dr inż. Rafał Kołodziejczyk
Uniwersytet Jana Kochanowskiego w Kielcach
Wydział Prawa, Administracji i Zarządzania
rkolodziejczyk@ujk.edu.pl

# NOWA ODSŁONA TERRORYZMU – CYBERTERRORYZM

# NEW WAVE OF TERRORISM – CYBERTERRORISM

**Streszczenie:** Jednym z największych zagrożeń cywilizacyjnych XXI wieku jest terroryzm, który wywołuje psychozę strachu i zaniepokojenie mieszkańców całego świata. Do niedawna ta forma przemocy przybierała postać zamachów bombowych, porywania zakładników czy uprowadzeń dla okupu. Niestety, w ostatnich latach gwałtowny rozwój nowych technologii stał się czynnikiem, powodującym powstanie nowego zagrożenia – cyberterroryzmu. W artykule omówione zostały rodzaje ataków, sposób ich przeprowadzania oraz metody ich finansowania.

**Słowa kluczowe:** cyberterroryzm, rodzaje, metody ataku, sposoby finansowania.

**Summary:** One of the greatest civilization threats of the 21st century is terrorism, which triggers the psychosis of fear and concern of the inhabitants of the whole world. Until recently, this form of violence took the form of bomb attacks, kidnapping hostages or abductions for ransom. Unfortunately, in recent years, the rapid development of new technologies has become a factor causing the emergence of a new threat – cyberterrorism. The article discusses the types of attacks, the manner of their implementation and methods of their financing.

**Keywords:** cyberterrorism, types, methods of attack, financing methods.

## Wstęp

Od najdawniejszych lat rozwój technologiczny w znaczący sposób wpływał na życie człowieka. W ostatnich latach szczególnie intensywnie rozwija się obszar informatyki oraz szerokopasmowego Internetu i przekłada się to jednoznacznie na zwiększenie udziału tych czynników w życiu każdego człowieka. Codzienne funkcjonowanie jest już nierozerwalnie związane z cyberprzestrzenią, czyli przestrzenią wirtualną, w której odbywa się komunikacja między komputerami połączonymi siecią internetową. Obecnie coraz więcej rutynowych czynności wykonujemy zdalnie za pomocą komputera, tabletu czy telefonu.

Niewątpliwie jest to rozwiązanie bardzo praktyczne, ale nie idealne. W ślad za udogodnieniami, jakie oferuje sieć internetowa, podążają również zagrożenia. Do najczęściej występujących należą: oszustwa internetowe, włamania na konta, kradzież danych czy pornografia dziecięca. Wirtualna przestrzeń stwarza również warunki do rozwoju nowej platformy walki zbrojnej, nowej formy terroryzmu – cyberterroryzmu.

## Geneza cyberterroryzmu

Zdefiniowanie cyberterroryzmu nie jest sprawą prostą, ponieważ obszar działań w tej materii jest dosyć szeroki i trudny do jednoznacznego określenia. Za twórcę pojęcia „cyberterroryzm" uważa się pracownika Institute for Security and Intelligence w Kalifornii – Barry'ego Collina, który w latach 80. dwudziestego wieku użył go jako pierwszy dla zdefiniowania terroryzmu, którego platformą działania jest cyberprzestrzeń (Denning, 2002, s. 79). Według niego, „cyberterroryzm to świadome wykorzystanie systemu teleinformatycznego, sieci komputerowej lub jej części składowych w celu wsparcia bądź też ułatwienia przeprowadzanie akcji terrorystycznej" (Tafoya, 2011). Natomiast Marcin Łapczyński (2009) uważa, że termin ten pojawił się wcześniej bo już w 1979 r., gdy szwedzkie Ministerstwo Obrony umieściło go w raporcie o zagrożeniach komputerowych, rekomendując by rząd zaangażował się w monitorowanie, zarówno publicznych, jak i prywatnych sieci komputerowych.

Jedną z najbardziej znanych i powszechnie cytowanych definicji jest sformułowana przez Departament Obrony USA na potrzeby powołania jednolitego słownika terminologii wojskowej, według której cyberprzestrzeń to: „Globalna domena środowiska informacyjnego składająca się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery" (Wasilewski, 2013).

Nieco inaczej cyberterroryzm definiuje Narodowe Centrum Ochrony Infrastruktury USA: „cyberterroryzm jest atakiem kryminalnym popełnionym przy użycia komputera oraz sieci telekomunikacyjnych, powodującym użycie siły, zniszczenie bądź też przerwanie usług w celu wywołania poczucia strachu, poprzez wytworzenie zamieszania i wywołania niepewności w określonej części populacji, w celu wpływania na rządy oraz ludność w sposób, mogący wykorzystać ich reakcje dla osiągnięcia z góry określonych celów politycznych, społecznych, ideologicznych bądź też głoszonego przez terrorystów programu" (DOD Dictionary of Military and Associated Terms, 2017).

Robert Kośla (2002) natomiast definiuje cyberterroryzm jako wszelkiego rodzaju działania blokujące, niszczące lub zniekształcające w stosunku do informacji przetwarzanej, przechowywanej i przekazywanej w systemach teleinformatycznych oraz niszczące (obezwładniające) te systemy. Według niego w zakresie tego pojęcia mieści się również wykorzystywanie systemów teleinformatycznych do dezinformacji oraz walki psychologicznej. Nieco bardziej zawężoną definicję podaje Dorothy Denning (2000) stwierdzając, że cyberterroryzm jest bezprawnym atakiem lub groźbą ataku na komputery, sieci lub systemy informatyczne mające na celu zastraszenie lub wymuszenia na rządzie lub ludziach daleko idących ustępstw. Uważa również, że za atak cyberterrorystyczny można uznać jedynie akt, który powoduje bezpośrednie szkody człowiekowi, jego mieniu lub przynajmniej wywołuje panikę i budzi strach.

Natomiast Agnieszka Bógdał-Brzezińska i Marcin Gawrycki (2003, s. 70) uważają, że cyberterroryzm to jedna z najbardziej nieprzewidywalnych form oddziaływania

zorganizowanych grup przestępczych na stabilność infrastruktury krytycznej państwa (np.: telekomunikacja, systemy energetyczne i finansowe). Ernest Lichocki (2009, s. 58) zdefiniował cyberterroryzm jako przemyślany politycznie lub militarnie atak lub jego groźba na systemy i sieci teleinformatyczne oraz zgromadzone dane teleinformatyczne w celu sparaliżowania lub poważnego zniszczenia infrastruktury krytycznej państwa w celu zastraszenia i wymuszenia na rządzie lub społeczności ściśle określonych działań lub ustępstw. Uważa on również, że cyberterroryzm to wykorzystanie przez organizacje terrorystyczne sieci do rekrutacji, komunikacji, propagandy czy zbierania materiałów o potencjalnych celach ataku oraz dezinformacji i walki psychologicznej. Cyberatak może być przeprowadzony jako element skomasowanej akcji polityczno-militarnej lub samodzielny atak.

Podsumowując można stwierdzić, że cyberterroryzmu to wykorzystywanie cyberprzestrzeni w działaniach terrorystycznych. Narzędziem do wykonywania aktów terroru jest sieć komputerowa, a celem związane z krytyczną infrastrukturą państw zasoby, do których należą między innymi: energia, woda oraz transport, telekomunikacja, bankowość i finanse. Przejęcie kontroli nad tymi zasobami, które sterowane są za pomocą komputerów i Internetu, powoduje chaos i panikę oraz brak stabilizacji w działaniach państwa.

Innym sposobem wykorzystywania cyberprzestrzeni przez terrorystów jest używanie jej do celów propagandowych: wzniecania konfliktów wewnątrz państwowych czy międzyreligijnych, szerzenia nienawiści czy prowadzenia wojny psychologicznej. Wykorzystują oni również sieć do werbowania i szkolenia nowych bojowników oraz zdobywania informacji, organizowania i przeprowadzania ataków terrorystycznych.

## Obszary działań cyberterrorystycznych

Omawiając cyberterroryzm nie sposób pominąć cyberprzestępstw, które można nazywać cyberterroryzmem, ale na znacznie mniejsza skalę i o mniejszej szkodliwości społecznej. Cyberprzestępstwa są najczęściej formami przestępstw i działań zabronionych dokonywanych w cyberprzestrzeni za pomocą komputerów i Internetu. Ze względu na rodzaj dokonywanych czynów zabronionych cyberprzestępstwa dzielimy na cztery grupy. Do pierwszej zalicza się oszustwa i fałszerstwa, do kolejnej należą: pozyskiwanie, wytwarzanie, rozpowszechnianie oraz samo posiadanie treści nielegalnych. Trzecią grupą są ataki na systemy informatyczne, a do ostatniej kategorii, zalicza się: kopiowanie i rozpowszechnianie w celach zarobkowych utworów chronionych prawem autorskim. Nieco odmiennego podziału dokonała Komisja Europejska, która do cyberprzestępstw zalicza:

- przestępstwa przeciwko poufności, integralności i dostępności danych dotyczących nielegalnego dostępu do systemów (hacking, podsłuchiwanie i podawanie fałszywej tożsamości, szpiegostwo komputerowe, sabotaże oraz wymuszenia komputerowe);
- manipulacje fakturami lub kontami firmowymi, nieprawdziwe aukcje czy nielegalne używanie kart kredytowych, komputerowe podróbki, molestowanie dzieci,

ataki na życie ludzkie, manipulowanie systemami szpitalnymi lub kontrolą ruchu powietrznego;
- przestępstwa obejmujące dziecięcą pornografię, przekazywanie instrukcji zachowań przestępczych, oferty popełniania przestępstw, molestowanie i lobbing poprzez sieć, rozpowszechnianie fałszywych informacji oraz internetowy hazard;
- przestępstwa powiązane z naruszeniem prawa autorskiego i praw pokrewnych (nieautoryzowane kopiowanie i rozpowszechnianie programów komputerowych, nieautoryzowane użycie baz danych itp.) (Szubrycht, 2005, s. 174).

Inną klasyfikację zagrożeń występujących w cyberprzestrzeni przedstawił Włodzimierz Gogołek (2007, s. 321), dzieląc je na siedem kategorii:
- *stealingpasswords* – uzyskiwanie haseł dostępu do sieci;
- *social engineering* – wykorzystanie niekompetencji osób posiadających dostęp do systemu;
- *bugs and backdoors* – nielegalne korzystanie z systemu lub używanie nielegalnego oprogramowania;
- *authenticationfailures* – zniszczenie mechanizmu autoryzacji;
- *protocolfailures* – wykorzystanie luk w oprogramowaniu i systemach;
- *information leakage* – przechwycenie informacji dostępnych dla administratora;
- *denial of service* – blokada kont użytkowników systemu.

Obszar działań cyberterrorystów jest bardzo obszerny, trudny do jednoznacznego określenia i ciągle powiększający swój zasięg na nowe strefy. Ze względu na rodzaj atakowanego celu można wprowadzić następujący podział:
- informatyczne systemy wojskowe, przechowujące między innymi informacje o planowanych ruchach i rozmieszczeniu wojsk oraz broni, systemach łączności czy prowadzonych badaniach nad nowymi rodzajami uzbrojenia;
- informatyczne systemy państwowej infrastruktury krytycznej, czyli systemy: bankowo-finansowe, energetyczne, wodne, telekomunikacyjne czy transportowe itp.;
- informatyczne systemy przedsiębiorstw, przechowujące informacje strategiczne dla firm: wykorzystywane w produkcji technologie, plany rozwoju itp. (Jędrzejewski, 2002).

Ataki cyberterrorystyczne wykorzystywane są do walki coraz częściej. Napastnik nie naraża w nich bezpośrednio swojego życia i nie musi mieć zbyt wygórowanych umiejętności. Powody wzrostu ich popularności usystematyzował Piotr Sienkiewicz. Wskazał on sześć podstawowych motywów, którymi kierują się terroryści wykorzystując cyberterroryzm do osiągnięcia określonych celów:
- niski koszt działań w porównaniu do regularnych działań zbrojnych;
- łatwość działania poprzez zacieranie granic zarówno pomiędzy państwami, jak i tym, co jest prywatne, państwowe czy wojskowe itd., a nawet pomiędzy stanem wojny a pokojem;
- możliwość dokonywania nagłych i nieprzewidywalnych akcji bez kosztownych i czasochłonnych przygotowań;

– gwarancja całkowitej anonimowości napastników w sieci co daje im możliwość manipulowania informacją oraz utrudnia państwom odparcie ataku i budowanie koalicji;
– minimalne ryzyko wykrycia przygotowywanego ataku;
– możliwość ataku na systemy wrogiego państwa zamiast zabijania niewinnych cywili;
– większy efekt propagandowy i uznanie opinii publicznej (Szubrycht, 2005, s. 50).

Walka z cyberterroryzmem jest dużo trudniejsza niż przy tradycyjnych sposobach działania terrorystów i wymaga znacznie większej koordynacji działań aby zidentyfikować, namierzyć, a następnie zlikwidować napastnika w cyberprzestrzeni.

## Ataki na cele infrastruktury krytycznej

Obecnie nie można wyobrazić sobie życia bez wody, energii elektrycznej, czy innych mediów infrastruktury krytycznej niezbędnych do codziennego funkcjonowania. Obecny rozwój techniki i współczesne społeczeństwo jest całkowicie od nich uzależnione i nie potrafi bez nich żyć. Z tych właśnie powodów cele infrastruktury krytycznej państwa są tak dobrze strzeżone i ochraniane, a jednocześnie stają się łakomym kąskiem dla cyberterrorystów i często przeprowadzane są próby ataków na te cele.

Do głównych celów infrastruktury krytycznej, których zniszczenie lub uszkodzenie może wpłynąć na osłabienie zdolności obronnej lub bezpieczeństwa ekonomicznego państwa można zaliczyć: telekomunikację – linie telefoniczne, satelity, sieci komputerowe; systemy energetyczne – produkcja, przesyłanie i dystrybucja energii wraz z transportem i magazynowaniem surowców niezbędnych do jej produkcji; zasoby gazu ziemnego i ropy naftowej – wydobycie, produkcja, magazynowanie i transport za pomocą rurociągów, statków oraz transportu kołowego i kolejowego; systemy bankowe i finansowe – systemy obiegu, przechowywania i transferu środków finansowych; systemy transportowe – logistyka towarów i osób za pomocą transportu lotniczego, morskiego, kolejowego i drogowego; systemy zaopatrzenia w wodę – ujęcia wody, zbiorniki wodne, wodociągi, systemy filtrowania i oczyszczania wody oraz jej dystrybucji dla rolnictwa, przemysłu oraz odbiorców indywidualnych; zintegrowane systemy służb ratowniczych – koordynacja komunikacji pomiędzy służbami ratunkowymi: służbą zdrowia, strażą pożarną, policją itd.; zapewnienie ciągłości funkcjonowania władzy i służb publicznych – ogół wszystkich elementów niezbędnych do zapewnienia stabilnego funkcjonowania lokalnych, regionalnych i centralnych władz itp. (Verton, 2004).

Najczęstszą formą ataku cyberterrorystów na cele infrastruktury krytycznej jest wpuszczenie do systemów komputerowych wirusów, które paraliżują i uniemożliwiają ich prawidłowe działanie. Rezultatem takiego działania może być np.: utrata kontroli nad systemem, brak komunikacji, czy nawet konieczność wyłączenia systemów. Czynnikiem wzmacniającym działania terrorystów jest wprowadzany przez nich chaos informacyjny podsycany publikowaniem fałszywych informacji na stronach internetowych. Następstwem takich działań jest zamęt i panika panująca w społeczeństwie.

We współczesnych czasach liczba ataków na cele strategiczne stale rośnie. Według raportu za 2011 rok działającego przy Amerykańskim Departamencie Bezpieczeństwa Wewnętrznego, Zespołu ds. Reagowania na Incydenty Komputerowe w Przemysłowych Systemach Kontroli ICS-CERT (*The Industrial Control Systems Cyber Emergency Response Team*) przeprowadzono w samych Stanach Zjednoczonych 198 cyberataków na infrastrukturę przemysłową, z czego zdecydowana większość (41%) skierowana była w sektor energetyczny (Kozłowski, 2014). W stosunku do roku poprzedniego nastąpił 4-ro krotny wzrost ataków na cele infrastruktury krytycznej.

Sektor energetyczny jest kluczowym do funkcjonowania państwa, od jego sprawności uzależnione jest funkcjonowanie wszystkich innych sektorów oraz całego społeczeństwa. Dlatego staje się on celem ataków cyberterrorystów. Niestety nie jest on całkowicie bezpieczny, na jego podatność ma wpływ wiele czynników. Do najistotniejszych należą: popularność systemów sprawujących nadzór oraz kontrolę nad przebiegiem procesów technologicznych i produkcyjnych w energetyce – SCADA (*Supervisory Control And Data Acquisition*); powszechne korzystanie z podwykonawców; wysokie koszty bezpieczeństwa; użytkowanie personalnych urządzeń przenośnych; wytwarzanie i wykorzystywanie niesprawdzonego oprogramowania własnej produkcji; czynnik ludzki (Kozłowski, 2014).

Człowiek, operator systemów komputerowych jest najsłabszym ogniwem w zabezpieczeniach teleinformatycznych, ponieważ często popełnia proste błędy, a jego wiedza na temat bezpieczeństwa jest zazwyczaj niewielka. Do najczęściej popełnianych błędów ludzkich należą: słaba jakość i moc haseł (proste hasła, łatwe do zapamiętania); słabe zabezpieczenie haseł (zapisywanie haseł w pobliżu stanowiska komputerowego w łatwo dostępnych miejscach); uruchamianie zainfekowanych nośników pamięci; uruchamianie zainfekowanej poczty e-mail. Skutecznie przeprowadzony atak cyberterrorystyczny na cele infrastruktury krytycznej wywołuje w społeczeństwie panikę, strach i destabilizuje normalne funkcjonowanie.

## Metody ataków cyberterrorystycznych

Sposobów na wykonanie ataków cyberterrorystycznych jest bardzo wiele, a pomysłowość terrorystów na ich przeprowadzenie stale się rozwija. Sieć internetowa i infrastruktura komputerowa wykorzystywane są w bezpośrednich cyberatakach oraz jako narzędzie do przygotowywania i koordynowania klasycznych ataków terrorystycznych. Ze względu na stale rozwijający się rynek komputerów i cyberprzestrzeni ewoluują również techniki ataków cyberterrorystów. Dlatego nie ma możliwości wymienienia wszystkich narzędzi i sposobów wykorzystywanych przez cyberterrorystów do ataków. Do najczęściej używanych metod ataków komputerowych należą między innymi:

- *backdoor* – specjalne tworzeniu „furtek" w aplikacjach przez programistów;
- robak – złośliwe oprogramowanie samoreplikujące niszczące dane;
- bomba logiczna – fragment kodu zawierający wirusa umieszczony w systemie;
- *cookies* – technika zbierania informacji o użytkownikach komputera;

- *cracking* –wykorzystywanie luki w systemie w celu usunięcia zabezpieczeń;
- *exploit* – złośliwe oprogramowanie pozwalające na bezpośredni dostęp do komputera ofiary;
- *hijacking* – przechwycenie transmisji danych pomiędzy dwoma komputerami;
- inżynieria społeczna – atak wykorzystujący niekompetencję i niewiedzę osób w zakresie działania systemów komputerowych;
- *keylogger* – oprogramowanie do przechwytywania danych wprowadzanych za pomocą klawiatury;
- trojan (koń trojański) – programy pozwalające na wykonanie przez użytkownika nieplanowanego działania, np. usunięcie plików, partycji dysku, czy wysłania danych na wskazany adres e-mail bez wiedzy użytkownika;
- *phishing* – metoda oparta głównie na inżynierii społecznej, polegającej na podszywaniu się pod instytucje celem kradzieży danych;
- *skimming* – nielegalne skopiowanie danych zawartych w pasku magnetycznym karty oraz danych zawartych w chipie znajdującym się na karcie;
- *sniffing* – śledzenie ruchu w sieci i przechwytywanie wysyłanych wiadomości;
- spam – wysyłanie na konto pocztowe atakowanego dużej ilości niechcianych wiadomości tekstowych;
- *spoofing* – podszycie się pod urządzenie w sieci, w celu dokonania włamania do systemu;
- *spyware* – program do szpiegostwa cybernetycznego;
- *wabbit* – złośliwe oprogramowanie powielające plik na dysku komputera w celu wyczerpania pamięci;
- wirus – złośliwe oprogramowanie w postaci samoreplikującego się kodu uszkadzającego dane, programy czy modyfikujące system (Bógdał-Brzezińska, Gawrycki, 2003, s. 98).

Wszystkie te ataki chociaż przeprowadzane w różny sposób mają za zadanie doprowadzić do jednego celu – pozwolić na sparaliżowanie lub nawet zniszczenie zaatakowanego systemu.

## Źródła finansowania cyberterroryzmu

Cyberterroryści przeprowadzający atak zazwyczaj wierzą, że walczą w słusznej sprawie lub dla idei. Zależy im na sławie, nagłośnieniu ataków i wzbudzaniu strachu w atakowanym społeczeństwie. Zorganizowanie zamachu terrorystycznego na dużą skalę przy jednoczesnym uzyskaniu rozgłosu wymaga wielkich nakładów finansowych. Nie wszystkie źródła finansowania cyberterrorystów są oficjalnie znane. Wiadomo jednak, że dzielą się one na legalne i nielegalne.

Do źródeł legalnych należą środki zdobyte w sposób jawny od państw, osób prywatnych, przedsiębiorstw, fundacji, organizacji charytatywnych, akcji humanitarnych, kościołów czy związków wyznaniowych najczęściej z krajów muzułmańskich i wyznawców islamu.

Na źródła nielegalne składają się wpływy z szantaży, okupów i wymuszeń zarówno na rządach, przedsiębiorstwach jak i pojedynczych osobach, prania brudnych pieniędzy, przemytu i produkcji narkotyków, przemytu towarów na znaczną skalę, fałszowania pieniędzy i kart kredytowych oraz napadów na banki czy konwoje (Bernard, 1978, s. 32).

Brak środków finansowych często doprowadza do sytuacji, że planowane zamachy terrorystyczne w ogóle nie dochodzą do skutku, są nieskuteczne, lub realizowane na mniejszą skalę niż były planowane.

## Podsumowanie

Do jednych z największych zagrożeń cywilizacyjnych XXI wieku zalicza się terroryzm, który wywołuje psychozę strachu i powoduje, że w obecnych czasach mieszkaniec żadnego państwa na świecie nie może czuć się bezpiecznym. Jeszcze niedawno ta forma przemocy przybierała postać zamachów bombowych, barykadowania się z zakładnikami czy uprowadzeń. Niestety, rozwijające się systematycznie nowe technologie stały się czynnikiem, który powoduje, że zmienia się również oblicze światowego terroryzmu. Od chwili powstania cyberprzestrzeni coraz większe znaczenie nabiera wykorzystywanie do walki cyberterroryzmu. Napastnikami w tej wojnie są najczęściej pracujący w domu wysokiej klasy eksperci z zakresu informatyki wspierani przez liczne grono analityków i specjalistów wywiadu i kontrwywiadu, a celem jest wniknięcie i przejęcie kontroli nad systemami komputerowymi. Ciągły rozwój i wzrost znaczenia cyberprzestrzeni otworzył przed nimi nowe możliwości zarówno organizowania grup przestępczych jak i prowadzenia szkoleń, czy też koordynowania i przeprowadzania zamachów.

Cyberterroryzm nie ogranicza się jedynie do ludzi dokonujących zamachu, obejmuje również środki finansowe, nowoczesne technologie oraz szeroko rozumianą logistykę. Terroryści werbują ludzi, organizują sprzęt, łączność oraz komunikację a ich działania stanowią wyzwanie dla bezpieczeństwa narodowego i publicznego.

Walka z cyberterroryzmem jest bardzo droga, trudna i mozolna, ze względu na bezmiar cyberprzestrzeni i trudności związane z ich zlokalizowaniem. Jednym ze sposobów na walkę z cyberterroryzmem jest pozbawienie napastników funduszy poprzez likwidację źródeł finansowania. Inną metodą jest wypracowanie stabilnego modelu strategii mogącej wspomagać zwalczanie cyberterrorystów oraz tworzenie porozumień i koalicji międzynarodowych dążących do zwalczania bądź ograniczania cyberterroryzmu, a także likwidacji zakłóceń w funkcjonowaniu krytycznej infrastruktury państw. Zaprezentowane informacje, nie przedstawiają całościowo tematu i należy je traktować, jako zarys problemów związanych ze szkodliwymi działaniami w cyberprzestrzeni.

## BIBLIOGRAFIA


Bernard, A. (1978). *Strategia terroryzmu*. Warszawa: Wydawnictwo Ministerstwa Obrony Narodowej.

Bógdał-Brzezińska, A., Gawrycki, M., (2003). *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie.* Warszawa: Oficyna Wydawnicza ASPRA-JR.

Denning, D.E. (2000). *Cyberterrorism.* Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, Washington, 23 maj 2000, Pobrane z: www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf [dostęp: 27.10.2017].

Denning, D.E., (2002). *Wojna informacyjna i bezpieczeństwo informacji.* Warszawa: Wydawnictwa Naukowo-Techniczne.

*DOD Dictionary of Military and Associated Terms.* Sierpień 2017. Pobrane 13 października 2017, z: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Gogołek, W., (2007). *Manipulacja w sieci.* [w:] B. Siemienicki (red.), *Manipulacja, media, edukacja* (s. 343-358). Toruń: Wydawnictwo Adam Marszałek.

Jędrzejewski, M. (2002). *Analiza systemowa zjawiska infoterroryzmu*. Warszawa: Akademia Obrony Narodowej.

Kośla, R. (2002). *Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski*. Wystąpienie na konferencji w Bemowie, 29 listopada 2002, [cyt. za.] W. Smolski. *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*. Pobrane 23 października 2017, z: www.repozytorium.uni.wroc.pl/Content/66149/32_Wieslaw_Smolski.pdf.

Kozłowski A. (2014). *Cyberbezpieczeństwo infrastruktury energetycznej*, FAE Policy Paper nr 7/2014. Pobrane 27 października 2017, z: http://fae.pl/faepolicypapercyberbezpieczenstwoinfrastrukturyenergetycznej.pdf

Lichocki, E. (2009). *Cyberterroryzm państwowy i niepaństwowy – początki, skutki i formy.* [w:] M.J. Malinowski, R. Ożarowski, W. Grabowski (red.), *Ewolucja terroryzmu na przełomie XX i XXI wieku* (s. 158-171). Gdańsk: Wydawnictwo Uniwersytetu Gdańskiego.

Łapczyński, M., (2009). *Czy grozi nam cyberterroryzm?* Pobrane 13 października 2017, z: http://konflikty.wp.pl/kat,1020225,title,Czy-grozi-nam-cyberterroryzm,wid,11640989,wiadomosc.html.

Szubrycht, T. (2005). *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego.* „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 1.

Tafoya, W.L., (2011). *Cyber Terror.* „Biuletyn służb porządku publicznego FBI", październik 2011. Pobrane 23 października 2017, z: https://leb.fbi.gov/articles/featured-articles/cyber-terror

Verton, D. (2004). *Black Ice. Niewidzialna groźba cyberterroryzmu*. Gliwice: Helion.

Wasilewski, J. (2013). *Zarys definicyjny cyberprzestrzeni.* „Przegląd Bezpieczeństwa Wewnętrznego" nr 9 (5).