

prof. dr hab. inż. Henryk Wyrębek
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych
ORCID: 0000-0001-9801-6905

dr Waldemar Perdion

ZAGROŻENIA INFRASTRUKTURY KRYTYCZNEJ ZE STRONY ATAKÓW CYBERTERRORYSTYCZNYCH

THREATS TO CRITICAL INFRASTRUCTURE FROM CYBERTERRORIST ATTACKS

Streszczenie

W opracowaniu pod tytułem *Zagrożenia infrastruktury krytycznej ze strony ataków cyberterrorystycznych*, autorzy przedstawiają problematykę zagrożeń infrastruktury krytycznej. Przedstawiono jak ważne zabezpieczenie obiektów, instalacji i usług zapewniających zaspokojenie tych podstawowych potrzeb ludności, w oparciu o systemy infrastruktury krytycznej, które ma zasadnicze znaczenie w kształtowaniu należytego poziomu bezpieczeństwa obywateli. Systemy infrastruktury krytycznej **są** narażone na nieustanne zakłócenia i awarie, w tym również na ataki terrorystyczne. Autorzy podkreślają, że bardzo duże znaczenie obiektów i systemów infrastruktury krytycznej dla bezpieczeństwa państwa wynika z ich strategicznego znaczenia dla podtrzymania niezakłóconego funkcjonowania państwa w warunkach współczesnych zagrożeń. Dlatego, niezmiernie ważne jest przedsięwzięcie odpowiednich kroków, mających na celu zabezpieczenie tych elementów poprzez odpowiednią ich ochronę.

Słowa kluczowe: atak, cyberterroryzm, obiekty, systemy, zakłócenia

Abstract

In the study entitled *Threats to critical infrastructure from cyberterrorist attacks*, the authors present the issues of threats to critical infrastructure. It was presented how important the protection of facilities, installations and services ensuring the satisfaction of these basic needs of the population, based on the systems of critical infrastructure, which is essential in shaping the appropriate level of security for citizens. Critical infrastructure systems are exposed to constant disruptions and failures, including terrorist attacks. The authors emphasize that the importance of objects and systems of critical infrastructure for state security results from their strategic importance for maintaining the uninterrupted

functioning of the state in the conditions of contemporary threats. Therefore, it is extremely important to take appropriate steps to protect these elements by properly protecting them.

Keywords: attack, cyberterrorism, objects, systems, disruptions

Wstęp

Dla sprawnego funkcjonowania gospodarki nowoczesnych społeczeństw, opartej na wysoko rozwiniętej technice, niezbędne jest niezakłócone działanie różnorodnych jej elementów (zaopatrzenie w energię, wodę, rozwinięte i szeroko dostępne sieci telekomunikacyjne i komputerowe, sprawnie działający transport). Zabezpieczenie obiektów, instalacji i usług zapewniających zaspokojenie tych podstawowych potrzeb społeczeństwa, w oparciu o systemy określone mianem infrastruktury krytycznej, ma zasadnicze znaczenie w kształtowaniu należytego poziomu bezpieczeństwa obywateli. Te obszary działalności narażone są na nieustanne zakłócenia i awarie, w tym także ataki terrorystyczne. Rosnące znaczenie obiektów i systemów infrastruktury krytycznej dla bezpieczeństwa państwa wynika z ich strategicznego znaczenia dla podtrzymania niezakłóconego funkcjonowania państwa w warunkach współczesnych zagrożeń. Dlatego, niezmiernie ważne jest przedsięwzięcie odpowiednich kroków, mających na celu zabezpieczenie tych elementów poprzez odpowiednią ich ochronę. Pozwoli to na zapewnienie ciągłości działania i integralności infrastruktury krytycznej oraz szybkiego odtwarzania na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie¹.

Ogólna charakterystyka infrastruktury krytycznej

Infrastruktura krytyczna (IK) to rzeczywiste i cybernetyczne systemy (obiekty, urządzenia bądź instalacje) niezbędne do minimalnego funkcjonowania gospodarki i państwa. Nie każdy strategiczny obiekt należy do infrastruktury krytycznej (IK). O tym czy dany zalicza się do IK decydują szczegółowe kryteria zapisane w niejawnym załączniku do Narodowego Programu Infrastruktury Krytycznej².

Infrastruktura krytyczna to, według ustawy o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r., systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania administracji publicznej, a także instytucji i przedsiębiorców³. Zdobycze nowoczesnej technologii stały się istotnym elementem egzystencji człowieka. Są też niezbędnym narzędziem wspierającym systemy

¹ M. Żuber, *Infrastruktura krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego*, [w:] Rocznik Bezpieczeństwa Międzynarodowego 2014 | 8 | 2 |, s. 178-197.

² <http://rcb.gov.pl/infrastruktura-krytyczna/> [dostęp 20.08.2020]

³ Tamże.

zaopatrzenia w energię, surowce energetyczne i paliwa, a także łączności i sieci teleinformatycznych. Bez wykorzystania współczesnych technologii trudno byłoby mówić o systemach automatyki przemysłowej, kontroli lotów, aplikacjach bankowych i giełdowych, zaopatrzenia w wodę i żywność, czy też produkcji substancji chemicznych. Taką właściwością charakteryzują się również systemy zapewniające ciągłość działania administracji publicznej oraz ochrony zdrowia, transportowe i ratownicze, tworzące razem tzw. infrastrukturę krytyczną niezbędną do minimalnego funkcjonowania gospodarki i państwa⁴.

Systemy infrastruktury krytycznej

Infrastruktura krytyczna obejmuje systemy⁵:

- zaopatrzenia w energię, surowce energetyczne i paliwa – elektrownie i inne obiekty elektroenergetyczne, bazy, składy i magazyny paliw, zakłady mające bezpośredni związek z wydobywaniem kopalin i ich pochodnych, sieci transportu, przesyła i dystrybucji energii i paliw;
- łączności sieci teleinformatycznych – infrastruktura operatorów publicznych świadczących usługi pocztowe, sieci telekomunikacyjne i teleinformatyczne oraz związane z nimi obiekty, a także systemy teleinformatyczne służące do przetwarzania danych i związane z nimi obiekty. Obiekty Telewizji Publicznej oraz Polskiego Radia.
- finansowe – obiekty NBP oraz BOK, PWPW S.A., Mennicy Państwowej S.A. oraz obiekty i systemy istotne dla zapewnienia stabilności systemu finansowego, systemy płatności, systemy rozliczeń i rachunku papierów wartościowych wraz z obsługującą infrastrukturą oraz rynki regulowane;
- zaopatrzenia w żywność i wodę – obiekty bezpośrednio związane z produkcją żywności i gromadzeniem wody, a także infrastruktura związana z przechowywaniem i transportem do bezpośrednich odbiorców;
- ochrony zdrowia – obiekty i systemy istotne ze względu na zapewnienie opieki i świadczeń zdrowotnych obywatelom (szpitale, placówki zdrowia), magazyny rezerw państwowych produktów leczniczych i wyrobów medycznych oraz zakłady i przedsiębiorstwa farmaceutyczne;
- transportowe – obiekty infrastruktury transportu samochodowego, kolejowego, lotniczego, śródlądowego i morskiego;
- ratownicze – wytypowane obiekty Państwowej Straży Pożarnej oraz infrastruktura jednostek powołanych do ratowania życia i ochrony własności;
- zapewniające ciągłość działania administracji publicznej – obiekty urzędów wojewódzkich, obiekty jednostek organizacyjnych służb zespolonych, inspekcji i straży;

⁴ Tamże.

⁵ http://www.rocznikbezpieczenstwa.dsw.edu.pl/fileadmin/user_upload/wydawnictwo/RBM/RBM_artykuly/2014_8_11.pdf, [dostęp 20.08.2020]

- administracji publicznej – obiekty organów i jednostek organizacyjnych podległych ministrowi właściwemu do spraw administracji lub przez niego nadzorowanych, obiekty podległe Ministrowi Spraw Zagranicznych, obiekty jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, obiekty Agencji Wywiadu, Agencji Bezpieczeństwa Wewnętrznego, Policji, Straży Granicznej, Służba Ochrony Państwa, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, obiekty znajdujące się we właściwości Ministra Sprawiedliwości oraz ważne obiekty innych organów centralnych.

Cyberterroryzm

Cyberterroryzm nie jest odrębnym lub specyficznym rodzajem terroryzmu ze względu na ideologię. Służy dokładnie tym samym celom co zamachy bombowe, porwania czy branie zakładników. Wyróżnia się tylko formą – zastosowaniem sprzętu i oprogramowania komputerowego⁶. Odrębną kwestią jest wykorzystanie Internetu i komputerów przez terrorystów w celach innych niż bezpośrednie zamachy. Systemy komputerowe są doskonałym środkiem zbierania i wymiany informacji oraz łączności. Zapewniają anonimowość, pozwalają na kodowanie lub ukrywanie informacji. Przekazy mogą być ukryte w nie budzących podejrzeń plikach tekstowych czy graficznych. Skala przepływu informacji za pomocą poczty elektronicznej uniemożliwia skuteczną kontrolę treści⁷. W przeciwieństwie do innych rodzajów łączności (np. telefonii komórkowej) odpowiednie korzystanie z Internetu może nie prowadzić do zlokalizowania sprawcy. Cyberterroryzm ma dla terrorystów wiele zalet, które czynią go doskonałym narzędziem godzenia w cel przy niskich kosztach i niewielkich możliwościach wykrycia. Ponadto jest bezpieczny dla przestępców. Nie wymaga wykorzystania środków zagrażających życiu – broni, materiałów wybuchowych czy substancji chemicznych⁸. Cyberterroryści nie muszą zmieniać swej lokalizacji ani w szczególny sposób maskować swej działalności przed postronnymi obserwatorami. W sytuacjach, gdy przemieszczanie się jest niezbędne w zupełności wystarcza samochód osobowy. Narzędzia do prowadzenia działalności cyberterrorystycznej są ogólnie dostępne, a ich posiadanie we wszystkich krajach Europy – legalne. Oprogramowanie, także to służące działalności przestępczej, dostępne jest w internecie. Ugrupowania terrorystyczne, które nie posiadają w swoich szeregach wykwalifikowanych informatyków z łatwością mogą znaleźć najemnych specjalistów. W przeciwieństwie do pirotechników, wyszkolonych żołnierzy czy policjantów, państwa nie są w stanie pro-

⁶ A. Podraza, P. Potakowski, *Cyberterroryzm zagrożeniem XXI wieku Perspektywa politologiczna i prawna*, Dyfin, Warszawa 2013, s. 38.

⁷ M. Górka, *Cyberbezpieczeństwa jako podstawa bezpieczeństwa państwa i społeczeństwa w XXI wieku*, Dyfin, Warszawa 2014, s. 48.

⁸ Tamże. s. 49.

wadzić ewidencji cywilnych specjalistów od systemów komputerowych⁹. Jest to dodatkowo utrudnione, gdy są to osoby amatorsko zajmujące się przestępczością komputerową. Dodatkową zaletą cyberterroryzmu jest możliwość długotrwałego działania bez wykrycia, wielokrotnego przełamывania systemów ochronnych bez alarmowania odpowiednich służb. Niektóre operacje, na przykład włamania do systemów bankowych, mogą zostać nigdy nie wykryte. Ponadto, zależnie od charakteru prowadzonych działań, istnieje możliwość odwleczenia w czasie zdarzenia lub zastosowania mechanizmu zegarowego¹⁰.

Cyberterroryzm może przybrać trzy zasadnicze formy:

- włamania i blokada serwerów. Może to przybrać formę zmieniania/uszkadzania systemów operacyjnych lub doprowadzenie do wielokrotnych połączeń atakowanego serwera i innych serwerów. Prowadzi to do stopniowego spowolnienia jego pracy a następnie do zawieszenia.
- Wirusy, czyli programy działające wbrew woli użytkownika systemu na jego szkodę. Mogą wywoływać różne efekty. Najczęściej przeznaczone są do uszkodzania baz danych i systemów operacyjnych. Mogą także paraliżować systemy zabezpieczające lub modyfikować zachowanie systemu. Zgodnie z powszechną nazwą „wirusy” mogą mieć zdolność do atakowania systemów połączonych z zaatakowaną jednostką, przenosząc się, np. wraz z pocztą elektroniczną. Mogą także być umieszczane w systemie podczas włamania albo atakować go po innym połączeniu z „zainfekowanym” serwerem.
- Atak konwencjonalny, który polega na fizycznym uszkodzaniu elementów systemu komputerowego; serwerów, linii telekomunikacyjnych lub linii energetycznych. Atak tego typu może, zależnie od sposobu przeprowadzenia, prowadzić do czasowego paraliżu systemu lub nieodwracalnej utraty danych¹¹.

Zagrożenia ze strony cyberataków na infrastrukturę krytyczną

Ucyfrowienie 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-tych XX wieku cyberprzestrzeń¹² 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

⁹ Tamże, s. 50.

¹⁰ Tamże, s. 51-53.

¹¹ M. Górka, *Cyberbezpieczeństwa jako podstawa bezpieczeństwa państwa...*, dz. cyt., s. 50.

¹² M. Lakomy, *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*, [w:] *Stosunki Międzynarodowe – International Relations*, 2010, Nr 3-4, s. 56.

wydarzenia z drugiej połowy pierwszej dekady XXI wieku, kiedy to doszło do szeregu poważnych incydentów teleinformatycznych. Należy tu wskazać przede wszystkim wydarzenia z kwietnia 2007 roku, kiedy po raz pierwszy 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 państwa¹³. 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. Szóstego września siły zbrojne 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 IDF¹⁴, bowiem został wcześniej zainfekowany wirusem komputerowym¹⁵. 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 komercyjnych¹⁶. 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 wszystkim z terytorium Chin. Wszystkie te wydarzenia stanowiły więc potwierdzenie opinii, wskazujących na zasadniczy wzrost teleinformatycznych zagrożeń dla bezpieczeństwa państw¹⁷.

Należy mieć bowiem na uwadze, iż szkodliwa działalność w cyberprzestrzeni charakteryzuje się niezwykle bogactwem nie tylko form i technik, ale także szeroko rozumianą wieloaspektowością i wielopłaszczyznowością. Technologie teleinformatyczne są bowiem współcześnie wykorzystywane na masową skalę, do rozmaitych celów, przez podmioty o różnym stopniu zorganizowania, odmiennych motywacjach i statusie prawnopolitycznym. Sytuację dodatkowo komplikuje specyfika funkcjonowania cyberprzestrzeni, wiążąca się m.in. z brakiem tradycyjnych granic czy łatwością do osiągnięcia anonimowości.

¹³ K. Liedel (red.), *Transsektorowe obszary bezpieczeństwa narodowego*, Dyfin, Warszawa 2011, s. 63.

¹⁴ IDF - Israeli Defense Forces

¹⁵ <http://oapuw.pl/wp-content/uploads/2013/11/M.Lakomy-zagrozenia-dla-bezpieczenstwa-teleinformatycznego.pdf> [dostęp 20.08.2020]

¹⁶ M. Lakomy, *Cyberwojna jako rzeczywistość XXI wieku*, [w:] *Stosunki Międzynarodowe – International Relations*, 2011, nr 3-4, s. 147

¹⁷ <http://oapuw.pl/wp-content/uploads/2013/11/M.Lakomy-zagrozenia-dla-bezpieczenstwa-teleinformatycznego.pdf> [dostęp 20.08.2020]

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 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*¹⁸.

Zagrożenia teleinformatyczne nie są właściwe jedynie poszczególnym państwom. Choćby ze względu na model funkcjonowania sieci, mają one charakter transnarodowy, globalny. 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 międzynarodowym¹⁹.

Dla sprawnego funkcjonowania gospodarki nowoczesnych społeczeństw, opartej na wysoko rozwiniętej technice, niezbędne jest niezakłócone działanie różnorodnych jej elementów (zaopatrzenie w energię, wodę, rozwinięte i szeroko dostępne sieci telekomunikacyjne i komputerowe, sprawnie działający transport). Zabezpieczenie obiektów, instalacji i usług zapewniających zaspokojenie tych podstawowych potrzeb społeczeństwa, w oparciu o systemy określane mianem infrastruktury krytycznej, ma zasadnicze znaczenie w kształtowaniu należytego poziomu bezpieczeństwa obywateli. Te obszary działalności narażone są na nieustanne zakłócenia i awarie, w tym także ataki terrorystyczne. Rosnące znaczenie obiektów i systemów infrastruktury krytycznej dla bezpieczeństwa państwa wynika z ich strategicznego znaczenia dla podtrzymania niezakłóconego funkcjonowania państwa w warunkach współczesnych zagrożeń²⁰. Dlatego niezmiernie ważne jest przedsięwzięcie odpowiednich kroków, mających na celu zabezpieczenie tych elementów poprzez odpowiednią ich ochronę. Pozwoli to na zapewnienie ciągłości działania i integralności infrastruktury krytycznej oraz szybkiego odtwarzania na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie²¹.

¹⁸ M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009, s. 9.

¹⁹ <http://oapuw.pl/wp-content/uploads/2013/11/M.Lakomy-zagrozenia-dla-bezpieczenstwa-teleinformatycznego.pdf>, [dostęp 20.08.2020]

²⁰ M. Żuber, *Infrastruktura krytyczna państwa jako...*, dz. cyt., s. 181.

²¹ Tamże.

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*²². 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 prawnopolitycznych;
- reperkusji incydentów teleinformatycznych;
- 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 międzynarodowego²³. Do źródeł zagrożeń o charakterze systemowym (ustrukturalizowanym) można więc zaliczyć:

- państwa i ich grupy,
- 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 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 chińskiego²⁴.

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

²² *Motywacja*, Encyklopedia PWN, <http://encyklopedia.pwn.pl/haslo.php?id=3943894>, [dostęp 20.08.2020]

²³ M. Lakony, *Zagrożenia dla bezpieczeństwa teleinformatycznego*, [w:] Kwartalnik Naukowy OAP UW „e-Politikon”, 2013 | 6 | s.107.

²⁴ Tamże, s. 109.

- hakerów,
- haktywistów,
- „cyberwojowników”,
- przestępców,
- pozostałych, czyli posiadających różną motywację amatorów.

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 państw²⁵. Innymi słowy, miałyby na uwadze wielopłaszczyznowy i wieloaspektowy charakter tych wyzwań, dostrzegając ich odmienne znaczenie z punktu widzenia nie tylko funkcjonowania infrastruktury krytycznej²⁶, ale także, np. wykładni prawa wewnętrznego i międzynarodowego oraz efektywności mechanizmów współpracy politycznej w środowisku międzynarodowym. Na podstawie powyższych rozważań oraz praktyki dotychczasowych cyberataków można więc pokusić się o wskazanie następujących zagrożeń²⁷:

- 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 międzynarodowego²⁸. 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 wykorzystania²⁹.

Zagrożenia cyberterrorystyczne dla systemów IK

Oto najważniejsze zależności, pokazujące związek technologii z elementami infrastruktury państwa. Infrastruktura ta może mieć istotny wpływ na sprawność

²⁵ M. Górka, *Cyberbezpieczeństwa jako...*, dz. cyt., s. 50.

²⁶ Ustawa o zarządzaniu kryzysowym, 26.04.2007, Dz.U. z 2007 r. Nr 89, poz. 590

²⁷ M. Lakony, *Zagrożenia dla bezpieczeństwa teleinformatycznego*, dz. cyt., s. 110.

²⁸ M. Górka, *Cyberbezpieczeństwa jako...*, dz. cyt., s. 50.

²⁹ M. Madej, M. Terlikowski (red.), *Bezpieczeństwo, ...dz. cyt.*, s.97.

działania organów państwa oraz na zdrowie i życie jego obywateli. Ważne staje się zatem określenie potencjalnych skutków ataków³⁰:

- System zaopatrzenia w energię, surowce, energetyczne i paliwa
 - a. Wsparcie przez technologię informacyjną (wybrane rozwiązania):
 - system nadzoru i monitorowania składowisk surowców i paliw;
 - system sterowana przesyłu i dystrybucji energii elektrycznej;
 - system zarządzania siecią energetyczną regionu/kraju;
 - system elektroenergetycznej automatyki zabezpieczeniowej.
 - b. Potencjalne zagrożenia cyberterrorystyczne (efekt):
 - wyładowania elektrostatyczne na skutek uszkodzenia elektronicznych części
 - urządzeń monitorujących opary i ciśnienie paliw;
 - wyłączenie zabezpieczeń generatorów i linii WN;
 - rozregulowanie przepustowości połączeń systemów energetycznych (elektroenergetycznego i gazowniczego).
 - c. Skutki:
 - chaos wśród ludności, wpływ na cierpienia fizyczne- duża liczba ofiar lub rannych;
 - konsekwencje ekologiczne- skażenie terenu;
 - uniemożliwienie świadczenia usługi zakłócenie codziennego życia;
 - straty ekonomiczne.
- System łączności i sieci teleinformatycznych
 - a. Wsparcie przez technologię informacyjną (wybrane rozwiązania):
 - system łączności ruchomej do zastosowań publicznych i społecznych;
 - ogólnodostępne systemy teletransmisyjne i komunikacyjne.
 - b. Potencjalne zagrożenia cyberterrorystyczne (efekt):
 - uszkodzenie i nieuprawniona modyfikacja łączy telekomunikacyjnych;
 - niewłaściwa ochrona sesji zarządzania i konfiguracji elementów aktywnych sieci.
 - c. Skutki:
 - panika i dezorganizacja wśród ludności;
 - uniemożliwienie świadczenia usługi zakłócenie codziennego życia.
- Systemy finansowe i bankowe (giełdowe)
 - a. Wsparcie przez technologię informacyjną (wybrane rozwiązania):
 - system do prowadzenia działań na rynku papierów wartościowych i rynku pieniężnym;
 - platformy informatyczne wspierające operacje giełd papierów wartościowych;
 - systemy zarządzania siecią bankomatów.
 - b. Potencjalne zagrożenia cyberterrorystyczne (efekt):

³⁰ <http://www.computerworld.pl/news/368103/Elementy.zagrozenia.krytycznej.infrastruktury.panstwa.html>, [dostęp 20.08.2020]

- wyłączenie lub nieprawidłowe działanie na skutek wprowadzenia złośliwego oprogramowania;
- blokada możliwości przyjmowania zleceń online;
- ograniczenie dostępnych przez Internet rachunków bankowych i maklerskich;
- uniemożliwienie rozliczenia transakcji dokonanych w sieci bankomatów i terminali POS.
- c. Skutki:
 - brak dostępu do środków płatniczych;
 - konflikt wśród ludności, kradzieże i wymuszenia.
- Systemy zaopatrzenia w żywność i w wodę
 - a. Wsparcie przez technologię informacyjną (wybrane rozwiązania):
 - zautomatyzowane systemy produkcji i sprawdzania jakości żywności;
 - systemy sterowania oczyszczaniem i uzdatnianiem wody;
 - systemy zautomatyzowane sterowania zaporą wodną.
 - b. Potencjalne zagrożenia cyberterrorystyczne (efekt):
 - niekontrolowane otworzenie tamy, zbiornika wodnego na skutek przejęcia kontroli;
 - wprowadzenie przekłamań do systemu kontroli żywności, parametrów wody.
 - c. Skutki:
 - istotny wpływ na cierpienie fizyczne i zakłócenie codziennego życia, w tym utrata podstawowych usług;
 - możliwość powstania epidemii.
- System ochrony zdrowia i ratownicze
 - a. Wsparcie przez technologię informacyjną (wybrane rozwiązania):
 - systemy telekomunikacyjne zapewniające obsługę numeru alarmowego 112;
 - system łączności radiowej służby ratownictwa medycznego.
 - b. Potencjalne zagrożenia cyberterrorystyczne (efekt):
 - unieruchomienie węzłów telekomunikacyjnych przy centrach powiadamiania ratunkowego;
 - wprowadzenie zakłóceń w kanały radiowe systemu łączności.
 - c. Skutki:
 - wpływ na zaufanie opinii publicznej;
 - zwiększona liczba nagłych zgonów wśród ludności.
- Systemy transportowe
 - a. Potencjalne zagrożenia cyberterrorystyczne (efekt):
 - systemy sterowania ruchem kolejowym;
 - systemy sterowania sygnalizacją świetlną/ ruchem drogowym;
 - inteligentne systemy transportowe monitorujące ruch pojazdów komunikacji miejskiej i sterujące sygnalizacją w sposób minimalizujący tworzenie się na drogach korki.
 - b. Potencjalne zagrożenia cyberterrorystyczne (efekt):

- przełamania kontroli szybkości na skutek zmanipulowania komputerem sterującym lokomotywą;
- przejęcie kontroli nad obwodami torowymi przekazującymi do lokomotywy sygnał o zajętości torów i dopuszczalnej maksymalnej szybkości;
- przesterowanie systemu kontroli zajętości torów;
- wprowadzenie przekłamań do systemu telemetrycznego.
- c. Skutki:
 - ofiary w ludziach lub ranni;
 - konsekwencje ekologiczne w przypadku przewożenia substancji niebezpiecznych.
- Systemy zapewniające ciągłość działania administracji publicznej
 - a. Potencjalne zagrożenia cyberterrorystyczne (efekt):
 - rejestry publiczne (np. PESEL, CEPIK, KRS, KRK, REGON, OEWiUDO) i sieci teletransmisyjne;
 - systemy telekomunikacyjne zapewniające łączność przewodową.
 - b. Potencjalne zagrożenia cyberterrorystyczne (efekt):
 - wprowadzenie przekłamań do rejestrów w celu utraty integralności gromadzonych danych;
 - zmanipulowanie urządzeń sieciowych w celu utraty dostępności informacji przesyłanych przy wykorzystaniu systemów teletransmisyjnych.
 - c. Skutki:
 - duży wpływ na zaufanie opinii publicznej;
 - nagły wzrost przestępczości.
- Systemy produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych
 - a. Potencjalne zagrożenia cyberterrorystyczne (efekt):
 - systemy pomiarowe i urządzenia zapewniające sygnalizację o zagrożeniach(system wczesno ostrzegania);
 - przemysłowe systemy sterowania rurociągiem;
 - systemy nadzoru instalacji substancji niebezpiecznych, w tym materiałów łatwopalnych, środków toksycznych i materiałów biologicznie zakaźnych.
 - b. Potencjalne zagrożenia cyberterrorystyczne (efekt):
 - przesterowanie urządzeń pomiarowych w wyniku wyładowań elektrycznych;
 - przejęcie kontroli nad systemem zarządzania rurociągiem.
 - c. Skutki:
 - znaczne konsekwencje ekologiczne;
 - konsekwencje ekologiczne -skażenie terenu.

Haktywizm

Już w latach 80. XX wieku, środowisko hakerów zaczęło ulegać stopniowemu podziałowi. Oprócz tradycyjnie rozumianego hakingu pojawiły się nowe formy niezinstytucjonalizowanych zagrożeń teleinformatycznych³¹. Niektórzy programiści postanowili wykorzystać własne umiejętności do nielegalnego osiągnięcia osobistych korzyści. Druga grupa natomiast zaczęła wykorzystywać potencjał cyberprzestrzeni do promowania określonych idei politycznych. W 1996 roku ukuło w tym kontekście termin *haktywizm*, który powstał z połączenia słów *hacking* i *aktywizm*. Został on po raz pierwszy użyty przez grupę *Cult of the DeadCow*³². Według nich, *haktywistą* miała być osoba wykorzystująca swoje umiejętności komputerowe do promocji określonych postulatów politycznych. W odróżnieniu od *hackingu* 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.³³ 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. Natomiast w 1994 roku wykorzystano technikę DDoS³⁶ 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 ACTA³⁴.

Cyberprzestępczość

Zjawiska cyberprzestępczości należy upatrywać w *hackingu*. 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 pro-

³¹ P. Zańsko, *Zabijemy was słowami. Prowokacja kulturowa w przestrzeni miejskiej i w Internecie*, Wydawnictwo Uniwersytetu Warszawskiego, Warszawa 2014, s. 16.

³² A. Piasecki, *Haktywizm*, Wydawnictwo UMCS, Lublin 2014, s. 25.

³³ Tamże.

³⁴ Tamże, s. 28.

cederu 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 autorskich³⁵. Można jednak sformułować zdecydowanie szerszą definicję, według której cyberprzestępczością byłoby wykorzystanie komputerów do jakiejkolwiek działalności wykraczającej poza granice prawa. Bardzo szeroko została sformułowana również polska definicja tego zjawiska, zawarta w Rządowym Programie Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na Lata 2011-2016. Stwierdzono w nim, iż cyberprzestępstwo to czyn zabroniony popełniony w obszarze cyberprzestrzeni³⁶.

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 cyberprzestrzeni³⁷. 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 technologii³⁸. 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 akcji³⁹.

³⁵ *Konwencja Rady Europy o Cyberprzestępczości*, Rada Europy, Budapeszt, 23.11.2001.

³⁶ Rządowy Program *Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na Lata 2011-2016*, Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2010, s. 6.

³⁷ A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2003, s. 61.

³⁸ Tamże, s. 63

³⁹ Tamże, s. 64.

Działania zbrojne w cyberprzestrzeni

Działania zbrojne w cyberprzestrzeni w połowie lat 90. XX wieku pojawiły się pierwsze głosy klasyfikujące cyberprzestrzeń jako kolejny teatr wojny⁴⁰. W styczniu 1996 roku ośrodek badawczy RAND ogłosił słynny raport, w którym stwierdzono możliwość prowadzenia „strategicznej wojny w cyberprzestrzeni”⁴¹. 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 wojny⁴². 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. 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.⁴³ Jak jednak słusznie zauważył Julian Borger z „The Guardian”, Pentagon nie zdecydował się, mimo posiadanego potencjału, na operację na pełną skalę w cyberprzestrzeni⁴⁴. Obawiano się nie tylko prawnych implikacji tego typu działań, lecz także ujawnienia swoich rzeczywistych zdolności w tej dziedzinie. Z drugiej strony serii odwetowych ataków na serwery należące do NATO dokonali hakerzy serbscy oraz chińscy⁴⁵. Po raz pierwszy na większą skalę ofensywne działania w cyberprzestrzeni towarzyszyły więc konwencjonalnemu konfliktowi zbrojnemu. W późniejszym okresie tendencja ta jedynie się potwierdziła⁴⁶.

⁴⁰ P. Sienkiewicz, H. Świeboda, *Niebezpieczna przestrzeń cybernetyczna*, „Transformacje”, 2006, nr 1-4, s. 47-50,

⁴¹ Tamże.

⁴² M. Lakony, *Zagrożenia dla bezpieczeństwa teleinformatycznego*, dz. cyt., s. 131.

⁴³ M. Górka, *Cyberbezpieczeństwa jako..*, dz. cyt., s. 49.

⁴⁴ M. Lakony, *Zagrożenia dla bezpieczeństwa teleinformatycznego*, dz. cyt., s. 131.

⁴⁵ Tamże, s. 132.

⁴⁶ M. Lakomy, *Cyberwojna jako rzeczywistość XXI wieku*, dz. cyt., s. 147.

Podsumowanie

Warunki niezbędne do funkcjonowania każdego systemu teleinformatycznego jest wyposażenie go w środki techniczne zapewniające bezpieczeństwo wymiany oraz współdziałania informacji pomiędzy takimi samymi oraz różnymi szczeblami kierowania organizacją. Jednocześnie. W celu poprawy bezpieczeństwa, a także minimalizowania błędów w obsłudze czy też dostępie do zasobów sieci, tworzy się możliwości automatycznego rejestrowania pracy w sieciach teleinformatycznych, a także kontroli wymienionych informacji. Przestrzeganie procedur bezpieczeństwa wymiany informacji, identyfikacji urządzeń i połączeń, jak również zastosowanie zabezpieczeń technicznych użytkowanego sprzętu stwarza bariery dla osób nieuprawnionych, które skutecznie powinny chronić współdzielenie danych za pomocą sieci teleinformatycznych, należało by brać pod rozwagę niżej wymienione przedsiębiorstwa⁴⁷:

- bezpieczeństwo transmisji danych – zgodne z potrzebami ochrony zabezpieczenia linii i urządzeń przekazujących informacje na potrzeby systemów teleinformatycznych,
- wpływ oprogramowania na bezpieczeństwo informacji w systemach teleinformatycznych; umożliwia działanie urządzeń poprzez wykorzystanie ustalonych mechanizmów zarządzania oraz kolejności realizacji poszczególnych zadań.
- ochrona fizyczna; realizowana jest praktycznie poprzez przedsięwzięcia zabezpieczania bezpośredniego.

Resort obrony narodowej jak każda inna organizacja narażony jest na ataki cybernetyczne i ingerencje z zewnątrz w systemy teleinformatycznych dowództw i wojsk. Zaawansowane technicznie ataki cybernetyczne wykorzystywane w Siłach Zbrojnych RP⁴⁸.

Incydenty w cyberprzestrzeni od lat stanowią rosnące zagrożenie dla bezpieczeństwa państw. Oprócz szeregu dylematów natury czysto technicznej wiążą się z nimi również bardzo poważne wątpliwości natury politycznej i prawnej. Z perspektywy nauk społecznych sfera bezpieczeństwa teleinformatycznego 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 odpowiedzi⁴⁹. 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

⁴⁷ M. Górka, *Cyberbezpieczeństwa jako...*, dz. cyt., s. 50.

⁴⁸ Tamże.

⁴⁹ M. Lakony, *Zagrożenia dla bezpieczeństwa teleinformatycznego*, dz. cyt., s. 138.

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.

Literatura:

1. Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2003.
2. Górka M., *Cyberbezpieczeństwa jako podstawa bezpieczeństwa państwa i społeczeństwa w XXI wieku*, Dyfin, Warszawa 2014.
3. M. Lakomy, Cyberwojna jako rzeczywistość XXI wieku, „Stosunki Międzynarodowe – International Relations”, 2011, nr 3-4,
4. M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego*, Kwartalnik Naukowy OAP UW „e-Politikon”, 2013 | 6 |.
5. M. Lakomy, *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*, „Stosunki Międzynarodowe – International Relations”, 2010, Nr 3-4.
6. K. Liedel (red.), *Transsektorowe obszary bezpieczeństwa narodowego*, Dyfin, Warszawa 2011.
7. M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009.
8. Narodowy Program Ochrony Infrastruktury Krytycznej 2015.
9. Podraza A., Potakowski P., *Cyberterroryzm zagrożeniem XXI wieku Perspektywa politologiczna i prawna*, Dyfin, Warszawa 2013.
10. Piasecki A., *Haktywizm*, Wydawnictwo UMCS, Lublin 2014.
11. Sienkiewicz P., Świeboda H., *Niebezpieczna przestrzeń cybernetyczna*, „Transformacje”, 2006, nr 1-4.
12. P. Zańsko, *Zabijemy was słowami. Prowokacja kulturowa w przestrzeni miejskiej i w Internecie*, Wydawnictwo Uniwersytetu Warszawskiego, Warszawa 2014.
13. M. Żuber, *Infrastruktura krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego*, *Rocznik Bezpieczeństwa Międzynarodowego* 2014 | 8 | 2 |.

Netografia:

14. <http://www.computerworld.pl/news/368103/Elementy.zagrozenia.krytycznej.infrastruktury.panstwa.html>
15. *Motywacja*, Encyklopedia PWN, <http://encyklopedia.pwn.pl/haslo.php?id=3943894>,
16. <http://oapuw.pl/wp-content/uploads/2013/11/M.Lakomy-zagrozenia-dla-bezpieczenstwa-teleinformatycznego.pdf>,
17. http://www.rocznikbezpieczenstwa.dsw.edu.pl/fileadmin/user_upload/wydawnictwo/RBM/RBM_artykuly/2014_8_11.pdf.
18. <http://rcb.gov.pl/infrastruktura-krytyczna/>