HISTORIA@TEORIA
ISSN 2450-8047 nr 2018/1 (7)
http://dx.doi.org/10.14746/ht.2018.7.1.16
s. 239-247

CYBERTERRORYZM „KONIEM TROJAŃSKIM" W DOBIE GLOBALIZACJI*

Bartosz MAZURKIEWICZ
Uniwersytet Szczeciński

ABSTRACT

CYBERTERRORISM "TROJAN HORSE" IN THE ERA OF GLOBALIZATION

The aim of the article is the general characterization of cyberterrorism as a new and constantly evolving form of terrorism. The phenomenon was described in the context of globalization processes and the main definitions of terrorism were cited, followed by the specific factors determining cyberterrorism. The article was based on an analysis of source documents – legislation on terrorism prevention and cyberspace protection. Definitions review was performed. The results of earlier research related to the topic of work are quoted.

It has been assessed that in the future the threat of cyber-attacks will be a challenge for states and international organizations. The development of modern technologies and the creation of computerized societies is a factor that provides new areas of action for terrorists. Potential targets of attacks are varied and difficult to protect. Preventive actions should be characterized by a comprehensive approach to the problem and systemic, long-term action in the international sphere.

KEYWORDS:

cyberterrorism, terrorism, cyberspace, globalization, critical infrastructure

* Artykuł powstał na podstawie opracowania przygotowanego w ramach przedmiotu *Problemy polityczne we współczesnym świecie* prowadzonego przez dra hab. prof. US Jarosława Piątka na III stopniu studiów (Nauki o polityce) w Instytucie Politologii i Europeistyki na Wydziale Humanistycznym Uniwersytetu Szczecińskiego.

WSTĘP

Procesy globalizacyjne wpływają na możliwe zwiększanie zagrożeń dla ludzkości. Rozwój współczesnego świata, zwłaszcza pod względem najnowszych technologii (duża dynamika procesów w tej dziedzinie), determinuje potencjalny wzrost zagrożeń. Różnego rodzaju grupy przestępcze, w tym również o charakterze terrorystycznym, zyskują nowe możliwości działania i potencjalne obszary (cele) ataków. Internet, nowoczesne rozwiązania informatyczne, teleinformatyczne w coraz większym stopniu uzależniają społeczeństwa od nowoczesnych technologii. W przypadku skutecznych prób ataków terrorystycznych w tym obszarze konsekwencje mogą być bardzo poważne. Mamy do czynienia z sytuacją następującą: z jednej strony, nowoczesne technologie wpływają na zdynamizowanie rozwoju ludzkości (i wszelkie z tym związane udogodnienia życia codziennego); z drugiej – nowoczesne technologie jak mityczny „koń trojański" mogą stać się niepozornym narzędziem wykorzystywanym przeciwko ludzkości przez rozmaite grupy interesu, zwłaszcza terrorystów.

ZGLOBALIZOWANY ŚWIAT – ZARYS UWARUNKOWAŃ

Współczesny świat, na progu XXI wieku, można określać mianem świata ery globalizacji[1]. Globalizację definiuje się z perspektywy różnych punktów widzenia, ogólnie rzecz ujmując: „to charakterystyczne, dominujące tendencje na przełomie XX i XXI wieku w światowej ekonomii, polityce, demografii, życiu społecznym i kulturze, polegające na rozprzestrzenianiu się analogicznych zjawisk, niezależnie od kontekstu geograficznego"[2].

Po wcześniejszych epokach (agrarnej i industrialnej), w obecnym czasie obserwuje się złożoność i mnogość procesów dotyczących sfer: kulturowej, społecznej i cywilizacyjnej. Ludzkość wkroczyła w nową fazę rozwoju cywilizacji – postindustrialną, którą nazywa się również trzecią falą cywilizacji[3]. Zmniejszenie roli tradycyjnego przemysłu, rozwój nowoczesnych technologii, dominacja sektora usług w gospodarce, zwiększenie znaczenia wiedzy – to wyznaczniki nowej ery. Wpływają one na rozwój procesu globalizacji. Czynnik geograficzny, dotychczas ograniczający możliwości rozwoju, został w bardzo dużym stopniu wyeliminowany. Na świecie dynamicznie

1 D. Bell, *Nadejście społeczeństwa postindustrialnego. Próba prognozowania społecznego*, Warszawa 1975; Z. Bauman, *Globalizacja. I co z tego dla ludzi wynika*, Warszawa 2000; S. Sassen, *Globalizacja. Eseje o nowej mobilności ludzi i pieniędzy*, Kraków 2007; A. Giddens, *Europa w epoce globalnej*, Warszawa 2009.

2 *Encyklopedia PWN*, http://encyklopedia.pwn.pl/szukaj/globalizacja.html [dostęp: 10.10.2017].

3 A.H. Toffler, *Budowa nowej cywilizacji. Polityka Trzeciej Fali*, Poznań 1996.

zyskują na znaczeniu międzynarodowe korporacje, globalne finanse (swobodny przepływ kapitału), transfery technologii, jak również przepływ siły roboczej.

WSPÓŁCZESNY TERRORYZM W UJĘCIU TEORETYCZNYM

Niemożliwe staje się stworzenie jednej, ogólnej definicji terroryzmu, gdyż nie da się jednocześnie opisać różnych jego odmian z uwzględnieniem wszystkich aspektów tego złożonego zjawiska. Rzeczywistość i „praktyka" wyprzedza teorię. Powinno się jednak możliwie najbardziej precyzyjnie dostosowywać (aktualizując) definicję terroryzmu do zmieniającej się rzeczywistości. Niemniej słowo *terroryzm* wywodzi się z łaciny, a oznacza strach *(terror)*, przerażanie (*terrere*).

Na podstawie jednej z bardziej skompilowanych, obszernych definicji, akceptowanej przez większość badaczy, terroryzm jest

wzbudzającą społeczny niepokój metodą powtarzalnych aktów przemocy, przyjętą przez działające, najczęściej w sposób tajny, jednostki, grupy albo podmioty państwowe, wybieraną z powodów kryminalnych lub politycznych, przy czym – w odróżnieniu od zamachów na życie określonych osób na ważnych stanowiskach – bezpośrednie akty przemocy nie są tu ostatecznym celem. Bezpośrednie ofiary ludzkie z reguły są wybierane przypadkowo, na ślepo (cele wynikające z okoliczności) lub selektywnie (cele reprezentatywne lub symboliczne) z docelowej populacji i służą jako przenośniki przesłania. Zagrożenie i bazujący na przemocy proces komunikacyjny pomiędzy terrorystą (organizacją) a ofiarami (zagrożonym) i głównymi celami wykorzystywane są dla manipulacji głównym celem (społecznością czy społecznościami), zmieniając je w cel terroru, cel żądań lub też skupienia uwagi społecznej, zależnie od tego, czy sprawcy zmierzają do zastraszenia, przymuszenia czy jedynie propagandy"[4].

Inni badacze[5] na podstawie statystycznej analizy wielu (ponad stu) różnych definicji zjawiska terroryzmu stwierdzili, że powtarzającymi się w nich elementami są: przemoc (siła), polityczny wymiar, strach, groźby, efekt psychologiczny, rozbieżność pomiędzy celem a ofiarą, celowe i zorganizowane działanie, taktyka, strategia i metody walki.

Współczesny terroryzm – nazywany religijnym, globalnym, ponowoczesnym[6] – odznacza się kilkoma cechami, wcześniej nieznanymi. Obecnie terroryści stosują

4 *Encyklopedia terroryzmu*, red. B. Zasieczna, A. Zasieczny, Warszawa 2004, s. 17.

5 A.P. Schmid, A.J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature*, Amsterdam 1988.

6 W. Laqueuer, *Terrorism*, Boston 1977.

niekonwencjonalne środki walki, a sama walka ma charakter asymetryczny. Inspiracja religijna stanowi ważny element motywujący. Globalny (ponadnarodowy) charakter działań terrorystów wpływa na ogólny, medialny rozgłos poszczególnych ataków, które z reguły pochłaniają więcej ofiar niż kiedykolwiek wcześniej. Warto zwrócić uwagę, że czynnik ekonomiczny (socjalny) traci na wartości: coraz częściej wśród sprawców ataków są osoby rekrutowane ze średnich lub nawet wyższych klas społecznych. Nierówności społeczne, ubóstwo nie są już więc główną motywacją dla terrorystów, zyskują na znaczeniu aspekty ideowe i religijne.

Fundamentalizm religijny powoduje, że współcześni terroryści (po części fanatycy religijni) dokonują ataków coraz bardziej nieprzewidywalnych oraz nie mają zahamowań, co potęguje skalę zniszczeń i liczbę ofiar. Wymiar metafizyczny: nagroda za ataki możliwa do odebrania po śmierci (w przyszłym życiu), jest bardzo efektywnym czynnikiem, pozwalającym szybciej i łatwiej rekrutować potencjalnych zamachowców. Mechanizm ten pozostaje zbieżny z teorią Huntingtona[7], zgodnie z którą historia ludzkości dotyczy dziejów cywilizacji, a konflikty religijne stanowią i będą stanowić podłoże wojen (również tych z terrorystami) w XXI wieku. Znane twierdzenie o „zderzeniu cywilizacji" wpisuje się w nurt tego typu rozważań.

CYBERTERRORYZM JAKO NOWY, NIEPRZEWIDYWALNY RODZAJ TERRORYZMU

Twórcą pojęcia *cyberterroryzm* jest Barry Collin,[8] starszy pracownik naukowy Institute for Security and Intelligence z Kalifornii. U schyłku XX wieku określił go jako połączenie (konwergencję, zbieżność) cybernetyki i terroryzmu. Bardziej poetycko ten sam autor ujął to w następujący sposób: dynamika terroryzmu jako transcendencja (wykroczenie) z fizycznego świata do wirtualnego królestwa; cyberterroryzm stanowi skrzyżowanie (połączenie) tych dwóch światów. Uściślając innymi słowy, można wyjaśniać zjawiska cyberterroryzmu jako „świadome wykorzystywanie systemu informacyjnego, sieci komputerowej lub jej części składowych w celu wsparcia lub ułatwienia akcji terrorystycznej"[9]. W tym samym roku jeden z agentów specjalnych FBI stworzył kolejną, nieco „roboczą" definicję: działanie z premedytacją, motywowany politycznie atak na informacje, systemy i programy komputerowe, jak również dane,

7 S.P. Huntington, *Zderzenie cywilizacji i nowy kształt ładu światowego*, Warszawa 2006.

8 B. Collin, *The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge*, 1997, http://www.crime-research.org/library/Cyberter.htm [dostęp: 10.10.2017].

9 K.C. White, *Cyber-Terrorism: Modem Mayhem*, Carlisle 1998.

w wyniku którego dokonuje się aktów przemocy na niekompatybilne cele przez grupy przestępcze[10].

Współcześnie bardzo reprezentatywne wyjaśnienie zjawiska cyberterroryzmu przedstawia się następująco: „bezprawny atak lub nawet tylko groźba ataku na komputery, systemy informatyczne i sieci informatyczne, celem zastraszenia lub wymuszenia na władzy państwowej ustępstw lub daleko idących, konkretnych celów o charakterze politycznym, społecznym"[11]. Działania tego typu zostaną zakwalifikowane do działań z zakresu cyberterroryzmu, jeśli będą powodowały znaczne szkody, straty dla społeczeństwa lub co najmniej zaistnieje groźba tego typu strat, która wzbudzi powszechne poczucie strachu, lęku.

Wśród potencjalnych obszarów ataków w cyberprzestrzeni wymienia się zarówno te o charakterze militarnym (wojskowym), jak i cywilne. Pierwsze z wymienionych miały miejsce zwłaszcza w okresie zimnej wojny, kiedy z uwagi na ówczesne okoliczności stanowiły newralgiczny, czuły punkt w wielu państwach. Ataki w obszarze cywilnym są szczególnie niebezpieczne dla korporacji o zasięgu międzynarodowym, które stanowią podatny grunt dla przestępców. To jednak stosunkowo nowe pojęcie określające grupę ważnych strategicznie celów, a mianowicie „infrastrukturę techniczną państwa", uznaje się obecnie za najbardziej wrażliwe, a jednocześnie atrakcyjne cele ataków terrorystycznych wykorzystujących nowe technologie. W USA pod koniec XX wieku zdefiniowano pojęcie „infrastruktury technicznej"[12], w skład której wchodzą systemy różnych dziedzin, a których zniszczenie lub tylko uszkodzenie zagraża bezpieczeństwu ekonomicznemu państwa oraz zmniejsza jego zdolności obronne. Do głównych elementów infrastruktury technicznej państwa[13] zalicza się przede wszystkim:

– sieci telekomunikacyjne i teleinformatyczne – linie telefoniczne, sieci komputerowe, satelity;

– system energetyczny – produkcję, przesyłanie, dystrybucję energii;

– system bankowy i finansowy – ogół operacji na instrumentach w skali globalnej;

– system transportowy – kolejowy, lotniczy, morski, rzeczny, drogowy;

– system zaopatrzenia w wodę, surowce energetyczne (zwłaszcza gaz ziemny i ropę naftową) – produkcję, magazynowanie, transport;

10 M. Pollitt, *A Cyberterrorism Fact or Fancy?* [in:] Proceedings of the 20th National Information Systems Security Conference, Virginia 1997, s. 285–289.

11 D.E. Denning, *Statement,* Georgetown University 2000, https://fas.org/irp/congress/2000_hr/00-05-23denning.htm [dostęp: 10.10.2017].

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

13 Rządowe Centrum Bezpieczeństwa, *Infrastruktura krytyczna*, http://rcb.gov.pl/infrastruktura-krytyczna/ [dostęp: 10.10.2017].

– system ratowniczy – policję, straż pożarną, służbę zdrowia;
– system władzy, administrację państwową – gwarancję ciągłości (kontynuacji).

W Polsce dostrzega się potrzebę regulacji kwestii związanych z zapobieganiem cyberterroryzmowi. Podstawowymi dokumentami z tym związanymi są: Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016[14] oraz Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej[15]. Wypełnianie zawartych w nich strategii i założeń ma skutkować realizowaniem celu, jakim jest osiągnięcie właściwego poziomu bezpieczeństwa państwa w cyberprzestrzeni. Ponadto w 2015 roku przyjęto w Polsce Narodowy Program Infrastruktury Krytycznej[16]. Ochrona poszczególnych elementów infrastruktury technicznej polega na zapewnianiu funkcjonalności, ciągłości działań, jak również integralności. Dzięki temu możliwe staje się zapobieganie potencjalnym zagrożeniom, minimalizowanie ryzyk oraz ograniczanie (a nawet neutralizacja) skutków nieprzewidzianych działań w przypadku słabych punktów systemu.

Równie ważnym wymiarem (obok globalnego) wydaje się skala lokalna. Tutaj także możliwe stają się różne formy ataków z wykorzystaniem różnorodnych narzędzi. Jedną z bardzo niebezpiecznych i trudnych do zwalczenia broni w rękach „lokalnych" terrorystów jest ta z pogranicza informatyki i socjotechniki, przez niektórych badaczy określana jako „socjoinformatyka"[17]. Socjotechniki dotyczą manipulowania ludźmi z rozmaitych przyczyn, w dowolnym celu. Natomiast narzędzia (broń) związane z socjoinformatyką dotyczą sytuacji, w których celem ataku staje się włamanie do obcego komputera lub systemu informatycznego, przejęcie tajnych danych, kradzież tożsamości lub inne, podobne naruszenia bezpieczeństwa. Socjoinformatyka może być w przyszłości (o ile już nie jest) jednym z najbardziej efektywnych narzędzi w zbrodniczej działalności. Wykorzystuje się w niej bowiem czynnik ludzki, który – jak wskazują badania – jawi się jako najbardziej zawodny, podatny na manipulacje, a tym samym kosztochłonny element w większości korporacji, administracji rządowych czy też innych organizacji. Rzeczywistość zdaje się potwierdzać powyższe założenia i teorie naukowe, w sezonie 2012/2013 odnotowano bowiem w największych polskich miastach około

14 Ministerstwo Spraw Wewnętrznych i Administracji, *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*, 2010, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf [dostęp: 10.10.2017].

15 Ministerstwo Administracji i Cyfryzacji, *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, http://www.cert.gov.pl/download/3/161/PolitykaOchronyCyberprzestrzeniRP148x210wersjapl.pdf [dostęp: 10.10.2017].

16 Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej*, http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-2015-Dokument-G%C5%82%C3%B3wny-tekst-jednolity.pdf [dostęp: 10.10.2017].

17 T. Trejderowski, *Kradzież tożsamości. Terroryzm informatyczny*, Warszawa 2013, s. 11.

25% otwartych sieci wi-fi, czyli sieci bez żadnych zabezpieczeń (szyfrowań), z którymi można było się połączyć przy użyciu laptopa czy tabletu bez większych przeszkód[18].

PODSUMOWANIE - WNIOSKI - PROGNOZY

W najbliższej przyszłości wojny w cyberprzestrzeni mogą stanowić jedno z głównych pól walk rozmaitych graczy (aktorów). Cyberterroryzm jest nowym rodzajem terroryzmu, a narzędzia i formy ataków – nowymi rodzajami broni w walce. Nieprzewidywalność tej formy stanowi atut w rękach sprawców, bardzo zgubny dla ofiar. Obszary zagrożeń są praktycznie nieograniczone, bardzo trudne do przewidzenia, a tym bardziej do właściwej ochrony. Przy relatywnie niskich kosztach utrzymania infrastruktury informatycznej (w porównaniu do zaplecza wojskowego) cyberterroryzm będzie mógł się rozwijać. Dodatkowo konsekwencje potencjalnych zamachów mogą wywołać zniszczenia na niespotykaną dotychczas skalę. Szczególnie wrażliwa wydaje się sfera infrastruktury krytycznej państwa, której zaatakowanie mogłoby obniżyć lub całkowicie zniszczyć możliwości (zdolności) obronne kraju w szerokim ujęciu. Skuteczny atak na systemy: zaopatrzenia w wodę, energetyczne, komunikacyjne, bankowe prowadziłby do trwałego paraliżu funkcjonowania państwa. Medialność takiego ataku byłaby ogromna, na przykład możliwość ogłoszenia przez daną organizację terrorystyczną faktu przejęcia totalnej kontroli nad państwem, groźba jego całkowitego paraliżu. Innymi czynnikami wpływającymi na atrakcyjność cyberterroryzmu są: niskie ryzyko śmierci sprawców, względnie duża anonimowość terrorystów w fazie planowania i bezpośredniego ataku.

W dobie rozwoju społeczeństwa informacyjnego i postępującej globalizacji szczególnie zasadne wydaje się podejmowanie w kwestiach ochrony działań kompleksowych, systemowych, wykraczających poza granice państw. W obliczu istniejącego zagrożenia zamachami przy wykorzystaniu cyberprzestrzeni organizacje międzynarodowe wraz z państwami powinny wypracować ujednolicone standardy przeciwdziałania mu. Zapobieganie tej formie ataków wymaga podjęcia działań prewencyjnych, bardzo dobrej współpracy i wymiany informacji oraz promowania prostych, transparentnych, a tym samym skutecznych metod zwalczania cyberterroryzmu. Nie bez znaczenia pozostaje kwestia edukacji społeczności w zakresie bezpieczeństwa w Internecie oraz ochrony i odpowiedniego zabezpieczania własnych systemów informatycznych przed różnego typu złośliwymi atakami.

18 M. Ziarek, *Bezpieczeństwo sieci wi-fi w Polsce 2012/2013: podsumowanie*, 2013, http://securelist.pl/analysis/7229,bezpieczenstwo_sieci_wi_fi_w_polsce_2012_2013_podsumowanie.html [dostęp 10.10.2017].

Cyberterroryzm stał się swoistym „koniem trojańskim" współczesnego świata. W czasie powszechnej informatyzacji stworzono nowy potencjalny obszar dla działalności terrorystycznej. Skuteczne ataki w cyberprzestrzeni z przeszłości są na to dowodem. W przyszłości przy braku odpowiedniej ochrony następstwa ewentualnych zamachów mogą być bardzo groźne, a niekiedy trudne do przewidzenia. Skrajnym (choć realnym) poglądem byłoby stwierdzenie, że jedynym ograniczeniem dla grup terrorystycznych w wyborze celów ataku jest ich własna wyobraźnia. Zaatakowany może zostać praktycznie każdy obiekt lub system, który działa przy wykorzystaniu narzędzi informatycznych podłączonych do globalnej sieci.

Przeszło dekadę wstecz zostały wygłoszone pewne zalecenia, rekomendacje i wytyczne samego twórcy definicji cyberterroryzmu. Dotyczyły one ogólnych zasad przeciwdziałania terroryzmowi i nowym jego odmianom[19]. Mimo upływu czasu nadal pozostają cenne i nie tracą na aktualności. Należy współpracować i dokonywać transferu wiedzy na coraz to nowe sposoby i metody przeciwdziałające cyberterroryzmowi, nieznane nigdy wcześniej (stale dostosować je do zmieniających się warunków). Dalej powinno się wykorzystywać pomoc i doświadczenia tych osób (specjalistów), które rozumieją istotę użycia nowych broni przez cyberterrorystów. Ponadto celowe jest zaakceptowanie pojawiania się nowych narzędzi, technologii i zasad walk, które będą wykorzystywane przeciwko państwom i społeczeństwu. Przestrzega się, aby w starciu asymetrycznym, gdy dodatkowo przeciwnik wykorzystuje niekonwencjonalne metody, nie walczyć przy użyciu tradycyjnych narzędzi i przestarzałych technologii. Nieefektywne procesy przetwarzania danych, niekompletne systemy zabezpieczeń stają się mankamentami, które trzeba eliminować. Bardzo dobrym technicznym sposobem wdrażania właściwych rozwiązań wydaje się współpraca z ekspertami, którzy rozumieją, z jakim przeciwnikiem toczy się walka, rozpoznają potencjalne obszary ataku, żyją wśród ludzi, którzy mogą być celem terrorystów, oraz są w stanie trenować (szkolić) kandydatów do walki z terrorystami z cyberprzestrzeni.

BIBLIOGRAFIA

Bauman Z., *Globalizacja. I co z tego dla ludzi wynika*, Warszawa 2000;

Bell D., *Nadejście społeczeństwa postindustrialnego. Próba prognozowania społecznego*, Warszawa 1975;

19 B. Collin, *The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge*, 1997, http://www.crime-research.org/library/Cyberter.htm [dostęp: 10.10.2017].

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

Collin B., *The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge*, 1997, http://www.crime-research.org/library/Cyberter.htm [dostęp: 10.10.2017];

Denning D.E., *Statement*, Georgetown University 2000, https://fas.org/irp/congress/2000_hr/00-05-23denning.htm [dostęp: 10.10.2017];

Encyklopedia PWN, http://encyklopedia.pwn.pl/szukaj/globalizacja.html [dostęp: 10.10.2017];

Encyklopedia terroryzmu, red. B. Zasieczna, A. Zasieczny, Warszawa 2004;

Giddens A., *Europa w epoce globalnej*, Warszawa 2009;

Huntington S.P., *Zderzenie cywilizacji i nowy kształt ładu światowego*, Warszawa 2006;

Ministerstwo Spraw Wewnętrznych i Administracji, *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*, 2010, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf [dostęp: 10.10.2017];

Ministerstwo Administracji i Cyfryzacji, *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, 2013, http://www.cert.gov.pl/download/3/161/PolitykaOchronyCyberprzestrzeniRP148x210wersjapl.pdf [dostęp: 10.10.2017];

Laqueuer W., *Terrorism*, Boston 1977;

Pollitt M., *A Cyberterrorism Fact or Fancy?* [in:] Proceedings of the 20th National Information Systems Security Conference, Virginia 1997;

Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej*, 2015, http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-2015-Dokument-G%C5%82%C3%B3wny-tekst-jednolity.pdf [dostęp: 10.10.2017];

Rządowe Centrum Bezpieczeństwa, *Infrastruktura krytyczna*, 2015, http://rcb.gov.pl/infrastruktura-krytyczna/ [dostęp: 10.10.2017];

Sassen S., *Globalizacja. Eseje o nowej mobilności ludzi i pieniędzy*, Kraków 2007;

Schmid A.P., Jongman A.J., *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature*, Amsterdam 1988;

Toffler A.H., *Budowa nowej cywilizacji. Polityka Trzeciej Fali*, Poznań 1996;

Trejderowski T., *Kradzież tożsamości. Terroryzm informatyczny*. Warszawa 2013;

White K.C., *Cyber-Terrorism: Modem Mayhem*, Carlisle 1998;

Ziarek M., *Bezpieczeństwo sieci wi-fi w Polsce 2012/2013: podsumowanie*, 2013, http://securelist.pl/analysis/7229,bezpieczenstwo_sieci_wi_fi_w_polsce_2012_2013_podsumowanie.html [dostęp: 10.10.2017].