych protestów[38].

W świetle lawinowo rosnącej popularności haktywizmu pojawiło się w literaturze naukowej szereg definicji tego fenomenu. Przykładowo, zdaniem Dorothy E. Denning, jest to *konwergencja hakingu i aktywizmu, gdzie haking odnosi się do wykorzystywania komputerów w sposób nietypowy i często nielegalny, z reguły z wykorzystaniem specjalistycznego oprogramowania* (…) *Haktywizm obejmuje elektroniczne nieposłuszeństwo obywatelskie, przenosząc metody obywatelskiego nieposłuszeństwa w cyberprzestrzeń*[39]. Zdaniem Marka G. Milone'a, haktywista, wykorzystując te same narzędzia[40] co haker, czyni to w celu zwrócenia uwagi na jakiś cel polityczny lub społeczny[41]. Natomiast zdaniem Marcina Terlikowskiego, współczesna forma haktywizmu ulega zmianom. Według niego, *jego motywacją są bieżące problemy polityczne, a ataki stają się po prostu kolejną formą walki politycznej, prowadzonej przez członków i sympatyków różnych organizacji*[42].

[38] Zob. np. E. Sterner, *The Paradox of Cyber Protest*, „Policy Outlook", April 2012, George C. Marshall Institute; M. Lakomy, *Arab Spring and New Media*, [w:] B. Przybylska-Maszner (red.), *The Arab Spring*, Poznań 2011, s. 45-55.

[39] Za J.L.C. Thomas, *Ethics of Hacktivism*, Aribo.eu, 12.01.2001, http://www.aribo.eu/wp-content/uploads/2010/12/Thomas_2001-copy.pdf, 13.02.2013.

[40] Narzędzia i techniki wykorzystywane przez hakerów, haktywistów, przestępców i inne grupy działające w sieci są oczywiście kategorią bardzo szeroką i stale ewoluującą. Generalnie wyróżnia się cztery fazy ataku teleinformatycznego: wybór celu, jego identyfikacja, dobranie metody ataku oraz jego przeprowadzenie. Dokonuje się go za pomocą szeregu technik. Do najpopularniejszych można zaliczyć: podsłuchiwanie i *snooping* (wykradanie haseł, skanowanie portów, analiza ruchu sieciowego, *DNS rangegrabbing*), *Denial of Service* i *Distributed Denial of Service* (polegający na paraliżu określonej sieci lub komputera, np. za pomocą *Ping of Death*, ataki SYN, *ICMP flooding*, *DNS Cache Pollution*), *protocolexploitation* (wykorzystanie błędów oprogramowania do zdobycia nieuprawnionego dostępu do danych), odtwarzanie roli (*impersonation*, które obejmują np. *Source RoutedAttacks* czy *DNS Service Impersonation*), *spearphishing* (obejmujący różnorodne metody z zakresu inżynierii społecznej i psychologii) czy *hijacking* (polegający na przejęciu istniejącego połączenia sieciowego). Do realizacji tych i innych technik wykorzystuje się szereg odmiennych narzędzi, w tym: trojany, *backdoory*, *packetsniffers*, skanery portów, robaki czy sieci *botnet*. Zob. *HackingExplained*, LinuxExposed, 14.08.2012, http://www.linuxexposed.com/hacking/hacking-explained-some-techniques/, 13.03.2013; R. Shimonsky, *HackingTechniques*, IBM, http://www.ibm.com/developerworks/library/s-crack/.,13.03.2013; *Ataki ukierunkowane, czyli od złośliwego łącznika do infiltracji firmowej sieci*, „DLP-Expert", 2012, nr 3.

[41] M.G. Milone, *Hacktivism: Securing the National Infrastructure*, „The Business Lawyer", 2002, nr 1, vol. 58, s. 385-386.

[42] M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty...,* s. 105.

W tym kontekście warto więc zaznaczyć, iż haktywizm nie jest jednorodną formą szkodliwej działalności w cyberprzestrzeni. Zwrócił na to uwagę François Paget, który wyróżnił trzy główne grupy haktywistów. Do pierwszej zaliczył Anonymous, której funkcjonowanie obejmuje włamania na witryny internetowe, zdobywanie poufnych informacji oraz blokowanie określonych usług sieciowych. Częstokroć dane te mają istotną wartość w kontekście bieżącej debaty publicznej, tak na poziomie regionalnym, państwowym, jak i międzynarodowym. Do drugiej grupy zaliczył tzw. cyberlokatorów (*cyberoccupiers*). Według autora, kategoria ta obejmuje właściwych aktywistów politycznych działających w cyberprzestrzeni, którzy wykorzystują ją w celach propagandowych lub informacyjnych. Jest to zjawisko spotykane coraz częściej w Internecie, gdzie tego typu jednostki lub grupy promują określone poglądy nie tylko za pomocą włamań, ale także m.in. na forach dyskusyjnych, blogach czy w mediach społecznościowych. Działalność tego typu haktywistów może się także przejawiać przygotowywaniem rozpowszechnianych w sieci materiałów o charakterze satyrycznym, wymierzonych w określone wartości lub poglądy polityczne. Warto przy tym pamiętać, iż nie zawsze jest to działalność o charakterze bezinteresownym, gdyż częstokroć sponsorują ją partie polityczne lub grupy interesu. Wreszcie, Paget wyróżnił „cyberwojowników", wchodzących w skład tzw.cyberarmii. Ta grupa, ze względu na swoją specyfikę, zostanie jednak omówiona oddzielnie[43]. Na tej podstawie haktywizm można określić jako wykorzystanie technik hakerskich oraz innych niestandardowych metod do promowania określonych postulatów politycznych lub społecznych w cyberprzestrzeni. Celem ataków haktywistów mogą być nie tylko instytucje państwowe, ale także organizacje rządowe i pozarządowe, korporacje, partie polityczne czy innego rodzaju podmioty funkcjonujące *online*.

Tak pojmowany haktywizm posiada więc dwie istotne cechy z punktu widzenia bezpieczeństwa narodowego i międzynarodowego. Przede wszystkim w większości

[43] F. Paget, *Hacktivism. Cyberspace Has become the new medium for politicalvoices*, „McAfeeLabs White Paper", s. 4; M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty…* s. 105.

wypadków jest to działalność o charakterze ideowym[44]. Co za tym idzie, wykorzystanie narzędzi i technik właściwych hakingowi nie ma z reguły na celu doprowadzenia do trwałych szkód, które mogłyby być odczuwalne przez całe społeczeństwo. Po drugie, akcje haktywistów muszą przede wszystkim spełniać warunek widowiskowości. Zasadniczym celem jest bowiem zwrócenie uwagi opinii publicznej na określony problem lub postulat, a nie dokonanie trwałych szkód w cyberprzestrzeni. Tego typu cyberataki miałyby bowiem efekt odwrotny do założonego[45]. W dużej mierze tendencje te udowodniły wspomniane już protesty Anonymous przeciwko umowie ACTA w styczniu 2012 roku. Grupa włamała się wówczas na strony internetowe należące do polskiego rządu, nie doprowadzając zarazem do trwałych zakłóceń funkcjonowania najważniejszych usług internetowych w kraju. W efekcie ich postulaty spotkały się z dużym zainteresowaniem mediów oraz poparciem podobnie nastawionych internautów[46]. Tym samym haktywizm, jakkolwiek jest stale ewoluującą i coraz powszechniejszą formą szkodliwego wykorzystania cyberprzestrzeni, nie stanowi poważniejszego zagrożenia dla bezpieczeństwa teleinformatycznego państw. Te aspekty haktywizmu, które łączą się z nielegalnym wykorzystaniem technik hakerskich, mogą czasami okazać się uciążliwe dla funkcjonowania instytucji publicznych, jednak wyrządzone szkody mają wymiar przede wszystkim wizerunkowy.

Haktywizm patriotyczny

Jak już wspomniano wyżej, istnieje odmiana haktywizmu, która zasługuje, z perspektywy politologicznej analizy zagrożeń dla bezpieczeństwa, na osobne omówienie. François Paget ten specyficzny typ haktywistów określił mianem „cyberwojowników", wchodzących w skład tzw. cyberarmii. Jest to grupa jakościowo

[44] Trzeba mieć przy tym na uwadze, iż, wbrew pozorom, często świadomość polityczna najbardziej aktywnych grup haktywistów bywa bardzo niska. Co za tym idzie, czasami ich postulaty mają niewielkie szanse realizacji.

[45] G. Coleman, *Coleman Discusses >>Anonymous<< as Civil Disobedience*, Steinhardt School of Culture, Education, and Human Development, http://steinhardt.nyu.edu/news/2011/3/11/Coleman_Discusses_Anonymous_as_Civil_Disobedience, 21.11.2012.

[46] Zob. *Hacktivism. Cyberspace has become the new medium for political voices*, „McAfee Labs White Paper"; T. Grynkiewicz, *Weekendowy zamach na strony rządowe*, „Gazeta Wyborcza", 23.01.2012.

odrębna od omówionego wyżej haktywizmu. Przede wszystkim należy zauważyć, iż np. Anonymous częstokroć swoje działania motywują obroną praw człowieka czy uniwersalnych wartości. Tymczasem „cyberwojownicy" działają przede wszystkim z pobudek patriotycznych, narodowych lub w obronie określonych wartości lub postaw politycznych właściwych danemu państwu. W tej perspektywie działalność „cyberarmii" ma częstokroć kontekst międzynarodowy lub objawia się w trakcie konfliktów zbrojnych. W porównaniu do konwencjonalnego haktywizmu inne są więc nie tylko jego motywacje, ale także stosowane metody działania[47].

Na tej podstawie można wskazać na wiele przykładów występowania tej formy zagrożeń teleinformatycznych. W czerwcu 2011 roku *Anonymous* rozpoczęło operację *Turkey*, której celem było wsparcie dla młodzieży tureckiej, protestującej przeciwko cenzurze Internetu. W efekcie tureckie strony rządowe przez kilka dni były atakowane metodą DDoS. W odpowiedzi na ten atak grupa haktywistyczna *Akincilar* dokonała zakończonego sukcesem włamania na stronę domową *AnonPlus*. Miała być to więc narodowa odpowiedź przeciwko mieszaniu się *Anonymous* w wewnętrzne sprawy Turcji. W sieci sławny stał się także konflikt między *SyrianCyberArmy*a Anonymous w kontekście wojny domowej w Syrii. W odpowiedzi na ataki Anonymous na syryjskie strony rządów SCA z sukcesem dokonało ataku na ich stronę domową[48]. W Internecie od lat można również zauważyć przejawy regularnej, masowej rywalizacji pomiędzy tego typu grupami, złożonymi z patriotycznie usposobionych haktywistów z różnych krajów. Za świetny przykład może tu posłużyć wieloletni konflikt w cyberprzestrzeni między Indiami a Pakistanem. Grupy haktywistów (np. *Pak CyberArmy*, *Pak CyberPirates*, *The United Indian Hackers*) od lat nawzajem dokonują cyberataków, głównie przeciwko stronom internetowym drugiej strony. Ich łupem w ostatnich latach padło w sumie kilkanaście tysięcy witryn. Szerokim echem odbiło się m.in. włamanie dwóch Pakistańczyków w grudniu 2012 roku na ponad 300

[47] F. Paget, *Hacktivism. Cyberspace has become the new medium for political voices*, „McAfee Labs White Paper", s. 26-27.
[48] Tamże, s. 26-29.

indyjskich stron internetowych[49]. Podobna sytuacja ma również miejsce w przypadku Izraela i Palestyny, gdzie ataki teleinformatyczne stale towarzyszą regularnym napięciom i incydentom zbrojnym w relacjach dwustronnych. Przykładowo, w reakcji na izraelską kampanię lotniczą w Strefie Gazy w listopadzie 2012 roku arabscy aktywiści w ciągu tygodnia zaatakowali izraelskie strony rządowe aż 44 miliony razy[50]. Warto także wspomnieć o głośnych atakach na Estonię w 2007 roku. W środowisku naukowym istnieją podzielone opinie co do tego, kto w rzeczywistości stał za organizacją i przeprowadzeniem rosyjskiej kampanii w cyberprzestrzeni. Pojawiają się głosy wskazujące zarówno na niezależne grupy patriotycznie zmotywowanych haktywistów, jaki na celową działalność służb specjalnych[51]. Wydaje się, iż pełna weryfikacja tych doniesień nie jest do końca możliwa. Z pewną dozą pewności można jednak przyjąć, iż przynajmniej część z nich została przeprowadzona niezależnie od czynników państwowych. Z drugiej strony, niektóre cyberataki były zbyt dobrze zorganizowane, miały tak duży potencjał oraz były na tyle korzystne dla Kremla, że brak zaangażowania służb państwowych wydaje się mało prawdopodobny.

Na tej podstawie należałoby wskazać kilka najistotniejszych cech tej formy zagrożeń teleinformatycznych. Przede wszystkim można zauważyć, iż działalność tego typu grup ma charakter zdecydowanie bardziej inwazyjny, a co za tym idzie groźniejszy, od tradycyjnej formy haktywizmu. Działania „cyberwojowników" z reguły opierają się na atakach DDoS przeciwko stronom internetowym, mogą jednak obejmować także inne, groźniejsze formy ataków[52]. Co prawda jest to raczej rzadkość, jednak nie ulega wątpliwości, iż haktywiści, szczególnie w trakcie kryzysów i konfliktów międzynarodowych, mogą przeprowadzić skuteczne ataki wykraczające poza standardowy *defacement* stron internetowych. Po drugie, tzw. *cyberarmie*

[49] J. Lee, *300 Indian sites defaced by Pakistani hackers*, Cyber War News, 09.12.2012, http://www.cyberwarnews.info/2012/12/09/300-indian-sites-defaced-by-pakistani-hackers/, 15.02.2013; B. Khanna, *India-Pak on Cyber War prior August 15*, „Hindustan Times", 21.08.2012, http://www.hindustantimes.com/Punjab/Chandigarh/India-Pak-on-Cyber-War-prior-August-15/SP-Article1-917212.aspx, 15.02.2012.

[50] *Mass cyber-war on Israel over Gaza raids*, Al Jazeera, 19.12.2012, http://www.aljazeera.com/news/middleeast/2012/11/2012111973111746137.html, 15.02.2013.

[51] Zob. K. Ruus, *Cyber War I: Estonia Attacked from Russia*, „European Affairs", 2008, nr 9:1.

[52] M. Lakomy, *Cyberwojna...,* s. 145-147.

działają z pobudek narodowych, patriotycznych lub w obronie określonych postaw i wartości w wymiarze międzypaństwowym. Co za tym idzie, ta forma aktywizmu występuje z reguły w sytuacjach napięć lub kryzysów o charakterze ponadnarodowym. Po trzecie, François Paget wskazał, iż grupy te cechują się szeroko pojętym fundamentalizmem oraz są właściwe państwom autorytarnym, swoją działalnością wspierają ich rządy. Nie do końca można się z tym jednak zgodzić, gdyż istnieje wiele ruchów aktywistycznych o motywacjach patriotycznych, działających, np. w Indiach, Rumunii czy Turcji[53]. W tym kontekście należałoby więc stwierdzić, iż ten swoisty „haktywizm patriotyczny" jest w ostatnich latach coraz powszechniejszą i poważniejszą formą zagrożeń teleinformatycznych.

Cyberprzestępczość

Jak wspomniano wyżej, źródeł zjawiska cyberprzestępczości należy upatrywać w hakingu. Już w latach 80. XX wieku z tego środowiska wyodrębnili się specjaliści, którzy chcieli wykorzystać swoje umiejętności do działalności o charakterze kryminalnym, osiągając tym samym znaczne korzyści osobiste. W tym kontekście nie ulega jednak wątpliwości, iż sam termin cyberprzestępczość jest często nadużywany i nie ma zgody co do jednoznacznego rozumienia tego zjawiska. W tym przypadku podstawą dyskusji na ten temat powinna być definicja sformułowana w jedynej dotychczas umowie międzynarodowej poświęconej tej problematyce. Według Konwencji Rady Europy o Cyberprzestępczości, podpisanej w 2001 roku w Budapeszcie, w skład tego procederu można zaliczyć cztery kategorie działań wykonywanych za pomocą komputerów: szeroko rozumiane naruszenia bezpieczeństwa (takie jak haking czy nielegalne uzyskanie danych), oszustwa i fałszerstwa, pornografię dziecięcą oraz naruszenia praw autorskich[54]. Można jednak sformułować zdecydowanie szerszą definicję, według której cyberprzestępczością byłoby wykorzystanie komputerów do jakiejkolwiek działalności wykraczającej poza

[53] F. Paget, *Hacktivism. Cyberspace has become the new medium for political voices*, „McAfee Labs White Paper", s. 4, 28-30.
[54] Konwencja Rady Europy o Cyberprzestępczości, Rada Europy, Budapeszt, 23.11.2001.

granice prawa. W ten sposób zagadnienie to określiły m.in. Kristin M. Finklea oraz Catherine A. Theohary[55]. Bardzo szeroko została sformułowana również polska definicja tego zjawiska, zawarta w Rządowym Programie Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na Lata 2011-2016. Stwierdzono w nim, iż cyberprzestępstwo to *czyn zabroniony popełniony w obszarze cyberprzestrzeni*[56].

W kontekście zaproponowanej wyżej typologii tak szerokie rozumienie cyberprzestępczości, jakkolwiek właściwe z perspektywy prawnej oceny incydentów teleinformatycznych, rodzi jednak pewne wątpliwości. W tym rozumieniu każdy bowiem akt, czy to haking, haktywizm, cyberterroryzm czy szpiegostwo komputerowe, powinien być uznany za przestępstwo. Z drugiej jednak strony, z uwagi na wielopłaszczyznowość i wieloaspektowość zagrożeń teleinformatycznych, a także skuteczność funkcjonujących mechanizmów politycznych lub wykładnię prawa międzynarodowego, taka definicja może rodzić pewne problemy natury interpretacyjnej. Sugerowałaby ona bowiem, iż organami właściwymi do reakcji na wszelkiego rodzaju incydenty komputerowe są krajowe organy ścigania, odpowiedzialne za walkę z przestępczością. Co za tym idzie, nawet najpoważniejsze ataki przeciwko infrastrukturze krytycznej nie mogłyby się spotkać, np. z reakcją sił zbrojnych lub protestem w oparciu o Kartę Narodów Zjednoczonych. Na tej podstawie można więc tę definicję zawęzić i wskazać na pewien wiodący nurt przestępczości komputerowej, który jakościowo odróżnia się od innych, wyróżnionych wyżej form szkodliwej działalności w cyberprzestrzeni. Jego cechą charakterystyczną jest motywacja obejmująca osiągnięcie określonych korzyści osobistych.

Tak rozumiana działalność kryminalna w sieci może się przejawiać, np. dążeniem do uzyskania wartościowych danych, które mogą zostać z zyskiem wykorzystane przez jednostki lub zorganizowane grupy przestępcze. W tym celu stosuje się szereg narzędzi i technik właściwych także innym zagrożeniom teleinformatycznym. Najpopularniejsze to: specjalistyczne oprogramowanie

[55] K.M. Finklea, C.A. Theohary, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, „Congressional Research Service", 20.07.2012.
[56] Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na Lata 2011-2016, Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2010, s. 6.

szpiegowskie, tzw. (*spyware*) oraz sieci *botnet*. Do tych pierwszych należy zaliczyć m.in.: *Adwarecookies*, będące metodą śledzenia aktywności użytkownika w sieci, *keyloggery,* rejestrujące wykorzystanie klawiatury komputera (a więc np. wpisane hasła i nazwy użytkownika), czy trojany umożliwiające zdalny dostęp do zainfekowanego komputera. Celem tego typu ataków jest więc uzyskanie poufnych informacji, które, np. mogą zostać sprzedane zainteresowanym podmiotom lub wykorzystane do kradzieży środków z internetowego konta bankowego. Warto mieć przy tym na uwadze, iż tego typu oprogramowanie jest szeroko dostępne w sieci i może zostać skutecznie użyte nawet przez osoby nie mające odpowiedniego przygotowania informatycznego. Jeśli chodzi natomiast o sieci *botnet*, to należy stwierdzić, iż są one coraz częściej wykorzystywane przez zorganizowane grupy cyberprzestępcze, które sprzedają swoje usługi na czarnym rynku. Obejmują one, np. przeprowadzenie ataku DDoS na wskazane przez mocodawców serwisy internetowe. Tego typu narzędzia mogą być również pomocne przy wymuszaniu pieniędzy od właścicieli atakowanych witryn lub rozsyłaniu „spamu". Wreszcie, sieci *botnet* mogą zostać także użyte jako wsparcie dla działań cyberszpiegowskich lub jako platforma udostępniająca nielegalne oprogramowanie[57]. Należy mieć przy tym świadomość, iż stopień zaawansowania przestępców komputerowych jest coraz wyższy. Z jednej strony można wskazać na coraz śmielsze działania grup pochodzenia chińskiego, które od lat wykorzystują najnowsze zdobycze techniki, aby penetrować systemy i sieci należące do zachodnich korporacji. Z drugiej stale rośnie liczba kryminalistów, wykorzystujących szeroko pojętą inżynierię społeczną[58]. Proceder ten od początku XXI wieku stale przybiera na sile. Przykładowo, tylko w 2008 roku aż 1,7 miliona Kanadyjczyków padło ofiarą kradzieży tożsamości, co przyczyniło się do strat szacowanych na ok. 2 mld dolarów[59]. Ponadto o bogactwie metod stosowanych przez cyberprzestępców świadczy fakt, iż Internet może być wykorzystywany także jako

[57] Zob. E.J. Esquibel, M.A. Laurenzano, J. Xiao, T. Zuvich, *Cyber Criminal Activity : Methods and Motivations*, University of Washington, Washington D.C. 2005.

[58] P. Gontarczyk, *Cyberprzestępcy opracowują nowe metody szkodliwych ataków*, PCLab, 07.07.2008, http://pclab.pl/news33122.html, 18.02.2013.

[59] *Canada's Cyber Security Strategy. For a stronger and more prosperous Canada*, Her Majesty the Queen in Right of Canada, Canada 2010.

platforma ułatwiająca łamanie prawa *offline*. Zwróciła na to uwagę Organizacja Narodów Zjednoczonych, twierdząc, że sieć coraz częściej stanowi nowy obszar promocji konsumpcji i sprzedaży narkotyków[60].

W tym kontekście należy jednak mieć na uwadze fakt, iż tak rozumiana cyberprzestępczość z punktu widzenia bezpieczeństwa narodowego i międzynarodowego stanowi jednak zagrożenie raczej pośrednie i z reguły dość ograniczone. Jak bowiem słusznie stwierdził Marcin Terlikowski, przestępcy *nie mają zazwyczaj interesu w bezpośrednim uderzeniu w podmioty państwowe, gdyż mogłoby to zwrócić uwagę władz i w konsekwencji skutkować wobec nich podjęciem działań przez organy ścigania*[61]. Co prawda, istnieją przykłady poważnych akcji tego typu, które ze względu na swoją skalę wywołały żywą reakcję władz państwowych. Są to jednak z reguły działania o wymiarze międzynarodowymi trudnej do oceny specyfice. Jest to szczególnie widoczne w relacjach chińsko-amerykańskich. Grupy rodem z ChRL od lat stoją za największą liczbą poważnych włamań komputerowych w USA, mając na celu przejęcie zaawansowanych technologii. Skala tego procederu sprawiła, iż spotkało się to w końcu z ostrą reakcją władz amerykańskich. Po serii włamań w 2010 roku, których celem była m.in. korporacja Google, sekretarz stanu Hillary Clinton skrytykowała bezczynność Pekinu w tej sprawie[62]. Warto mieć przy tym na uwadze, iż z reguły niezwykle trudno oddzielić ataki przeprowadzane przez grupy powiązane z chińskimi służbami specjalnymi i armią od tych, które mają podłoże czysto kryminalne.

W świetle powyższych rozważań należy więc podkreślić, iż ocena i klasyfikacja zjawiska cyberprzestępczości zależy przede wszystkim od jego definicji. W przytoczonym wyżej, wąskim rozumieniu tego procederu, cyberprzestępczość

[60] Zob. *Prospective Analysis on Trends in Cybercrime from 2011 to 2020*, French National Gendarmerie, Lille 2010; T. Maurer, *Cyber Norm Emergence at the United Nations – an Analysis of the Activities at the UN Regarding Cyber-Security*, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011, s. 37-38.

[61] M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm*, [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*…, s. 96.

[62] *Secretary of State Hillary Clinton says China's Cyber Attacks Must Face Consequences*, Government Security, http://www.governmentsecurity.org/latest-security-news/secretary-of-state-hillary-clinton-says-chinas-cyber-attacks-must-face-consequences.html, 18.02.2013.

stanowi głównie wyzwanie dla krajowych organów ścigania oraz międzynarodowych procedur współpracy w tej dziedzinie. W kontekście analizy zagrożeń dla bezpieczeństwa państw jest ona jednak wyzwaniem w znacznym stopniu pośrednim, a za co za tym idzie, dość ograniczonym. Cyberprzestępcy niezwykle rzadko biorą bowiem na cel te elementy cyberprzestrzeni, nad którymi bezpośrednio czuwają służby państwowe, w tym np. teleinformatyczną infrastrukturę krytyczną. Tym samym w zdecydowanej większości przypadków proceder ten nie wiąże się z reperkusjami o charakterze politycznym, prawnym lub wojskowym.

Cyberterroryzm

Jednym z najczęściej stosowanych terminów w przestrzeni publicznej z zakresu bezpieczeństwa teleinformatycznego w ostatnich kilkunastu latach jest cyberterroryzm. Media i elity polityczne częstokroć stosują ten termin do opisania zjawisk, które *de facto* z terroryzmem w cyberprzestrzeni nie mają wiele wspólnego. Co więcej, nie ma także zgody środowiska naukowego co do rozumienia tego terminu. Jest to tym wyraźniejsze, iż nie ma również konsensusu badaczy co do definicji samego terroryzmu, na co słusznie zwrócili uwagę Agnieszka Bógdał-Brzezińska oraz Marcin F. Gawrycki[63]. W świetle zaproponowanej wyżej typologii warto więc podjąć próbę szczegółowej analizy, czym w zasadzie jest cyberterroryzm oraz jakie posiada cechy.

W literaturze przedmiotu funkcjonuje wiele definicji tego pojęcia. Wspomniana już Dorothy E. Denning uznała go za *konwergencję terroryzmu i cyberprzestrzeni*. Jej zdaniem, cyberatak, który zostałby uznany za akt terroryzmu, powinien skutkować przemocą przeciwko osobom lub mieniu, lub chociaż generować strach[64]. Według Jamesa A. Lewisa jest to *wykorzystanie sieci komputerowych jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe, itp.) bądź*

[63] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 63.

[64] D.E. Denning, *Cyberterrorism*, Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, Georgetown University, Washington 23.05.2000.

też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań[65]. Według Marcina Terlikowskiego jest to *właśnie działalność terrorystyczna, w której programy i urządzenia elektroniczne oraz systemy teleinformatyczne spełniają funkcję specyficznego rodzaju narzędzia – broni w rękach terrorystów*[66]. Z kolei Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na Lata 2011-2016 definiuje to pojęcie jako cyberprzestępstwo o charakterze terrorystycznym[67]. W tym świetle warto przytoczyć opinię Tomasza Szubrychta, który zauważył, iż w większości definicji cyberterroryzmu można zauważyć dwie odrębne tendencje. Pierwsza charakteryzuje się zwróceniem szczególnej uwagi na możliwość wykorzystania sieci komputerowych do przeprowadzenia ataków. Druga natomiast dostrzega fakt, iż to komputery i systemy są ich obiektem[68]. Wydaje się, iż oba podejścia są w dużej mierze prawidłowe. Cyberterroryzm obejmuje bowiem wykorzystanie komputerów, czy szerzej, technologii ICT do działań terrorystycznych w cyberprzestrzeni.

Na tym tle warto wskazać na dwie definicje, które jak się wydaje, najpełniej uchwyciły to zjawisko. Pierwszą z nich sformułowali Agnieszka Bógdał-Brzezińska oraz Marcin F. Gawrycki. Ich zdaniem, cyberterroryzm jest to *politycznie motywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów*. Co więcej, w szerszym rozumieniu, ich zdaniem, jest to także *wykorzystanie Internetu przez organizacje terrorystyczne do komunikowania się, propagandy i dezinformacji*[69]. Druga została zaproponowana przez Ernesta Lichockiego. Według niego, cyberterroryzm jest to *przemyślany politycznie lub militarnie motywowany atak albo groźba ataku na systemy*

[65] J.A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, Washington 2002.
[66] M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe Haking, haktywizm i cyberterroryzm*, [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*…, s. 111.
[67] Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na Lata 2011-2016, Warszawa 2010, s. 6.
[68] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej", 2005, nr 1, s. 176.
[69] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 73.

teleinformatyczne oraz zgromadzone dane w celu sparaliżowania lub poważnego zniszczenia Infrastruktury Krytycznej Państwa oraz zastraszenia i wymuszenia na rządzie lub społeczności daleko idących polityczno-militarnych działań. Cyberatak może być przeprowadzony jako część składowa większej polityczno-militarnej akcji lub samodzielnego ataku. E. Lichocki za cyberterroryzm uznał także wykorzystanie sieci teleinformatycznych przez organizacje terrorystyczne do *propagandy, rekrutacji, komunikacji, mobilizacji, zbierania informacji o potencjalnych celach ataku, planowania i koordynacji akcji oraz szeroko pojętej dezinformacji i walki psychologicznej*[70].

Na tym tle można więc wskazać na kilka zasadniczych cech zagrożenia dla bezpieczeństwa teleinformatycznego jakim jest cyberterroryzm. Przede wszystkim cyberterroryzm charakteryzuje się szeroko pojętą polityczną motywacją. Przykładowo, może on więc obejmować promocję określonych postulatów o charakterze ideologicznym lub religijnym. Jak wskazano wcześniej, polityczna inspiracja towarzyszy również szeroko pojętemu haktywizmowi. Jak jednak słusznie zauważyła Dorothy E. Denning, cyberterroryzm od haktywizmu odróżnia cel, jakim jest wyrządzenie możliwie dużych strat przeciwnikowi, włącznie z ofiarami ludzkimi[71]. Co za tym idzie, działania w sieci mogą mieć reperkusje nie tylko w wymiarze *online*, ale także *offline*. Podczas gdy hakerzy i haktywiści ograniczają się do stosunkowo niegroźnych technik, cyberterroryści stosują najbardziej zaawansowane metody przeciwko celom mającym kluczowe znaczenie dla bezpieczeństwa państwa. Słusznie więc Ernest Lichocki wskazał na infrastrukturę krytyczną jako obszar szczególnego zainteresowania terrorystów w cyberprzestrzeni. Potencjalny atak, np. przeciwko sieci elektroenergetycznej miałby bowiem katastrofalne skutki, paraliżując w zasadzie funkcjonowanie państwa oraz doprowadzając do trudnych do przewidzenia

[70] E. Lichocki, *Cyberterroryzm jako nowa forma zagrożeń dla bezpieczeństwa*, [w:] K. Liedel (red.), *Transsektorowe obszary bezpieczeństwa narodowego*, Warszawa 2011, s. 71.
[71] Za A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy…*, s. 61.

konsekwencji w wymiarze społecznym i gospodarczym[72]. Mimo braku zgody ekspertów co do rzeczywistych źródeł tych incydentów, jako przykłady tego typu aktów cyberterrorystycznych podaje się awarie brazylijskiej sieci elektroenergetycznej w 2005 i 2007 roku[73]. Za akt cyberterroryzmu należałoby także uznać ataki przeciwko estońskiej bankowości internetowej, stanowiącej część systemu finansowego państwa, w kwietniu 2007 roku lub wykorzystanie wirusa *Stuxnet* przeciwko irańskiemu programowi atomowemu. Ponadto należy pamiętać, iż ta forma szkodliwej działalności w sieci posiada także niezwykle istotny wymiar psychologiczny[74]. Co za tym idzie, celem cyberterrorystów jest nie tylko dokonanie określonych zniszczeń, ale także osiągnięcie określonego celu politycznego poprzez oddziaływanie w wymiarze propagandowym i psychologicznym. Tak więc założeniem takiego ataku może tu być m.in. wywarcie określonego wpływu na decydentów państwowych lub wywołanie poczucia strachu wśród społeczeństwa. Po trzecie, w odróżnieniu od wyżej omówionych zagrożeń, za aktami cyberterrorystycznymi stoją z reguły podmioty o wysokim stopniu zorganizowania. Co prawda, można sobie wyobrazić sytuację, w której pojedynczy programista mógłby zorganizować poważny atak przeciwko infrastrukturze krytycznej państwa, jest to jednak mało prawdopodobne. Odpowiedni potencjał do tego typu działań posiadają natomiast organizacje terrorystyczne, sympatyzujące z nimi grupy oraz przede wszystkim państwa. Świadczy o tym skuteczne wykorzystanie, stworzonego przez USA i Izrael, wirusa *Stuxnet*[75]. Wreszcie, jak słusznie podkreślono w przytoczonych wyżej definicjach A. Bógdał-Brzezińskiej, M.F. Gawryckiego oraz E. Lichockiego, w szerokim rozumieniu cyberterroryzm obejmuje również wykorzystanie Internetu do rekrutacji,

[72] Skutkiem tego typu ataku mógłby być bowiem, np. paraliż sieci transportowej czy służby zdrowia, co najprawdopodobniej skutkowałoby ofiarami wśród ludności cywilnej. Zob. E. Bumiller, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, „The New York Times", 11.10.2012.

[73] M. Mylrea, *Brazil's Next Battlefield: Cyberspace*, „Foreign Policy Journal", 15.11.2009, http://www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace/, 18.02.2012.

[74] Za E. Lichocki, *Cyberterroryzm jako nowa forma zagrożeń dla bezpieczeństwa,* s. 73.

[75] Zob. *Annual Report PandaLabs*, Panda Security 2010; A. Matrosov, E. Rodionov, D. Harley, J. Malcho, *Stuxnet Under the Microscope*, ESET Report 2010, Rev. 1.31.

komunikacji czy bieżącej propagandy politycznej. Wbrew pozorom jest to fenomen bardzo powszechny, szczególnie w krajach Szerokiego Bliskiego Wschodu[76].

Cyberszpiegostwo

W ciągu ostatnich kilkunastu lat szczególną i jednocześnie jedną z najpopularniejszych form zagrożeń teleinformatycznych stało się cyberszpiegostwo. Można je najogólniej zdefiniować jako wykorzystanie przestrzeni teleinformatycznej do zdobywania informacji niejawnych. Proceder ten jest z reguły zdecydowanie prostszy, bezpieczniejszy i tańszy niż tradycyjne formy szpiegostwa. Co prawda, nigdy w pełni nie będzie w stanie zastąpić działań odpowiednich służb wywiadowczych w terenie, jednak w wielu przypadkach może ułatwić zdobycie tajnych informacji, które współcześnie są traktowane jako wartościowy towar. To właśnie z tego wynika stale rosnąca popularność tego typu działalności w cyberprzestrzeni. W ciągu ostatnich dwóch dekad można było bowiem zaobserwować stale rosnącą liczbę włamań komputerowych, których głównym celem było zdobycie zastrzeżonych danych. Wykształcił się proceder szeroko zakrojonych operacji, których celem stały się zachodnie korporacje, instytuty badawcze lub instytucje rządowe. Głównym ich powodem jest chęć uzyskania zaawansowanych technologii. Należy zauważyć, iż w takim ujęciu fenomen ten nie nosi znamion działalności *stricte* przestępczej. Poziom skomplikowania i zaawansowania wielu operacji wywiadowczych w sieci daje bowiem podstawy do stwierdzenia, iż coraz częściej cyberprzestrzeń jest wykorzystywana w ten sposób przez służby państwowe. Wiele wskazuje również na fakt, iż częstokroć rządy zatrudniają różnego rodzaju podmioty pozapaństwowe do prowadzenia tego typu akcji[77].

Warto przytoczyć tu kilka przykładów, które dowodzą rosnącego znaczenia tego procederu. Pierwsze włamania mające na celu zdobycie poufnych informacji zdarzały się już w latach 80. XX wieku. Jednak to dopiero na początku XXI wieku

[76] Zob. *The Use of the Internet for Terrorist Purposes*, United Nations Office on Drugs and Crime, New York 2012.
[77] Zob. *Exposing One of China's Cyber Espionage Units*, Mandiant Report 2012.

cyberszpiegostwo stało się jedną z najpopularniejszych form szkodliwej działalności w sieci. W 2003 roku w wyniku operacji *Titan Rain* łupem chińskiej grupy padły serwery należące do amerykańskiego rządu, korporacji oraz instytucji badawczych. Udało jej się uzyskać dane dotyczące m.in. planów i technologii NASA, Lockheed-Martin czy Redstone Arsenal, w tym projektu *Joint Strike Fighter*[78]. W kolejnych latach doszło do całej serii doskonale zorganizowanych i przeprowadzonych włamań do komputerów i sieci należących do instytucji rządowych, biznesowych i naukowych w USA oraz Europie Zachodniej. W 2007 roku chińscy specjaliści wzięli na cel serwery amerykańskiego Departamentu Handlu, Obrony i Stanu. W 2008 roku wyprowadzono tajne dane z wewnętrznej sieci amerykańskiej armii, wykorzystując do tego metody inżynierii społecznej oraz błędy personelu[79]. W 2009 roku natomiast kanadyjski zespół „Information Warfare Monitor" odkrył chińską grupę cyberszpiegowską *GhostNet*, która stała za włamaniami w 103 krajach, w tym m.in. w Niemczech, Pakistanie, Tajlandii czy na Cyprze. Co ciekawe, objęły one również komputery należące do tybetańskich opozycjonistów. O sprawności i wysokim zaawansowaniu ataków świadczył fakt, iż do zbierania informacji wykorzystywano nawet zainstalowane w komputerach kamery internetowe[80].

Jak wspomniano wcześniej, poziom zorganizowania i dobór celów wielu operacji cyberszpiegowskich przeciwko państwom zachodnim często bywa zbyt wysoki, by sądzić, iż stoją za nimi wyłącznie grupy przestępcze. W tym kontekście warto zwrócić uwagę na jeszcze dwa incydenty. Po pierwsze, jak wspomniano już wcześniej, władze amerykańskie skrytykowały bezczynność Pekinu po atakach na korporację Google[81]. Po drugie, w lutym 2013 roku zaprezentowano raport korporacji Mandiant, który został poświęcony chińskiej aktywności cyberszpiegowskiej w USA. Według niego, za wieloma incydentami stoi tajna chińska jednostka 61398 z siedzibą

[78] B. Graham, *Hackers Attack Via Chinese Web Sites*, „Washington Post", 28.08.2005; M. Lakomy, *Cyberwojna…*, s. 144-148.
[79] T. Greene, *Pentagon officials details U.S. military net attack*, 25.08.2010, http://www.networkworld.com/news/2010/082510-pentagon-net-hack.html, 20.02.2013.
[80] M. Lakomy, *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw…*, s. 62-63.
[81] *Secretary of State Hillary Clinton says China's Cyber Attacks Must Face Consequences*, Government Security, http://www.governmentsecurity.org/latest-security-news/secretary-of-state-hillary-clinton-says-chinas-cyber-attacks-must-face-consequences.html, 18.02.2013.

w Szanghaju, funkcjonująca w ramach sił zbrojnych ChRL. Ma ona zatrudniać tysiące specjalistów, których zadaniem jest zdobywanie poufnych informacji i technologii z serwerów należących do zachodnich instytucji państwowych, naukowych oraz korporacji. Zasadniczym celem tego typu operacji jest oczywiście zmniejszenie technologicznej przepaści między Chinami a Stanami Zjednoczonymi, szczególnie w wymiarze militarnymi gospodarczym. Władze w Pekinie odrzuciły te oskarżenia, dodając przy tym, iż nie istnieje ustalona w wymiarze międzynarodowym definicja „ataków hakerskich" oraz brakuje podstaw prawnych do ich odróżnienia od „rutynowego zbierania informacji" w sieci[82]. Potwierdziło to tym samym potrzebę opracowania odpowiedniej umowy międzynarodowej, która uregulowałaby wskazane przez ChRL wątpliwości.

Na tej podstawie cyberszpiegostwo można więc określić jako pozyskiwanie niejawnych danych i informacji przy wykorzystaniu potencjału sieci teleinformatycznych przez państwa lub powiązane z nimi podmioty. Z perspektywy analizy zagrożeń dla bezpieczeństwa teleinformatycznego posiada ono kilka istotnych cech. Po pierwsze, najpoważniejsze wyzwania dla bezpieczeństwa poufnych informacji, np. w sieciach wojskowych, stanowią zatrudnione przez państwa grupy przestępcze, lub jak wspomniano wyżej, wyspecjalizowane jednostki wywiadowcze lub wojskowe. Po drugie, cyberszpiegostwo posługuje się innym zestawem metod niż np. cyberterroryzm. Wykorzystuje się przede wszystkim techniki zapewniające niskie prawdopodobieństwo wykrycia, w tym np. wyspecjalizowane oprogramowanie (np. robaki, konie trojańskie, *keyloggery*), *phishing* czy techniki z zakresu inżynierii społecznej. Częstokroć bowiem to właśnie czynnik ludzki jest najsłabszym elementem zabezpieczeń komputerowych[83]. Po trzecie wreszcie, celem tego procederu nie jest wyrządzenie bezpośrednich szkód, lecz uzyskanie poufnych informacji, których wyciek

[82] *Exposing One of China's Cyber Espionage Units*, Mandiant Report 2012; *Chiny odrzucają oskarżenia o hakerskie ataki w USA*, Wirtualna Polska, 20.02.2013, http://konflikty.wp.pl/kat,1356,title,Chiny-odrzucaja-oskarzenia-o-hakerskie-ataki-w-USA,wid,15348738,wiadomosc.html, 20.02.2013.

[83] *Cyber Espionage. The harsh reality of advanced security threats*, Deloitte, Center for Security & Privacy Solutions, 2011, s. 7.

może stanowić zasadnicze zagrożenie dla bezpieczeństwa narodowego i międzynarodowego.

Działania zbrojne w cyberprzestrzeni

Jak wspomniano wyżej, już w połowie lat 90. XX wieku pojawiły się pierwsze głosy klasyfikujące cyberprzestrzeń jako kolejny teatr wojny[84]. W styczniu 1996 roku ośrodek badawczy RAND ogłosił słynny raport, w którym stwierdzono możliwość prowadzenia „strategicznej wojny w cyberprzestrzeni"[85]. Wraz z dynamicznym rozwojem Internetu oraz procesem digitalizacji niemal wszystkich dziedzin życia wizje te stopniowo stawały się coraz bardziej realne. Pojawienie się wielu nowych form szkodliwej działalności w cyberprzestrzeni na przełomie XX i XXI wieku postawiło pytanie, czy sieć może być wykorzystana do walki zbrojnej. Była to kwestia o tyle istotna, iż obejmowała szereg poważnych dylematów, w tym m.in.: niematerialną specyfikę sygnału elektronicznego w kontekście prawa wojny, prawa międzynarodowego czy najważniejszych umów (np. Karty Narodów Zjednoczonych), rzeczywisty potencjał militarny cyberprzestrzeni czy samą istotę pojęcia walki zbrojnej i wojny.

Stosunkowo szybko okazało się, iż ataki teleinformatyczne mogą być naturalnym zjawiskiem towarzyszącym konfliktom zbrojnym, tak w wymiarze wewnętrznym, jak i międzynarodowym. Do pierwszych, bardzo ograniczonych prób wykorzystania cyberprzestrzeni w konflikcie zbrojnym, doszło w 1991 roku w trakcie operacji „Pustynna Burza". Bardzo proste włamania komputerowe towarzyszyły również obu wojnom w Czeczenii[86]. Cyberprzestrzeń stała się również polem starć serbskich i natowskich informatyków w 1999 roku w trakcie interwencji Sojuszu Północnoatlantyckiego w Kosowie. Z jednej strony specjaliści Sojuszu dokonali ograniczonych ataków teleinformatycznych przeciwko reżimowi w Belgradzie. Jak

[84] J.A. Warden, *Enemy as a System*, „Air power Journal", 1995, nr 9, s. 40-55; P. Sienkiewicz, H. Świeboda, *Niebezpieczna przestrzeń cybernetyczna*, „Transformacje", 2006, nr 1-4, t. 47-50, s. 58.
[85] *Strategic War…in Cyberspace*, „RAND Research Brief", styczeń 1996; R.C. Molander, A.S. Riddile, P.A. Wilson, *Strategic Information Warfare: A New Face of War*, Santa Monica 1996.
[86] F. Schreier, *On Cyberwarfare*, „DCAF Horizon 2015 Working Paper", vol. 7, s. 107.

jednak słusznie zauważył Julian Borger z „The Guardian", Pentagon nie zdecydował się, mimo posiadanego potencjału, na operację na pełną skalę w cyberprzestrzeni. Obawiano się nie tylko prawnych implikacji tego typu działań, lecz także ujawnienia swoich rzeczywistych zdolności w tej dziedzinie[87]. Z drugiej strony serii odwetowych ataków na serwery należące do NATO dokonali hakerzy serbscy oraz chińscy[88]. Po raz pierwszy na większą skalę ofensywne działania w cyberprzestrzeni towarzyszyły więc konwencjonalnemu konfliktowi zbrojnemu. W późniejszym okresie tendencja ta jedynie się potwierdziła. Ograniczone ataki w cyberprzestrzeni miały miejsce w czasie amerykańskiej interwencji w Iraku w 2003 roku. Jednak i w tym wypadku Biały Dom nie zdecydował się na wykorzystanie swego pełnego potencjału do zaatakowania irackiej infrastruktury krytycznej, z obawy przed trudnymi do przewidzenia konsekwencjami prawnymi oraz niepotrzebnym ujawnieniem technik włamań przyszłym przeciwnikom[89].

Przełom w dyskusji na ten temat nastąpił jednak dopiero w 2007 roku. Jak wspomniano już wcześniej, w kwietniu 2007 roku doszło do masowych cyberataków na Estonię, które zostały określone mianem „pierwszej cyberwojny", choć nie miały charakteru militarnego. Przyczyniły się one jednak do dostrzeżenia tej problematyki przez międzynarodową opinię publiczną. Już w kilka miesięcy później, we wrześniu 2007 roku, doszło do modelowego wykorzystania cyberprzestrzeni jako kolejnego teatru wojny. Wówczas doszło bowiem do izraelskiej operacji *Orchard*, której celem było zniszczenie syryjskiego ośrodka badań nad bronią atomową. Aby zapewnić sukces nalotu, służby wywiadowcze Izraela zainfekowały syryjski system obrony powietrznej wirusem komputerowym. W efekcie oślepiono radary sił zbrojnych Syrii, które nie były w stanie wykryć wlatujących w jej przestrzeń powietrzną izraelskich samolotów[90]. Wydarzenie to stało się symbolem rosnącego potencjału

[87] J. Borger, *Pentagon kept the lid on cyberwar in Kosovo*, „The Guardian", 09.11.1999.
[88] S. Myrli, *NATO and Cyber Defence*, NATO Parliamentary Assembly, 173 DSCFC 09 E BIS; J. Carr, *Real Cyber Warfare: Carr's Top Five Picks*, „Forbes", 02.04.2011, http://www.forbes.com/sites/jeffreycarr/2011/02/04/real-cyber-warfare-carrs-top-five-picks/, 20.02.2013.
[89] C.R. Smith, *Cyber War Against Iraq*, Newsmax.com, 13.03.2003, http://archive.newsmax.com/archives/articles/2003/3/12/134712.shtml, 20.02.2013.
[90] Zob. T. Rid, *Cyber War Will Not Take Place*, „Journal of Strategic Studies", 2012, nr 1.

cyberprzestrzeni jako kolejnego teatru działań zbrojnych. Po raz pierwszy, i jak dotąd jedyny, na taką skalę udało się bowiem z sukcesem połączyć ataki teleinformatyczne z konwencjonalnym uderzeniem zbrojnym, *de facto* paraliżując jeden z kluczowych elementów systemu obronnego reżimu Baszara al Assada.

W tym kontekście warto także wspomnieć o wojnie gruzińsko-rosyjskiej w sierpniu 2008 roku. Federacja Rosyjska na atak gruziński zareagowała bowiem nie tylko konwencjonalnymi siłami zbrojnymi, lecz także aktywnymi działaniami w cyberprzestrzeni. Głównie dzięki wykorzystaniu sieci *botnet* i metod DDoS, Rosjanom szybko udało się sparaliżować najważniejsze witryny internetowe należące do rządu Gruzji (np. civil.ge). Zaatakowano również wiele popularnych stron komercyjnych, informacyjnych oraz naukowych. Według niektórych źródeł, ataki objęły także gruzińską sieć telekomunikacyjną. Spotkały się onez bardzo ograniczoną odpowiedzią specjalistów gruzińskich, którzy zablokowali strony należące m.in. do agencji prasowej RIA Nowosti czy niektórych telewizji. W odróżnieniu od operacji *Orchard* działania rosyjskich specjalistów nie miały bezpośredniego wpływu na przebieg konfliktu zbrojnego. Miały natomiast zasadnicze znaczenie z punktu widzenia walki informacyjnej i propagandy wojennej, zapewniając Kremlowi znaczącą przewagę nad rządem w Tbilisi. Został on bowiem częściowo pozbawiony możliwości prezentowania swojego stanowiska w trakcie konfliktu. Podobnie jak w przypadku Kosowa, Iraku czy Estonii, również i w tym wypadku nie doszło jednak do działań, które stanowiłyby bezpośrednie zagrożenie dla infrastruktury krytycznej państwa[91].

W świetle powyższych wydarzeń w literaturze specjalistycznej używa się z reguły dwóch grup pojęć. Z jednej strony wskazuje się na coraz większą możliwość wykorzystania cyberprzestrzeni jako kolejnego teatru walki zbrojnej, co udowodniła operacja Izraela przeciwko Syrii w 2007 roku. Warto tu przytoczyć opinię Alexisa Bautzmanna z francuskiego Centre d'Analyse et de Prévision des Risques Internationaux (CAPRI), według którego na przełomie pierwszej i drugiej dekady XXI wieku należy ponownie przemyśleć znaczenie bezpieczeństwa oraz narodowej

[91] M. Lakomy, *Geopolityczne następstwa wojny gruzińsko-rosyjskiej*, „Przegląd Zachodni", 2010, nr 4, s. 185; D. Hollis, *Cyberwar Case Study: Georgia 2008*, „Small Arms Journal", 06.01.2011.

suwerenności w kontekście rozwoju technologii ICT. Można bowiem zauważyć rosnącą militaryzację Internetu, przejawiającą się powstawaniem jednostek wojskowych, wyspecjalizowanych w walce w środowisku teleinformatycznym. Działania w tym kierunku podjęły nie tylko Stany Zjednoczone (dowództwo USCYBERCOM), ale także m.in. Wielka Brytania czy Chiny. Co ciekawe, plany stworzenia osobnego rodzaju wojsk informacyjnych sformułowała również Polska. Przy czym, jak zauważył Alessandro Bufalini, rozwój cyberprzestrzeni w tym kierunku rodzi szereg poważnych wyzwań nie tylko natury wojskowej i politycznej, ale także prawnej[92]. Z drugiej jednak strony, np. w przypadku wojny w Gruzji, często wykorzystuje się termin walki informacyjnej. Piotr Sienkiewicz i Halina Świeboda wyróżnili następujące jej cechy: celem jest uzyskanie przewagi informacyjnej nad przeciwnikiem, przeciwnik jest „niewidzialny", terenem działań jest cyberprzestrzeń, podstawową formą walki są cyberataki, obiektem ataków szczególnej wagi jest infrastruktura krytyczna, a istotnym czynnikiem pozostaje czas. Ponadto, jak zauważyli, walka informacyjna była od zawsze istotnym aspektem działań zbrojnych[93].

Mając to na uwadze, należy jednak stwierdzić, iż termin „informacyjny" (np. walka informacyjna czy bezpieczeństwo informacyjne), wykorzystywany tak w polskiej, jak i zagranicznej literaturze oraz w wielu oficjalnych dokumentach (np. Stanów Zjednoczonych), może niekiedy budzić pewne wątpliwości natury interpretacyjnej. Zgodnie z interpretacją kategorii bezpieczeństwa informacyjnego przytoczoną przez Krzysztofa Liedela, zwraca się szczególną uwagę na ochronę informacji przed niepożądanym *ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania*. W tym rozumieniu informacja posiada m.in. takie funkcje jak: decyzyjna, modelowania (opisywania), sterująca (systemy informatyczne), rozwoju wiedzy, kapitałotwórcza czy kulturotwórcza[94]. Powstaje

[92] A. Bautzmann, *Le cyberespace, nouveau champ de bataille?*, "Diplomatie. Affaires Stratégiques et Relations Internationales", luty-marzec 2012, s. 80-81 ; *Wizja Sił Zbrojnych RP – 2030*, Warszawa 2008, s. 23; A. Bufalini, *Les cyber-guerres a la lumière des regles internationales sur l'interdiction du recours à la force*, [w :] M. Arcari, L. Balmond (red.), *La gouvernance globale face aux défis de la sécurité collective*, Napoli 2012, s. 92.

[93] P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*, [w:] M. Madej, M. Terlikowski (red.), dz. cyt., s. 84.

[94] K. Liedel, *Bezpieczeństwo informacyjne państwa*, [w:] K. Liedel (red.), dz. cyt. , s. 53-56.

jednak zasadnicze pytanie, czy walka informacyjna obejmowałaby wszystkie aspekty szkodliwego wykorzystania cyberprzestrzeni. Istnieje bowiem wątpliwość, czy ataki teleinformatyczne, których rezultatem byłyby szkody fizyczne, materialne można zakwalifikować jako manipulację informacją. W tym kontekście, aby uniknąć tego problemu, walkę informacyjną często definiuje się bardzo szeroko, z reguły jako konflikt, w którym *informacja jest jednocześnie zasobem, obiektem ataku i bronią, a zarazem obejmuje on fizyczne niszczenie infrastruktury, wykorzystywanej przez przeciwnika do działań operacyjnych*[95]. W tym rozumieniu obejmowałaby ona jednak w zasadzie wszystkie kategorie wyzwań pojawiających się w cyberprzestrzeni. Takie rozwiązanie, jakkolwiek z jednego punktu widzenia uzasadnione, mogłoby jednocześnie zamazać odmienne cechy poszczególnych form zagrożeń teleinformatycznych dla bezpieczeństwa państw oraz, z pewnej perspektywy, wykraczać poza definicję słowa „informacja"[96]. Warto w tym kontekście zauważyć, iż w Wizji Sił Zbrojnych RP – 2030, opracowanej przez Departament Transformacji Ministerstwa Obrony Narodowej RP, wymiar teleinformatyczny (cyberprzestrzenny) oraz sferę informacyjną potraktowano jako obszary nieco odmienne. Stwierdzono tam bowiem: *Obok tradycyjnych, fizycznych geoprzestrzeni jak ląd, morze, przestrzeń powietrzna (powietrzno-kosmiczna) do prowadzenia walki będą wykorzystywane sfery pozbawione parametrów geograficznych, niemierzalne i nieograniczone takie jak wirtualna przestrzeń cybernetyczna i sfera informacyjna. Obszary te będą się na siebie nakładać i wzajemnie uzupełniać tworząc jednolitą, nieznaną do tej pory przestrzeń walki sił zbrojnych*. W punkcie 44. dokumentu dodano również, iż w przyszłości operacje sił zbrojnych będą miały charakter operacji połączonych, obejmujących m.in. siły realizujące zadania *w cyberprzestrzeni oraz w sferze informacyjnej*[97]. Na tej podstawie warto przywołać opinię eksperta Geneva Center for the Democratic Control of ArmedForces, Freda Shreiera, który słusznie wskazał, iż walka informacyjna jest pojęciem zdecydowanie szerszym niż walka

[95] Zob. P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa…*, s. 80.
[96] Np. A. Webster określił informację jako wiedzę przekazywaną *przez innych ludzi bądź uzyskiwaną przez studia, obserwacje, badania*. Za K. Liedel, *Bezpieczeństwo informacyjne państwa*,s. 50.
[97] *Wizja Sił Zbrojnych RP – 2030,*Warszawa 2008, s. 13-15.

w cyberprzestrzeni, obejmuje nie tylko działania dokonywane za pomocą sieci teleinformatycznych, ale także działania psychologiczne, walkę elektroniczną czy wprowadzanie przeciwnika w błąd[98].

Na podstawie powyższych rozważań można więc stwierdzić, iż militarne zastosowanie cyberprzestrzeni obejmuje różnorodne formy i metody cyberataków[99], wymierzone w obiekty o żywotnym znaczeniu dla bezpieczeństwa państwa, w tym m.in. elementy infrastruktury krytycznej czy sieci, serwery i systemy wojskowe. Głównym celem tego typu działań jest realizacja określonego zadania o charakterze militarnym, mającym doniosłe skutki w wymiarze fizycznym (zniszczenia materialne), w sferze informacyjnej[100] lub w szeroko rozumianej cyberprzestrzeni. Militarne zastosowanie sieci teleinformatycznych przejawia się więc takimi atakami, które w zasadniczym stopniu ułatwiłyby lub zastąpiły konwencjonalne działania na innych obszarach konfliktu lub operacji wojskowej. Ponadto należy podkreślić, iż ta forma zagrożeń teleinformatycznych jest właściwa tylko tym państwom, które dysponują odpowiednim potencjałem oraz posiadają adekwatną motywację[101].

Zakończenie

Incydenty w cyberprzestrzeni od lat stanowią rosnące zagrożenie dla bezpieczeństwa państw. Oprócz szeregu dylematów natury czysto technicznej wiążą

[98] F. Schreier, *On Cyberwarfare*…, s. 19-21.

[99] Mogą to być np. ataki DDoS za pomocą sieci *botnet* czy wyspecjalizowane złośliwe oprogramowanie.

[100] Celem może być, np. uzyskanie przewagi informacyjnej nad przeciwnikiem, jak również zablokowanie możliwości pozyskiwania lub przesyłania przez niego informacji. Tego typu działania podjęli rosyjscy specjaliści w trakcie wojny gruzińsko-rosyjskiej.

[101] Artykuł pomija fenomen cyberwojny, który jest w ostatnich latach często omawiany w literaturze specjalistycznej. Należy zauważyć, iż nie ma zgody badaczy co do jednoznacznego rozumienia tego terminu, jego zasadności oraz najważniejszych cech. Według jednych, oznacza on wykorzystanie cyberprzestrzeni jako piątego teatru wojny. Inni postrzegają go jako neologizm zawierający się w szeroko rozumianej wojnie ery informacyjnej. W opinii Autora natomiast, obejmuje on działalność państw o charakterze cyberterrorystycznym, cyberszpiegowskim oraz militarne wykorzystanie sieci teleinformatycznych. Bez względu na te różnice nie ulega wątpliwości, iż cyberwojna jest zjawiskiem wiążącym się z szeregiem poważnych dylematów natury politycznej, prawnej i militarnej, przez co zasadnym jest omówienie tej problematyki w osobnym opracowaniu. Zob.: P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, [w:] L.H. Haber (red.), *Społeczeństwo informacyjne – wizja czy rzeczywistość?*, Kraków 2003; P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*, [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009; K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe", 2011, nr 1; M. Lakomy, *Cyberwojna jako rzeczywistość XXI wieku*, „Stosunki Międzynarodowe – International Relations", 2011, nr 3-4.

się z nimi również bardzo poważne wątpliwości natury politycznej i prawnej. Jak wspomniano wyżej, z perspektywy nauk społecznych sfera bezpieczeństwa teleinformatycznego[102] jest bowiem obszarem wysoce skomplikowanym, niejednoznacznym i wielowymiarowym. Mimo niemal trzech dekad dyskusji na ten temat nadal nie przygotowano skutecznych i ogólnie przyjętych rozwiązań dotyczących politycznej i prawnej oceny skutków najpoważniejszych cyberataków oraz właściwej nań odpowiedzi. Ze względu na odmienne podejście poszczególnych państw nie opracowano międzynarodowego traktatu, który uregulowałby wszystkie wątpliwości związane z ofensywnym, militarnym wykorzystaniem przestrzeni teleinformatycznej, aktami cyberszpiegostwa lub cyberterroryzmu. Brak jest także powszechnej zgody co do interpretacji najpoważniejszych incydentów komputerowych z punktu widzenia wykładni istniejących już przepisów prawa międzynarodowego, czy takich kategorii jak suwerenność i integralność terytorialna. W wymiarze wewnętrznym natomiast niewiele państw dotychczas jasno określiło, w jaki sposób będą reagować na najpoważniejsze zagrożenia pojawiające się w cyberprzestrzeni[103].

Na tym tle opracowanie spójnego aparatu pojęciowego, który byłby właściwy zarówno dla nauk technicznych, jak i społecznych, jest rzeczą mało prawdopodobną. Każdy z tych obszarów wiedzy skupia się bowiem na odmiennych zagadnieniach. W tym kontekście, zaprezentowana typologia zagrożeń teleinformatycznych jest próbą uchwycenia ich najistotniejszych i zarazem najbardziej podstawowych cech z perspektywy politologicznej. Może ona stanowić przyczynek do sformułowania szerszej, kompleksowej i interdyscyplinarnej klasyfikacji zagrożeń w cyberprzestrzeni, która uwzględniłaby nie tylko najistotniejsze uwarunkowania techniczne, ale także ich źródła, stopień organizacji, motywacje i cele oraz obszar działań. Wydaje się, iż tylko

[102] Czyli zestawu zagadnień odpowiednio zawężonych w stosunku do kategorii bezpieczeństwa informacyjnego, obejmujących wyłącznie sferę funkcjonowania cyberprzestrzeni.

[103] Dotychczas najbardziej klarowne stanowisko zajęły Stany Zjednoczone, które jednoznacznie zarezerwowały sobie prawo do reagowania siłą militarną na najpoważniejsze ataki w cyberprzestrzeni. Zob. D. Alexander, *U.S. reserves right to meet cyber attack with force*, Reuters, 15.11.2011, http://www.reuters.com/article/2011/11/16/us-usa-defense-cybersecurity-idUSTRE7AF02Y20111116, 03.03.2013.

tak szerokie i wieloaspektowe podejście pozwoli przyczynić się do lepszej percepcji zagrożeń teleinformatycznych w naukach społecznych, a przez to do wypracowania skuteczniejszych rozwiązań prawnych i politycznych tak w wymiarze wewnętrznym, jak i międzynarodowym.

Tabela 1. Cechy najpoważniejszych zagrożeń teleinformatycznych.

	Źródła	Stopień organizacji	Motywacje	Cele	Stopień zagrożenia dla bezpieczeństwa państwa	Wybrane konsekwencje polityczne	Wyzwaniadla prawa międzynarodowego
Haking	Jednostki Grupy	Niski	Indywidualne	Rozwój własnych umiejętności	Bardzo niski	Brak	Brak
Haktywizm	Jednostki Grupy	Niski z pewnymi elementami koordynacji na poziomie narodowym lub międzynarodowym	Polityczne, społeczne, uniwersalne	Promocja określonych postaw, wartości lub ideologii w przestrzeni publicznej	Bardzo niski	Czasami niewielkie straty wizerunkowe dla rządu	Brak
„Haktywizm patriotyczny”	Jednostki Grupy	Niski z elementami koordynacji na poziomie narodowym	Polityczne, Patriotyczne (narodowe)	Promocja lub obrona określonych postaw, idei politycznych oraz wartości, związanych z państwem pochodzenia. Zwalczanie innych, narodowych grup haktywistycznych lub ataki na instytucje rządowe i pozarządowe	Uzależniony od obiektu ataku. Z reguły są to strony internetowe, jednak łupem „cyberwojowników” mogą paść również elementy infrastruktury krytycznej	Wpisuje się w napięcia lub konflikty wewnętrzne i międzynarodowe. Działalność ta może być uznana za atak o charakterze zbrojnym. Pogarszają one stosunki dwustronne	Brak wykładni dotyczącej interpretacji takich aktów z perspektywy np. integralności terytorialnej, suwerenności lub definicji działań zbrojnych.
Cyberprzestępczość	Jednostki Grupy	Niski z pewnymi elementami koordynacji na poziomie narodowym lub międzynarodowym	Zróżnicowane, obejmujące np. osiągnięcie korzyści osobistych, materialnych	Uzyskanie korzyści osobistych dzięki wykorzystaniu cyberprzestrzeni	Pośredni, uciążliwy przede wszystkim z punktu widzenia rozwoju gospodarczego i społecznego	Z reguły brak. Cyberprzestępczość w wymiarze międzynarodowym może powodować jednak wzrost napięcia między państwami	Np. pominięcie tych kwestii z perspektywy międzynarodowej współpracy w zakresie zwalczania przestępczości zorganizowanej
Cyberterroryzm	Organizacje terrorystyczne i sympatyzujące z nimi grupy ekstremistów Państwa	Wysoki stopień organizacji i koordynacji	Polityczne	Dokonanie poważnych zniszczeń (materialnych lub niematerialnych), osiągnięcie założonego efektu psychologicznego i promocja własnej ideologii lub postulatów	Wysoki – głównym celem są elementy infrastruktury krytycznej i sieci oraz serwery wojskowe.	Może się wpisywać w napięcia, kryzysy i konflikty międzynarodowe. Może być również uznany za akt o charakterze militarnym	Brak wykładni dotyczącej interpretacji takich aktów z perspektywy, np. integralności terytorialnej, suwerenności lub definicji działań zbrojnych
Cyberszpiegostwo	Państwa i powiązane z nimi podmioty poza-państwowe	Wysoki stopień organizacji i koordynacji	Polityczne Gospodarcze	Uzyskanie niejawnych danych w różnych celach (np. rywalizacja wywiadowcza, technologiczna)	Wysoki – łupem mogą paść dane o żywotnym znaczeniu dla bezpieczeństwa państwa, w tym np. zaawansowane technologie, informacje wywiadowcze	Prowadzi do pogorszenia stosunków dwustronnych (przykład USA-Chiny). Stanowi element rywalizacji państw w cyberprzestrzeni	Brak międzynarodowej definicji, która określiłaby, czym jest działalność cyberszpiegowska oraz z jakimi wiąże się konsekwencjami (*casus* Chin)
Militarne zastosowanie cyberprzestrzeni	Państwa	Bardzo wysoki stopień organizacji i koordynacji	Polityczne Wojskowe	Realizacja określonego celu o charakterze militarnym (np. zniszczenie ośrodka badań nad bronią atomową – operacja *Orchard*)	Bardzo wysoki – wiąże się z operacjami o charakterze zbrojnym. Może skutkować zniszczeniami fizycznymi i śmiercią obywateli	Wpisuje się w napięcia, kryzysy i konflikty międzynarodowe. Stanowi akt o charakterze zbrojnym	Brak obowiązującej interpretacji takich działań w świetle, np. Karty Narodów Zjednoczonych czy prawa wojny

Źródło: opracowanie własne.

dr Miron Lakomy – adiunkt w Zakładzie Stosunków Międzynarodowych Instytutu Nauk Politycznych i Dziennikarstwa Uniwersytetu Śląskiego

Abstrakt

Artykuł jest próbą opracowania podstawowej typologii najpoważniejszych zagrożeń dla bezpieczeństwa teleinformatycznego państw z perspektywy nauk społecznych. Biorąc pod uwagę różnorodny stopień organizacji oraz odmienność form, a więc uwarunkowania, motywacje, metody i cele stawiane sobie przez działające w cyberprzestrzeni podmioty, wyróżniono następujące wyzwania dla bezpieczeństwa państw: haking, haktywizm, „haktywizm patriotyczny", wąsko rozumianą cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, militarne wykorzystanie cyberprzestrzeni. Źródłami tych form zagrożeń są zarówno podmioty państwowe, jak i pozapaństwowe. Szczególne znaczenie mają te wyzwania, które wiążą się z działalnością służb państwowych. Rodzą one bowiem różnorodne kontrowersje natury politycznej i prawnej. Jest to tym bardziej widoczne, iż do dziś nie ma zgody społeczności międzynarodowej co do sposobu interpretacji najpoważniejszych ataków teleinformatycznych. W tym kontekście wydaje się, iż zaproponowane w artykule szerokie i wieloaspektowe podejście pozwoli przyczynić się do lepszej percepcji zagrożeń dla cyberbezpieczeństwa w naukach społecznych, a przez to do wypracowania skuteczniejszych rozwiązań prawnych i politycznych tak w wymiarze wewnętrznym, jak i międzynarodowym.

CHALLENGES FOR THE CYBER SECURITY OF STATES – A TYPOLOGY ATTEMPT

Abstract

This article is an attempt to create a precise typology and definitions of cyber threats for the national security from the social sciences perspective. The analysis included multiple important cyber attack features, such as organization, technical determinants, motivations, techniques, tools, goals or political consequences. The

article distinguished several important cyber threat forms: hacking, hacktivism, patriot hacktivism, cyber crime, cyber terrorism, cyber espionage or cyber warfare. Sources of these challenges are usually very diverse, ranging from amateur individuals up to states and international organizations. Activity of states in cyberspace usually pose the gravest threats for the national and international security. It is not only due to their high complexity, but also grave political, legal and military consequences. On this basis, it is crucial to underline that nowadays there is no consensus within the international community when it comes to cyber security solutions. Typology and definitions presented in this article may contribute to a better understanding of major cyber challenges, as well as to an elaboration of more precise and efficient cyber defense mechanisms on the national and international level.