MAGDALENA EL GHAMARI
Uniwersytet w Białymstoku
Zakład Bezpieczeństwa Międzynarodowego
elghamari@op.pl

NOWOCZESNE NARZĘDZIA INFORMATYCZNE W WALCE Z EKSTREMIZMEM ISLAMSKIM

MODERN TOOLS IN THE FIGHT AGAINST ISLAMIC EXTREMISM

Piraci komputerowi rozsyłają w świat wirusa, który otwiera na twardym dysku „tylne drzwi", umożliwiające terrorystom zdalne kontrolowanie komputerów elektrowni atomowych, banków, linii lotniczych, laboratoriów farmaceutycznych, wodociągów. Cyfrowa epidemia paraliżuje cały świat[1]

ABSTRACT

Combating terrorism information has become not only an important matter of policy, but also, and perhaps above all, the problem of economic nature. Cyberterrorist can also adjust their activities in order to maximize the positive outcome for themselves. In addition, cyberterrorism does not require physical training or high security logistics. There also requires travel. Cyberterrorism is not a separate or specific type of terrorism because of ideology. It serves exactly the same purpose as bombings, kidnapping or hostage taking. There are only a form – using computer hardware and software.

Cyberattacks do not pose a risk of death or physical injury, reduce the need for so risking life – attacks on the network do not require for suicide attacks. To carry out such an attack, you do not need to have virtually no skill – you can rent a cracker who broke security (often without realizing the consequences of his actions) money will carry out a terrorist attack.

Past examples of cyber crimes show how a large number of people may be affected by the consequences of such action; this is due to the global nature of computerization. Thus one of the essential objectives of terrorists – mediality attack – is huge. A separate issue is the use of the Internet and computers

[1] Meyer E., Kerdellant Ch., *Cyfrowa katastrofa*.

by terrorists for purposes other than direct attacks. Computer systems are a great collection and exchange of information and communication. They provide anonymity, allow coding or hiding information. Transfers can be hidden do not raise suspicions text files or graphics.

Keywords: *extremism, radicalization, modern technology, cyberterrorism*

STRESZCZENIE

Zwalczanie terroryzmu informatycznego stało się nie tylko ważnym zagadnieniem natury politycznej, ale również, a może przede wszystkim, problemem natury ekonomicznej. Cyberterroryści mogą również dostosować swoje działania tak, aby zmaksymalizować pozytywny dla siebie wynik. Ponadto cyberterroryzm nie wymaga treningu fizycznego ani dużego zabezpieczenia logistycznego. Nie wymaga również podróżowania. Cyberterroryzm nie jest odrębnym lub specyficznym rodzajem terroryzmu ze względu na ideologię. Służy dokładnie tym samym celom co zamachy bombowe, porwania oraz branie zakładników. Wyróżnia się tylko formą – zastosowaniem sprzętu i oprogramowania komputerowego.

Ataki w cyberprzestrzeni nie stwarzają ryzyka poniesienia śmierci lub obrażeń fizycznych, ograniczają więc konieczność narażania życia – zamachy w sieci nie wymagają bowiem ataków samobójczych. Aby przeprowadzić taki atak, nie potrzeba posiadać praktycznie żadnych umiejętności – można wynająć crackerów, którzy łamiąc zabezpieczenia (często nie zdając sobie sprawy ze skutków swojego działania), za pieniądze przeprowadzą atak terrorystyczny.

Dotychczasowe przykłady przestępstw informatycznych pokazują, jak wielka liczba ludzi może być dotknięta skutkami takiego działania; wynika to z globalnego charakteru informatyzacji. Tym samym jeden z zasadniczych celów terrorystów – medialność ataku – jest przeogromny. 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 niebudzących podejrzeń plikach tekstowych czy graficznych.

Słowa kluczowe: *ekstremizm, radykalizacja, nowoczesna technologia, cyberterroryzm*

WPROWADZENIE

Do podstawowych zasad rządzących współczesnym światem należą: zmienność, ekspansywność oraz z pewnością żywotność. Jedna sekunda w sieci 3 października 2016 roku w skali światowej oznaczała:

- 7363 wysłane nowe tweety,

- 744 nowe zdjęcia na Instagramie,
- 1164 nowe posty na Tumblr,
- 2294 rozmowy prowadzone za pomocą komunikatora Skype,
- 38 456 GB nowych danych,
- 56 538 wyszukiwań fraz oraz słów w wyszukiwarce Google,
- 132 412 obejrzanych filmów na YouTubie,
- 2 528 192 wysłanych maili[2].

Jak pokazuje to krótkie doświadczenie, dostęp do tej kompleksowej sieci wymiany doświadczeń oraz wiedzy staje się przymusem w obecnym świecie. Chcąc nadążać za współczesnym światem i jednocześnie nowymi technologiami, nie mamy wyboru – musimy płynąć z nurtem wiedzy zanurzonej w technologii. Świat, jaki powstaje poprzez fundamentalne zmiany, które nastąpiły wraz z rozwojem Internetu, ciągle wywołuje transformację, której efektów nie jesteśmy w stanie przewidzieć. Zmiana społeczna, kulturowa, ekonomiczna, nowa jakość zagrożeń. To wszystko to jedynie początek tego, co przyniosła nam rewolucja technologiczna XXI wieku – kultura cyberprzestrzeni, wirtualne społeczności, nowy język sieci, owe wzory interakcji międzyludzkich. Wszystko to warunkuje stwierdzenie, że funkcjonujemy w obszarze czterech społeczności etnicznych w sieci: społeczeństwo wirtualne, gdzie ludzie kontaktują się wyłącznie przez Internet; społeczeństwo obywatelskie, którego celem jest rozpowszechnianie informacji dotyczącej danej grupy oraz działania systemu demokratycznego; społeczeństwo dyskusyjne – jego członkowie skupiają się wokół wybranego problemu, forum dyskusyjnego, zainteresowań, oraz społeczeństwo wspomagające, gdzie ludzie kontaktują się zarówno przez Internet, jak i w świecie rzeczywistym.

CYBERTERRORYZM

Po raz pierwszy termin „cyberterroryzm" użyty został w 1979 roku przez szwedzkie Ministerstwo Obrony w raporcie o zagrożeniach komputerowych. Cyberterroryzm, zwany również hi-terroryzmem albo terroryzmem informacyjnym, jest połączeniem dwóch słów: cyberprzestrzeni i terroryzmu. Czym jest cyberprzestrzeń? To przestrzeń komunikacyjna tworzona przez system powiązań internetowych. Jeśli chodzi o sam

[2] http://www.internetlivestats.com/one-second/ [data dostępu: 3.10.2016].

terroryzm, terminów i definicji jest wiele. Ogólnie rzecz biorąc, jest to fakt dokonywania aktów terroru z pobudek politycznych, powodujących ogromne straty i wywołujących powszechne poczucie strachu. W cyberterroryzmie broń zastąpiona zostaje komputerem podłączonym do sieci, a atak wymierzony jest w system informatyczny państwa i znajdujące się w nim dane. Przeważnie atak taki skutkować ma uniemożliwieniem efektywnego wykorzystania najważniejszych gałęzi gospodarki państwa, takich jak infrastruktura bankowa, transport, energetyka czy instytucje państwowe (E. Aronson, A. Pratkanis, 2004, s. 41).

Tezą niniejszego artykułu, poddaną wnikliwej analizie, jest stwierdzenie, że każde państwo może być zagrożone atakiem cyberterrorystów. Niestety, ze szkodami tym większymi, im bardziej skomputeryzowana jest gospodarka danego kraju. Co więcej, każde państwo może dokonać ataku cybernetycznego, jeżeli tylko znajdą się w nim profesjonalni hakerzy, zdolni, zmotywowani i gotowi do jego przeprowadzenia.

Termin „cyberterroryzm" poruszył Barry Collin z Institute for Security and Intelligence w Kalifornii (J. Adamski, 2007, s. 56). Stworzył termin „cyberterroryzm" jako pojęcie zbieżne dla przestrzeni cybernetycznej i terroryzmu. Natomiast Mark Pollit, agent FBI, zaproponował definicję roboczą: „Cyberterroryzm to zamierzony, motywowany politycznie atak na informację, system komputerowy, programy komputerowe i dane, którego skutkiem jest użycie przemocy wobec celów niewalczących przez grupy ponadnarodowe bądź tajnych agentów" (M. Pollit, październik 1997, s. 285–289).

Później pojawiały się kolejne definicje starające się uzupełnić ciągle ewoluujący termin. Według US Federal Bureau of Investigation: „(...) jest to obmyślony, politycznie umotywowany akt przemocy wymierzony przeciwko informacjom, programom, systemom komputerowym lub bazom danych, który mając charakter niemilitarny, przeprowadzony jest przez ponadnarodowe lub narodowe grupy terrorystyczne", zaś Dorothy Denning stwierdza, że jest to „(...) groźba lub bezprawny atak wymierzony w system informatyczny lub zgromadzone dane, w celu zastraszenia czy wymuszenia na władzach państwowych lub jej przedstawicielach ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych celów (np. politycznych). Aby działania takie zostały zakwalifikowane jako terroryzm informacyjny, atak powinien powodować znaczne straty lub takie skutki, które wywołu-

ją powszechne poczucie strachu". Inny badacz, James Lewis, konkluduje, iż cyberterroryzm to: „wykorzystanie sieci komputerowych jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe itp.) bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań". Według US National Infrastructure Protection Centre jest to: „akt kryminalny popełniony przy użyciu komputera i możliwości telekomunikacyjnych, powodujący użycie siły, zniszczenie i/lub przerwanie świadczenia usług dla wywołania strachu, poprzez wprowadzanie zamieszania lub niepewności w danej populacji, w celu wpływania na rządy, ludność tak, aby wykorzystać ich reakcje dla osiągnięcia określonych celów politycznych, społecznych, ideologicznych lub głoszonego przez terrorystów programu" (R. Kosta, 2007, s. 27). Analiza przedstawionych definicji pozwala zaobserwować pojawiające się w nich dwa zasadnicze wyróżniki. Definicje cyberterroryzmu uzupełniają się i uwzględniają to, że istnieje możliwość wykorzystania systemów komputerowych lub telekomunikacyjnych do przeprowadzenia ataku cybernetycznego. Ponadto powyższe definicje zawierają określenie, że komputery i systemy informacyjne są celem takiego ataku. Problematyczne staje się to, iż wielokrotnie cyberterroryzm i cyberatak są traktowane jako elementy równoważne, co w konsekwencji prowadzi do nieporozumień. D. Denning uważa, że politycznie umotywowany cyberatak, który prowadzi do śmierci, ofiar lub uszkodzeń ciała, eksplozji bądź poważnych strat materialnych, może być przykładem cyberterroryzmu[3]. Takim działaniem nie jest przypadek ataku, który jedynie zakłóca przyjęty porządek prawny lub ekonomiczny lub taki, który nie pociąga za sobą zasadniczych zakłóceń lub strat. Opierając się na wybranych wskaźnikach i wybiórczym traktowaniu przedstawionych definicji, należy stwierdzić, że do tej pory nie było przypadku cyberterroryzmu (D. Denning, 2002, s. 77). Jeśli zaś zastosuje się kryteria kwalifikacyjne, okazuje się, że zdarzyło się kilka przypadków takich działań. Nie były one jednak poparte motywacją polityczną lub inną, która kwalifikowałaby je jako przypadki terroryzmu[4].

[3] D. Denning, *Cyberterrorism*, http://www.cs.georgetown.edu/ ~denning/infosec/cyberterror-GD.doc [data dostępu: 24.08.2000].

[4] L. Garrison., M. Grand, *Cyberterrorism: An evolving concept, NIPC Highlights*, http://www.nipc.gov/publications/highlights/2001/ highlight-01-06.htm 6.

Efekty działań zagrożeń cyberterrorystycznych można sklasyfikować za pomocą poniższego podziału:

- małe skutki ekonomiczne zakłócenia systemu informatycznego,
- małe skutki ekonomiczne zakłócenia systemu informatycznego połączone z ofiarami,
- poważne skutki ekonomiczne zakłócenia systemu informatycznego,
- poważne skutki ekonomiczne zakłócenia systemu informatycznego połączone z ofiarami,
- działania stanowiące zagrożenie dla bezpieczeństwa narodowego[5].

Charakter działań cyberterrorystów można podzielić na: działania bezprawne, hakerstwo, szpiegostwo, cyberterroryzm i cyberagre. Ponadto na działalność cyberterrorystyczną składa się wiele technik. Część z nich może być stosowana praktycznie przez każdego członka organizacji, natomiast pozostałe wymagają dużych umiejętności praktycznych oraz właściwego przygotowania teoretycznego. Jedną z technik jest tzw. *web sit-in*, czyli okupowanie sieci przez dużą liczbę użytkowników w tym samym czasie, powodując przez to utrudnienie lub brak możliwości wywołania strony (D. Verton, 2004, s. 133). Takie zdarzenie miało miejsce chociażby w listopadzie 2000 roku po wybuchu powstania palestyńskiego, gdy witrynę IDF okupowało tygodniowo blisko 130 tys. osób, podczas gdy przed wybuchem zamieszek stronę odwiedzało około 7 tys. internautów. Skuteczność kolejnej techniki zwanej *flooding* przedstawia atak separatystów tamilskich na serwery ambasad Sri Lanki w 1998 roku. Polegał on na wysyłaniu około 1 tys. e-maili przez okres dwóch tygodni z oświadczeniem kwestii roszczeń niepodległościowych, zakończonych informacją mówiącą o celowości działań. Atak całkowicie sparaliżował komputerowy system łączności MSZ Sri Lanki oraz systemy informatyczne kilku ambasad tego państwa. W ostatnim okresie wśród zwolenników radykalnych islamistów można zaobserwować zjawisko postępującej koordynacji ataków tego typu. Przygotowania do nich są zapowiadane z wyprzedzeniem na internetowych forach dyskusyjnych. Koordynaty oraz termin i czas ataków podaje się dopiero około 30 minut przed ich dokonaniem. Czę-

[5] L. Staten Clark, zeznanie przed Subcommitte of Technology, Terrorism and Government Information, U.S. Senate Judiciary Committee [data dostępu: 24.02.1998].

sto dołączane jest również specjalistyczne oprogramowanie opracowane przez islamistyczne grupy hakerskie, np. Al-Jihad czy Dorach War Engine (M.F. Gawrycki, 2003, s. 166–167).

Najnowsze wersje programów opracowywanych przez radykalnych islamistów umożliwiają zdalne ładowanie obiektów ataków ze stron ich administratorów oraz synchronizowanie akcji z innymi uczestnikami. W atakach uczestniczy zwykle kilka tysięcy osób. Mimo że skuteczność takich działań jest obecnie niewielka, zagrożenia nie można lekceważyć, ponieważ islamiści nie rezygnują z prowadzenia takich akcji i stale udoskonalają wykorzystywane oprogramowanie. O wysokich ambicjach ich działań świadczy planowany zmasowany atak przeciw serwerom wybranych banków amerykańskich w grudniu 2006 roku pod nazwą „The Electronic Guantanamo Raid". Ostatecznie został on jednak odwołany najprawdopodobniej z powodu dekonspiracji[6].

Kolejne zagrożenie wiązało się z możliwością wprowadzenia do systemów szkodliwego oprogramowania. Rozpowszechnione i łatwo dostępne w Internecie automatyczne generatory są w stanie utworzyć nieskomplikowane wirusy i robaki. Takie oprogramowanie usiłował nabyć pod koniec 1998 roku Khalid Ibrahim, członek powiązanego z Al-Kaidą separatystycznego ugrupowania Hakat-ul-Ansar, działającego w Indiach. Opierając się na amerykańskich źródłach, z pełną odpowiedzialnością można stwierdzić, że organizacje terrorystyczne mają już specjalistów zdolnych do tworzenia szkodliwego oprogramowania. Agencja Bezpieczeństwa Narodowego Stanów Zjednoczonych (NSA) wskazuje, że tylko do końca 2001 roku około 60% dyplomów ukończenia studiów uniwersyteckich przez studentów zagranicznych w USA na kierunkach związanych z informatyką uzyskali obywatele państw muzułmańskich. Wynika z tego, że Amerykanie sami szkolą swoich potencjalnych wrogów, a także wrogów całej cybernetyki. Sytuacja jest o tyle groźna, że duża część grupy absolwentów nie wróciła do swoich państw, lecz została w USA (K. Kerr, 2003, s. 29).

Pewną klasyfikację osób dokonujących ataków w cyberprzestrzeni (ze względu na motywacje polityczne) podaje Dorothy E. Denning. Wyróżnia ona (oprócz hakerów) także: aktywistów, haktywistów i cyberterrorystów. Ponadto wyróżnia się grupy zorganizowane i cyberterrorystów indywidualnych.

[6] I. Bunsch., J. Świątkowska, *Cyberterroryzm – Nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI wieku*, s. 17, http://ik.org.pl/pl/ publikacja/nr/4298/ [data dostępu 15.06.2012].

Wszystkie organizacje terrorystyczne, które korzystają z sieci, charakteryzują się pewnymi cechami. Są to przede wszystkim:

- budowanie i zmienianie komunikacji oraz koordynacji stosownie do zadań,
- nieformalne powiązania o różnym stopniu intensywności (zależnie od potrzeb),
- brak biurokratycznego zarządzania, lecz więzy wewnętrzne i zewnętrzne umożliwiające podzielanie wspólnych norm i wartości oraz wzajemne zaufanie,
- uzupełnianie wewnętrznych sieci przez łączność z osobami niezwiązanymi z organizacją (możliwość wychodzenia poza granice państw) (por. B. Adkins, 2001, s. 51).

Systemy informatyczne, które mogą być zaatakowane, to między innymi:

- systemy, które wspomagają zarządzanie transportem (szczególnie kolejowym) oraz ruchem powietrznym,
- systemy, które wykorzystywane są w instytucjach państwowych, a których działanie opiera się na sprawnym funkcjonowaniu baz danych,
- systemy powiadamiania służb ratowniczych i reagowania antykryzysowego,
- systemy, które pracują w różnych sektorach – np. bankowości – oraz stosowane są przy produkcji i dystrybucji dóbr o strategicznym znaczeniu (energia elektryczna, woda, gaz, ropa) (zob. P. Monge, F. Janet, [w:] Shaping G. Desanctis, J. Fulk, 1999 s. 58–61).

Ataki te mogłyby zniszczyć lub przerwać działanie infrastruktury krytycznej państwa poprzez wykorzystanie słabości komputerowych. Do głównych elementów tej infrastruktury zalicza się:

- telekomunikację: linie telefoniczne, satelity, sieci komputerowe, komercyjne, wojskowe, akademickie,
- system energetyczny: produkcja, przemysł i dystrybucja energii oraz transport i magazynowanie surowców niezbędnych do jej produkcji,
- produkcję, magazynowanie i transport gazu ziemnego i ropy naftowej: cały proces wydobycia ropy naftowej i gazu ziemnego,
- przetwarzanie, magazynowanie i transportu za pomocą statków, rurociągów, transportem kolejowym i kołowym,

- system bankowy i finansowy: system przepływu kapitałów,
- transport: lotniczy, kolejowy, morski, rzeczny, drogowy osób i towarów oraz system wsparcia logistycznego,
- system zaopatrzenia w wodę: ujęcia wody, zbiorniki wodne, wodociągi, systemy filtrowania i oczyszczania wody, dostarczania jej dla rolnictwa, przemysłu, straży pożarnych i indywidualnych odbiorców,
- służby ratownicze: komunikacja ze służbą zdrowia, strażą pożarną i policją,
- ciągłość funkcjonowania władzy i służb publicznych.

Wśród obiektów infrastruktury krytycznej należy wymienić również tzw. krytyczną infrastrukturę teleinformatyczną, na której działaniu opiera się większość systemów odpowiedzialnych za prawidłowe funkcjonowanie większości instytucji i przedsiębiorstw w państwie. Działanie tej infrastruktury oparte jest na prawidłowym działaniu wielu systemów na nią złożonych.

Obecnie można wyróżnić trzy poziomy zagrożenia związanego z cyberterroryzmem. Pierwszym z nich jest tzw. *simple-unstructured*. Polega on na dokonaniu przez cyberterrorystów prostych włamań do indywidualnych systemów informacyjnych poprzez wykorzystanie narzędzi internetowych skonstruowanych przez inną osobę. Zgodnie z tym organizacje terrorystyczne nie mają zdolności analizy celów, które będą przedmiotem ataku, a także dowodzenia, kontroli czy uczenia się nowych metod atakowania w cyberprzestrzeni. Drugim poziomem zagrożenia jest tzw. *advanced-structured*. W poziomie tym cyberterroryści dokonują bardziej skomplikowanych ataków przeciw złożonym sieciom komputerowym i systemom. Mają możliwość tworzenia lub modyfikacji własnych narzędzi, które służą do atakowania w cyberprzestrzeni, mają zdolność analizy celów, które będą przedmiotem ataku, a także dowodzenia, kontroli i uczenia się nowych metod atakowania. Ostatnim – najpoważniejszym – poziomem zagrożenia jest tzw. *complex-coordinated*. Cyberterroryści dokonują tu skoordynowanych ataków mających na celu totalną destrukcję zintegrowanego systemu obronnego, mają możliwość tworzenia skomplikowanych narzędzi, które służą do niszczenia celów w cyberprzestrzeni, a także analizy celów będących przedmiotem ataku. Mogą dowodzić, kontrolować, jak również samodoskonalić się (zob. S. Serwiak, [w:] E. Pływaczewski, 2005, s. 589–613).

Niezwykle istotne jest podkreślenie, że organizacje terrorystyczne, które posługują się nowymi technikami, można (zdaniem A. Rathmella) podzielić na trzy kategorie:

- kategoria I, która obejmuje nowe techniki używane przez terrorystów do prowadzenia tradycyjnej działalności. Internet wykorzystuje się tutaj do zbierania informacji, komunikacji, zdobywania środków finansowych i komunikacyjnych,
- kategoria II, w której wykorzystywane są stare techniki do nowej działalności. Używana jest tutaj siła fizyczna, która ma na celu zniszczenie systemu informacyjnego,
- kategoria III, w której używa się nowe techniki do nowych działań – jest to atak w cyberprzestrzeni na system informacyjny (H. Münkler, 2004, s. 21).

Należy również pamiętać, że nie da się z działalności w sieci wykluczyć wszystkich agresorów. Richard Clarke w wywiadzie dla autora Dana Vertona twierdzi również: „załóżmy dla przykładu, że następny atak jest planowany przez Al-Kaidę. Nawet gdyby udało się dobrać im do skóry i wyeliminować całkowicie albo zmniejszyć do pozbawionej znaczenia grupki, nie wyeliminuje to całkowicie zagrożenia w cyberprzestrzeni. Ktoś inny wyszuka słabe punkty naszych systemów i wykorzysta je do ataków. Nie ma co zgadywać, kto będzie następnym atakującym, nawet gdyby w końcu udało się go wyśledzić i zrobić z nim, co należy. Trzeba zająć się słabościami, które umożliwiają ataki. Dopóki sobie z nimi nie poradzimy, dopóty będziemy narażeni na ryzyko ataków". Działalność cyberterrorystów w sieci jest bardzo poważnym problemem, gdyż ich poczynania są ukryte. Z uwagi na łatwość maskowania tożsamości można mówić o relatywnej anonimowości atakujących, którzy bez obaw, że zostaną wykryci, przeprowadzają za pomocą sieci wrogie działania. Wynika stąd kolejny problem – skala potencjalnych strat, zarówno pod względem finansowym, jak i bezpieczeństwa, jest trudna do oszacowania.

KLASYFIKACJA ATAKÓW

Pierwszą zaprezentowaną metodą klasyfikacji jest lista siedmiu kategorii działań w cyberprzestrzeni, opracowana przez S. Bellovina i W. Cheswicka:

- *stealing passwords* (kradzież haseł) – metoda polegająca na uzyskaniu haseł dostępu do sieci,

- *social engineering* (inżynieria społeczna) – wykorzystanie niekompetencji osób mających dostęp do systemu,
- *bugs and backdoors* (błędy i tylne drzwi) – używanie oprogramowania z nielegalnych źródeł lub korzystanie z systemu bez specjalnych zezwoleń,
- authentication failures (błędy uwierzytelniania) – zniszczenie lub uszkodzenie procedur mechanizmu autoryzacji,
- *protocol failures* (błędy protokołu) – wykorzystywanie luk w zbiorze reguł, które sterują wymianą informacji pomiędzy dwoma lub wieloma niezależnymi urządzeniami bądź procesami,
- *information leakage* (wyciek informacji) – uzyskanie informacji dostępnych tylko administratorowi, które niezbędne są do poprawnego funkcjonowania sieci,
- *denial of services* (odmowa usługi) – uniemożliwienie użytkownikom korzystania z systemu (D.E. Denning, [w:] J. Arquilla, D. Ronfeldt, 2001, s. 239–262).

F. Cohen, mając na uwadze powyższą listę kategorii, stworzył własną kategoryzację, która uwzględniała przede wszystkim rezultat ataku w cyberprzestrzeni. Rozpatrywane kategorie to:

- *corruption* – nieuprawniona zmiana informacji,
- *leakage* – informacja znalazła się w niewłaściwym miejscu,
- *denial* – kiedy komputer lub sieć nie nadają się do użytkowania (A. Bogdół-Brzezińska, M.F. Gawrycki, 2003, s. 73).

Warto zauważyć, że wielu specjalistów (w tym J. Howard i T. Longstaff) podkreśla, iż działania w sferze cyberprzestrzeni nie da się zakwalifikować tylko do jednej kategorii. Często są to akcje mieszczące się w wielu kategoriach. W efekcie takiego ujęcia P. Neumann i D. Parker zaproponowali następujący podział, który opiera się na dostępnych danych empirycznych:

- *external information theft* – przeglądanie oraz kradzież informacji przez osobę spoza systemu,
- *external abuse of resources* – zniszczenie twardego dysku,
- *masquerading* – podawanie się za kogoś innego,
- *pest programs* – zainstalowanie złośliwego programu,
- *bypassins authentication or authority* – złamanie haseł,
- *authority abuse* – fałszowanie danych,

- *abuse through inaction* – celowe prowadzenie złego zarządzania,
- *indirect abuse* – używanie innych systemów do stworzenia „złośliwych" programów (M. Zanini, S.J.A. Edwards, [w:] J. Arquilla, D. Ronfeldt, 2001, s. 29–60).

Atakujący dokonują uderzenia w niecodziennych sytuacjach. Wynika stąd, że działań w sferze cyberprzestrzeni nie da się zakwalifikować wyłącznie do jednej kategorii.

Klasyfikacja oparta na działaniu polega na czterech rodzajach ataków zdefiniowanych przez W. Stallingsa. Ma jednak ona ograniczoną możliwość zastosowania, gdyż dotyczy jedynie ataków traktowanych jako seria działań. Są to:

- *interruption* (przerwanie) – nie można zastosować zabezpieczenia systemu lub zostało ono zniszczone,
- *interception* (przechwytywanie) – dostęp do istniejących zabezpieczeń zdobyła nieuprawniona osoba,
- *modification* (modyfikacja) – nieuprawniona osoba zdobyła dostęp, a także manipulowała zabezpieczeniem,
- *fabrication* (produkcja) – przez nieuprawnioną osobę do systemu wprowadzony został sfałszowany obiekt (B. Hoffman, 1998, s. 131–134).

Początki pierwszych ataków. Pierwsze wzmianki o niebezpieczeństwie zamachów terrorystycznych przy użyciu systemów komputerowych pojawiły się w 1979 roku w raporcie szwedzkiego ministerstwa obrony na temat zagrożeń społecznych związanych z komputeryzacją. W wypowiedziach amerykańskich specjalistów w dziedzinie wywiadu wojskowego samo słowo „cyberterroryzm" zaczęło być używane już w latach 80. O tej nowej formie terroryzmu zaczęto mówić coraz częściej (S. Reeve, 1999). Na przełomie lat 80. i 90. XX wieku medialną gwiazdą został Kevin Mitnick. Na liście poszukiwanych przez FBI oszustów komputerowych zajmował pierwsze miejsce. Został schwytany w 1995 roku i skazany wyrokiem sądu na wieloletnie pozbawienie wolności uzasadnieniem: „uzbrojony w klawiaturę, jest groźny dla społeczeństwa". Był znakomitym hakerem, włamał się m.in. do komputerów Pentagonu, laboratorium Digital Equipment Corporation, banków i sieci telefonicznej Pacific Bell, z których wykradał tajne dane. Po odbyciu wyroku został konsultantem firmy zabezpieczającej komputery, a narzędzia, których

używał w czasie włamań, zostały wykorzystane w systemach zabezpieczeń wielu krajów. Zbieranie informacji oraz operacje psychologiczne i manipulowanie percepcją w wojnie informacyjnej stosowali również terroryści. Niektóre grupy w swoich działaniach wykorzystywały Internet do propagandy i zbierały informacje z różnych bezpośrednio przyłączonych źródeł. Clark Staten, dyrektor ENRI (Emergency Response & Research Institute – Instytut Badania Nagłych Sytuacji i Reagowania) w lutym 1998 roku zeznał przed podkomisją senatu amerykańskiego, że „nawet małe grupy terrorystyczne korzystają teraz z Internetu do nadawania komunikatów i jednoczesnego wprowadzania w błąd ludności wielu krajów". Przekazał on również kopie komunikatów z propagandą antyamerykańską i antyizraelską oraz groźbami, gdzie szeroko było rozpowszechniane hasło ekstremistów wzywające do „dżihadu" przeciw Ameryce i Wielkiej Brytanii. W czerwcu tego samego roku w US News & World Report podano, że z 30 grup terrorystycznych (które umieszczone są na liście amerykańskiego Departamentu Stanu) 12 znajduje się w Internecie i nie można zmusić ich do opuszczenia sieci (zob. M. Whine, 1999).

W 1997 roku amerykański nastolatek unieruchomił główną kampanię telefoniczną obsługującą mały port lotniczy w Worcester (Massachusetts) na sześć godzin. W tym czasie wieża kontrolna nie miała możliwości świadczenia usług normalnymi kanałami. Bezpieczeństwo lotów zapewniono dzięki informacjom przekazywanym samolotom przez inne porty lotnicze drogą radiową. Jak wielkie zagrożenie stanowią takie ataki, można sobie uświadomić, analizując dane dotyczące ataków informatycznych, które wykonywane są na pozawojskowe systemy informatyczne. W 2003 roku szacunkowe straty wywołane takimi atakami wyniosły 82 mld dolarów. Na świecie ich liczba systematycznie wzrasta.

W lutym 1998 roku to, co było tematem Eligible Receiver, stało się rzeczywistością – dokonano kilkuset ataków na serwery Departamentu Obrony. Zastępca sekretarza obrony John Hamre określił to jako „najlepiej zorganizowany atak w historii" i przyznał, że jeszcze nigdy nie był atakowany w tak systematyczny sposób. Początkowo sądzono, że atak ten był sponsorowany przez Irak, a celem było uniemożliwienie wysłania sprzętu i posiłków na Zatokę Perską. Okazało się jednak, że atakującymi byli 18-latek z Izraela i dwóch 16-latków z Kalifornii. Hakerzy, po dostaniu się do komputerów, zainstalowali program do przeszukiwania danych, dzięki czemu mogli zdobyć hasła do komputerów wojskowych i rządowych. Mieli też dostęp do serwerów

z kontami osobistymi. Strony rządowe, tak jak i prywatne, są bardzo podatne na tego typu ataki. Wskutek działań hakerów bardzo szybko można narobić sporego zamieszania. Ważne jest, aby pamiętać, iż jeśli nie zadbamy o bezpieczeństwo, ataki w przyszłości będą się stawały coraz groźniejsze.

W 2000 roku hakerzy należący do Pakistan Hackerz Club skradli numery kart kredytowych około 700 członków i fundatorów proizraelskiej organizacji Amerykańsko-Izraelskiego Komitetu Spraw Publicznych, działającego na terenie Stanów Zjednoczonych. Kolejnym sposobem pozyskania w nielegalny sposób środków finansowych jest wykorzystanie grup hakerskich do ataków wymierzonych w systemy informatyczne instytucji finansowych. Jesienią 2000 roku, działając na zlecenie Hezbollahu, podczas tzw. drugiej intifady, hakerzy spenetrowali systemy informatyczne zarządzane przez Bank Izraela i giełdę w Tel Awiwie. Dane dotyczące liczby ataków nie są w tym przypadku znane, powodem jest oczywiście dbałość o renomę instytucji oferujących usługi w sektorze finansowo-bankowym. Każdy ujawniony atak to potencjalnie mniej klientów obawiających się o bezpieczeństwo swoich oszczędności (J. Stern, 2000, s. 115–126).

Al-Kaida, chcąc wzbudzić nieufność obywateli państw zachodnich do oficjalnej polityki informacyjnej, podejmuje próby prostowania lub dementowania informacji podawanych przez oficjalne ogólnoświatowe serwisy informacyjne. W artykule „Świadectwo Talibanu" z 2002 roku na stronie Al Neda oskarżono „zachodnie i wschodnie" media o demonizowanie i pozbawienie czci talibów, poprzez opisywanie ich w wulgarny sposób, jako wrogo usposobionych fanatyków, którzy prześladują kobiety i mniejszości narodowe. Przykładem operacji nakierowanej na dążenie do wywierania presji na władze poprzez wywołanie poczucia zagrożenia wśród obywateli była kampania psychologiczna prowadzona przez Al-Kaidę w październiku i listopadzie 2001 roku (zob. Organised Crime Situation Report 2004, Focus on the Threat of Cybercrime, 2003, s. 125). Terroryści w Pakistanie dążyli do wywołania fali demonstracji i zamieszek przeciwko udziałowi tego państwa w koalicji antyterrorystycznej oraz wspieraniu operacji wojskowej w Afganistanie. Przedstawiciele Al-Kaidy wydali ostrzeżenia za pośrednictwem prasy i Internetu, że w przypadku amerykańskiego ataku na Afganistan przeprowadzą szereg zamachów na terenie Pakistanu z wykorzystaniem broni jądrowej. Było to niedługo po atakach na World Trade Center w 2001 roku, dlatego też opinia publiczna traktowała groźby z pełną

powagą. Pakistan uległ groźbom i ograniczył swoją pomoc do pozornej kontroli na granicy z Afganistanem. Następnym krokiem był apel przywódcy talibów mułły Omara, z dnia 23 października 2006 roku, aby państwa Organizacji Traktatu Północnoatlantyckiego wycofały swoje wojska z Republiki Afganistanu i zaprzestały tym samym poświęcać życie swoich żołnierzy dla realizacji interesów Stanów Zjednoczonych. Al-Kaida stale prowadzi kampanię psychologiczną skierowaną w stronę ludności państw zachodnich. Takim przykładem była wypowiedź przedstawiciela tej organizacji, Sulaimana Abu Ghaithema, że w kolejnych zamachach na Amerykę ucierpi około 4 mln obywateli tego kraju w wyniku użycia broni chemicznej i biologicznej. Specjalnością talibów w zakresie zastraszania stało się również publikowanie egzekucji pojmanych zakładników. Ponieważ wszystkie stacje telewizyjne odmówiły emisji materiałów wideo, z uwagi na makabryczną zawartość, przedstawiających śmierć niewinnych ludzi poprzez odcięcie głowy, zapisy z egzekucji są publikowane w Internecie. Martwi fakt ogromnego zainteresowania takimi filmami zwłaszcza przez internautów z państw zachodnich. Ugrupowania terrorystyczne zamieszczają także na swoich stronach pliki wideo zachęcające do wstępowania w ich szeregi. W przypadku Al-Kaidy były to między innymi wystąpienia nagrane w Finsbury Park w Londynie i umieszczone na stronie Haganah. Jak to możliwe, że w stolicy Anglii zostały nagrane takie materiały. Otóż w tym czasie Finsbury Park w Londynie był zarządzany przez radykalnego islamistę Abu Hanza al-Masri powiązanego z Al-Kaidą, zanim został aresztowany 27 maja 2004 roku.

W listopadzie 2001 roku w Australii Vitek Boden został skazany na dwa lata więzienia za wykorzystanie Internetu, radia i ukradzionego oprogramowania do wypuszczenia miliona litrów ścieków do rzeki i wód przybrzeżnych Maroochydore w Queensland w Australii. Skazany był konsultantem przy opracowywaniu projektu wodnego. Opisany atak przeprowadził w marcu 2000 roku, po tym jak odrzucono jego kandydaturę na pracownika władz hrabstwa Maroochy. W efekcie jego działań na akwenie objętym wyciekiem zamarło życie biologiczne, a mieszkańcy tego rejonu ze względu na panujące warunki musieli na wiele tygodni opuścić miejsce zamieszkania.

Rosnące zagrożenie cyberterrorystyczne zauważono także w 2002 roku, kiedy CIA w liście przesłanym do przewodniczącego Senackiej Komisji specjalnej do spraw wywiadu – senatora Boba Grahama – stwierdza, że „(...) Al-Kaida i różne sunnickie grupy ekstremistyczne popierające działania

antyamerykańskie prawdopodobnie spróbują dokonać w przyszłości ataku cybernetycznego. Jest to zgodne zarówno z ich intencjami, jak i z żądzą rozwijania umiejętności hackerskich i informatycznych potrzeb do stworzenia efektywnego modus operandi, nieodzownego do dokonywania skutecznych cyberataków (...). Przeprowadzenie cyberataków na systemy staje się coraz bardziej możliwe dla terrorystów – w miarę zapoznawania się przez nich z celami ataków i technologiami potrzebnymi do ich przeprowadzenia. Różne grupy terrorystyczne, łącznie z Al-Kaidą i Hezbollahem, coraz skuteczniej posługują się technologiami internetowymi i komputerowymi – FBI odnotowuje rosnącą liczbę zagrożeń" (R. Borkowski, 2006, s. 51).

W 2008 roku również doszło do ataków cybernetycznych. Miały one miejsce w Gruzji, a odbyły się równolegle do konwencjonalnych działań wojennych. Doszło wtedy do zmasowanych ataków na gruzińskie strony internetowe, a zniekształcone zostały najważniejsze strony państwowe. Dziś o te ataki podejrzewa się głównie obywateli Rosji, a w szczególności organizację Russian Business Network. Wynika to z faktu, iż na rosyjskich serwisach internetowych podczas rozpoczęcia działań zbrojnych zaczęły się pojawiać narzędzia i ogólnodostępne instrukcje do przeprowadzania ataków wraz z listą celów.

Szokującą informacją dla świata była również wiadomość na temat ataku cybernetycznego z października 2010 roku, wskutek którego zainfekowane zostały irańskie systemy obsługujące niemal całą infrastrukturę państwa – od sieci elektrowni, przez rurociągi ropy naftowej, aż po systemy wojskowe. Przypuszcza się, że celem ataku było zniszczenie, uszkodzenie bądź zlikwidowanie reaktora jądrowego Iranu. Nie wyklucza się, że trojan, którego użyto – Stuxnet – został wprowadzony do irańskiego systemu przez pracownika jednej z rosyjskich firm podwykonawczych zaangażowanych w budowę elektrowni. Trojan ten skutecznie sparaliżował irański system komputerowy, który nadzorował pracę podziemnego ośrodka wzbogacania uranu w Natanz, opóźniając uruchomienie elektrowni jądrowej w Buszerze o dwa miesiące. O skali ataku świadczyć może fakt, że w Iranie zainfekowanych zostało blisko 30 tys. komputerów (D. Doroziński, 2001; M.F. Gawrycki, 2003, s. 50–65).

W Polsce zjawisko cyberterroryzmu zaczęto poważnie traktować również dopiero z początkiem XXI wieku. Obecnie nasz kraj znajduje się na piątym miejscu pod względem ataków internetowych pochodzących z urządzeń mobilnych (A. Bógdał-Brzezińska, M. Gawrycki, 2003, s. 63). Dane na ten temat opracowała amerykańska firma Akamai, która jest jedną z naj-

większych firm na świecie zajmujących się zarządzaniem ruchu sieciowego. Fakt, że Polska stoi tak wysoko w zestawieniu państw, w których najczęściej dochodzi do ataków pochodzących z sieci, wynika z kilku przyczyn. Jedną z najważniejszych jest to, że nasz kraj nie nadąża z rozwojem mechanizmów i procedur bezpieczeństwa w stosunku do tempa rozwoju technologii informacyjnych. Ponadto Polacy nie zdają sobie sprawy z zagrożeń, jakie mogą wynikać z coraz powszechniejszego informatyzowania wielu dziedzin życia[7]. Co więcej, do niedawna zagrożenia pochodzące z cyberprzestrzeni bagatelizowano. Dopiero na początku 2012 roku zauważono, że Polska również może być zagrożona cyberterroryzmem. Zaatakowane zostały wtedy strony rządowe, czego powodem był sprzeciw w sprawie podpisania porozumienia ACTA. Protesty związane z tymi wydarzeniami pokazały, że serwisy rządowe są niezwykle słabo zabezpieczone w Internecie. Ataki hakerów dobitnie udowodniły, że realne jest zagrożenie[8].

Daesh, czyli tak zwane Państwo Islamskie, czy też wcześniej Al-Kaida, w swej aktywności nigdy nie stroniły od używania najnowszych technologii teleinformatycznych. Wykorzystywane są one zarówno do promowania swoich poglądów wśród rozsianych na całym świecie zwolenników, jak i do szerzenia przekazów propagandowych, skierowanych do nowych, potencjalnych odbiorców. Tym samym Internet, dotychczas postrzegany jako narzędzie Zachodu w zakresie promocji własnego obrazu świata, zyskał nowy wymiar i stał się bronią przeciwników Zachodu (M. El Ghamari, 2016, s. 47–90).

Jednocześnie cały czas cyberprzestrzeń jest polem znaczącej aktywności służb specjalnych niemal wszystkich państw świata, zarówno w obrębie pozyskiwania danych o rywalach, jak i sojusznikach. Nie chodzi przy tym o samo pozyskiwanie danych, ale również ich odpowiednie pozycjonowanie, nie mówiąc o tworzeniu specjalnych przekazów w celu wprowadzenia w błąd przeciwnika i wywołania u niego zamierzonej reakcji. Jest to o tyle istotne, że wraz z pojawieniem się nowej fali mediów, opierających się o przekaz publikowany w sieci, można bardzo łatwo docierać do społeczeństw czy wybranych jednostek bez czasochłonnego lokowania własnych aktywów operacyjnych w klasycznych mediach.

[7] Zob. http://technologie.gazeta.pl/ internet/1,104530,9036923,Mobilny_Internet_na_swiecie___Polacy_na_ni echlubnym.html [data dostępu: 15.06.2012].

[8] Zob. http://next.gazeta.pl/internet/1,104530,90369,Mobilny_Internet_na_swieciePolacynaniechlubnym.html.

W ostatnich latach znaczną siłą stały się media społecznościowe, gdzie jakże trudno jest wielokrotnie uchwycić jednolitą strukturę decyzyjną oraz proces powstawania informacji.

Wystarczy przytoczyć przykład tak zwanych arabskich rewolucji z 2011 roku. Fala protestów, zainicjowana często na portalach społecznościowych zmieniła oblicze regionu MENA – Bliski Wschód i Afryka Północna. Jej niezaprzeczalnym elementem były komunikatory sieciowe i różnorakie media społecznościowe. To dzięki nim możliwe było organizowanie się w grupy przez demonstrujących, omijanie przez nich kordonów policji oraz sił bezpieczeństwa, a przede wszystkim pokazywanie światu własnego obrazu wydarzeń bez pośredników. Nie było to jednak działanie jednostronne, ale zostało przejęte przez wszystkie strony różnych konfliktów społecznych, politycznych itp.

W ten sposób bez zrozumienia nowego obiegu danych nie jest możliwe ustalenie wielu aspektów w zakresie taktycznej oceny wydarzeń, a tym bardziej prób wnioskowania na płaszczyźnie strategicznej. Lecz i ich czas nieubłaganie się kończy. Twitter w ciągu ostatnich sześciu miesięcy zawiesił 235 tys. kont za promowanie terroryzmu – podaje portal money.cnn.com. W sumie od połowy 2015 roku Twitter zawiesił już 360 tys. kont. Wiele z nich powiązanych jest z Państwem Islamskim (IS), które szczególnie aktywnie na Twitterze i innych portalach społecznościowych szerzy propagandę i przyciąga nowych rekrutów. Jak informuje amerykański portal, zarówno Facebook, jak i YouTube również w ostatnich miesiącach podjęły kroki, które doprowadziły do zawieszenia kont lub zablokowania treści udostępnionej przez zwolenników IS. Zwolennicy IS, w reakcji na blokady kont, posunęli się tak daleko, że zaczęli nawet grozić założycielom Twittera i Facebooka[9].

Na podstawie przeprowadzonych badań można stwierdzić, iż nowe techniki komunikacji i komputeryzacji nadają sieci trojakie cechy:

- zredukowanie czasu transmisji, które umożliwia rozproszonym organizacjom (grupom) porozumiewanie się i koordynowanie zadań,
- znaczne zmniejszenie kosztów komunikacji, które sprzyja rozproszeniu organizacji przez decentralizację,
- zwiększenie zakresu i kompleksowości informacji.

[9] Zob. http://niezalezna.pl/84940-twitter-na-wojnie-z-terroryzmem.

Takie innowacje, jak telekonferencje czy czaty internetowe, pozwalają uczestnikom na szeroką wymianę informacji bez względu na odległość. Posługiwanie się Internetem przyspiesza mobilizację członków grup terrorystycznych, umożliwia dialog między nimi i zwiększa elastyczność organizacji przez możliwość zmiany taktyki w razie potrzeby. Członkowie grup terrorystycznych mogą dzielić się na podgrupy, ustalać miejsca spotkania, przeprowadzać operacje terrorystyczne, po czym szybko przerywać swoje powiązania i się rozpraszać.

Zgodnie z raportami osób, które były w górskiej kwaterze Ibn Ladina w Afganistanie, ten koordynator i finansista terroryzmu dysponuje nowoczesnym komputerem i sprzętem telekomunikacyjnym, a nawet wykorzystuje telefonię satelitarną do koordynacji działań rozproszonych grup. Dysponuje też urządzeniami dającymi mu bezpieczeństwo, gdy korzysta z systemów komunikacji. Najczęściej dyktuje on polecenia asystentowi, który przekazuje je telefonicznie z różnych miejsc. Funkcjonariusze Ibn Ladina używają dysków CD-ROM do zapisu i rozpowszechniania informacji dotyczących rekrutacji członków, produkcji bomb, ciężkiej broni i operacji terrorystycznych. Amerykańskie agencje wywiadowcze otrzymały ostatnio kopie dysków komputerowych zawierających podręczniki szkoleniowe używane przez Ibn Ladina podczas szkolenia rekrutów (S.M. Lawson, 2002, s. 16–37).

Egipscy eksperci komputerowi, którzy walczyli w Afganistanie, opracowali dla Ibn Ladina sieć komunikacyjną na bazie internetowej i e-mailowej. W latach 90. w operacjach antyterrorystycznych przeciw bazom algierskiej GIA skonfiskowano komputery i dyskietki z instrukcjami dotyczącymi konstrukcji bomb (Organised Crime Situation Report 2004, Focus on the Threat of Cybercrime, 2003, s. 125).

Bojowa grupa islamska Hamas również posługuje się Internetem w przekazywaniu operacyjnych informacji. W Stanach Zjednoczonych aktywiści Hamasu wykorzystują kanały dyskusyjne, czyli chatrooms, podczas planowania i realizacji operacji. Agenci Hamasu posługują się także pocztą elektroniczną w koordynowaniu akcji w Gazie, na Zachodnim Brzegu Jordanu i w Libanie. Zauważyli oni, że informacje mogą być przekazywane względnie bezpiecznie przez Internet, gdyż wywiad kontrterrorystyczny nie jest w stanie ściśle monitorować całego ich przepływu i treści. Ponadto sieci terrorystyczne mogą chronić przepływ informacji dostępnymi technikami, np. programami kodującymi. Nowe programy

kodujące są tak wyrafinowane, że kody zabezpieczające pocztę elektroniczną niezwykle trudno jest złamać. Prawdopodobnie izraelskim siłom nie udało się złamać kodów używanych przez Hamas do przesyłania przez Internet instrukcji terrorystycznych ataków. Terroryści mogą posługiwać się też steganografią, tj. metodą ukrywania tajnych danych w innych informacjach, w tym w plikach graficznych. Mogą także kodować transmisje realizowane przez telefony komórkowe, kraść numery takich telefonów i przeprogramowywać je albo używać opłaconych z góry kart telefonicznych sprzedawanych anonimowo. Te ostatnie techniki komunikowania się umożliwiają terrorystom operowanie z prawie każdego zakątka świata przy dostępie do niezbędnej infrastruktury IT. Analitycy twierdzą, że terroryści mający możność kodowania informacji są niezależni od sponsorów oraz pomocy państwa i mogą zapewnić sobie większy stopień bezpieczeństwa. Inni wskazują, że grupy terrorystyczne mogą zdobywać pieniądze, wykorzystując sieć. Z Pakistanu jest znany przypadek podjęcia tak dużych sum z kont wahhabitów z Arabii Saudyjskiej, że terroryści planowali utworzenie na ich bazie własnego banku. Dzięki Internetowi informacje o zamachach bombowych mogą małym kosztem przedostać się bezpośrednio ze stron internetowych do prasy – o ile życzą sobie tego terroryści (zob. E. Aronson, A. Pratkanis, 2004, s. 4). Terroryści mający bezpośrednią kontrolę treści informacyjnych mogą dokonywać manipulacji obrazami, stosować specjalne efekty i oszustwa (por. R. Borkowski, 2006, s. 16).

Internet jest korzystny także ze względu na możliwość mobilizacji czasowej cyberterrorystów (*parttime cyberterrorists*), tj. osób niezwiązanych bezpośrednio i na stałe z ugrupowaniami terrorystycznymi, ale wspierających ich działania. Na przykład zarówno rząd Palestyny, jak i rząd Izraela zachęcały prywatne osoby do przesyłania danych z komputerów w związku z konfliktem dotyczącym świątyni Al-Aksa i późniejszą intifadą.

Cyberterroryści mogą wykorzystywać IT do ataków elektronicznych, które wpływają negatywnie na wolę walki przeciwników. Destrukcyjne ataki obejmują także dławienie systemów komputerowych (*choking*) za pomocą takich metod i narzędzi, jak e-bomby, masowe rozsyłanie wiadomości elektronicznych (*fax-spamming*) i włamania hakerów w celu zniekształcenia stron internetowych. Liczba tych destrukcyjnych ataków ma tendencję wzrostową (zob. J. Adamski, 2002, s. 12–21).

NARZĘDZIA DO WALKI Z CYBERTERRORYZMEM?

Ciekawym przypadkiem jest modułowy system informatyczny CSI. Jego autorzy skupili swoją uwagę na dualnej strukturze wykrywania i analizy potencjalnych zagrożeń, obejmujących zarówno te fizyczne, jak i wirtualne. Narzędzie ma charakteryzować się uniwersalnością i można je stosować, zgodnie z założeniami twórców, do całego spektrum współczesnych wyzwań – od terroryzmu po lokalne zamieszki bądź działania coraz groźniejszych hakerów. Oprogramowanie tego rodzaju daje możliwość monitorowania różnych źródeł generujących istotne informacje, tj. komentarzy zamieszczanych w sieci, forów internetowych, portali informacyjnych, aż do mediów społecznościowych włącznie. Według producenta analityk jest w stanie dzięki temu sprawnie i szybko dokonywać określenia chociażby najbardziej zagrożonych miejsc – począwszy od potencjalnych celów dla terrorystów po możliwe działania osób dążących do wszczęcia zamieszek lub innego rodzaju prób naruszenia porządku publicznego. Oczywiście, w myśl zasady, że wszelkie działania w sieci pozostawiają ślady, które zastosowanie narzędzi pokroju Comarch CSI pozwala odpowiednio odnajdywać i układać w większą całość.

W dobie ciągłego zagrożenia terrorystycznego ewidentnie nowego znaczenia nabiera skuteczna analiza działań różnych organizacji terrorystycznych, chociażby tzw. Państwa Islamskiego w sieci. Jak już niejednokrotnie pokazały dokładne, szczegółowe dochodzenia, rozpoczęte po konkretnych zamachach terrorystycznych, kluczowe w tworzeniu systemu zapobiegania jest wyszukiwanie i śledzenie wszelkich informacji pozwalających na wyznaczenie potencjalnych kierunków działań terrorystów. Niezwykle istotna jest możliwość monitorowania komunikacji związanej z ugrupowaniami terrorystycznymi, jak również wykorzystania zdobytych informacji do lokalizowania miejsc działań ekstremistów.

Do kolejnych pomocnych narzędzi przy analizie zagrożeń o charakterze terrorystycznym należą:

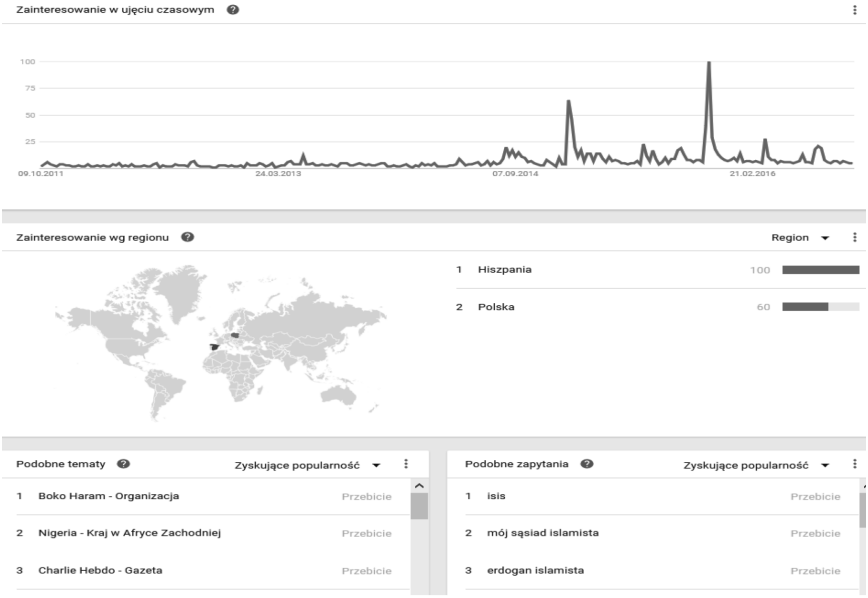
- platforma Quintly – narzędzie badające treści i jej przepływy w Internecie. Badania wykazują, że najbardziej popularne, atrakcyjne są grupy fundamentalistyczne, zmierzające ku idei nacjonalizmu. Przykładem jest: Pegida (wskaźnik polubień – algorytm)[10],

[10] Zob. https://www.quintly.com/.

- platforma Google Trends (wskaźnikiem jest kraj i 24-godz. popoularność wiadomości w danym kraju),
- platforma IceRocket,
- platforma Keyhole.

W kontekście portali społecznościowych niezwykle ważny jest tak zwany feedback, czyli informacja zwrotna. Reakcja zwrotna. Jej skutek można zaobserwować poprzez stosowanie przez użytkowników tak zwanego przycisku polubień. Co ciekawe, w przypadku Pegidy przycisk „lubię to" zastosowało około 300 tys. osób, zaś grupy Emisco jedynie 90 razy. Podobny wyraz mają komentarze i udostępnianie. Pegida osiągnęła poziom 80 tys. komentarzy, a jej artykuły zostały udostępnione ponad 70 tys. razy, zaś Emisco uzyskało jedynie 8 komentarzy i 33 udostępnienia. Platforma analityczna Quintly udowadnia za pomocą wskaźników zależności pomiędzy badanymi stronami użytkowników.

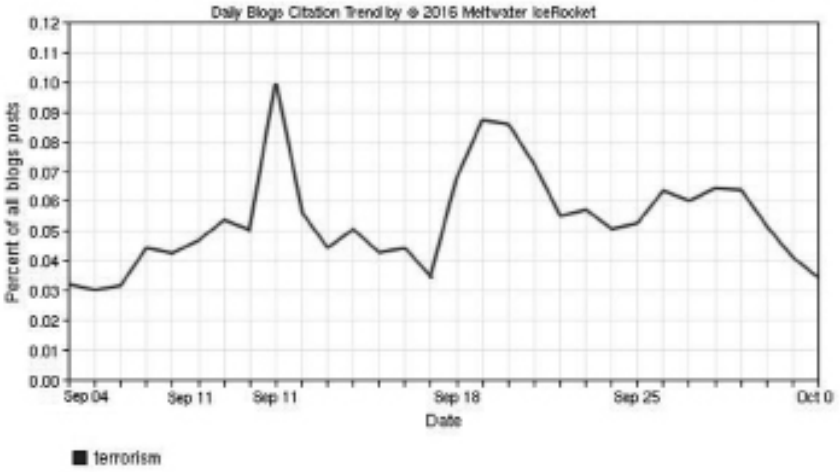
Schemat 1.
Zainteresowanie hasłem „islamista" – w ujęciu czasowym (ostatnie 5 lat) oraz regionalnym (cały świat)



Źródło: Opracowanie własne na podstawie https://www.google.pl/trends/explore?q=islamista [dostęp 04.10.2016]

Platforma Google Trends analizuje współzależności pomiędzy poszczególnymi hasłami i wykazuje ich składowe. Na przykładzie ataku we Francji można wskazać pewne zależności pojawiające się w hasłach, wiadomościach, nagłówkach, komunikatorach i tytułach artykułów, blogach itd. Korzystając z możliwości Google Trends, można porównać zależność pomiędzy hasłami „muzułmanin" czy „islamista" a odsetkami społeczeństw imigracyjnych w społecznościach rdzennych, które wyszukiwały to hasło. Im wyższy odsetek imigrantów w regionie, tym więcej wyszukiwania i jednostkowego pojawiania się samego hasła (schematy 1, 2).

Schemat 2.
Popularność hasła „Daesh" w wybranym czasie



Źródło: http://www.icerocket.com/trend?query1=ISIS&days=30 [dostęp: 03.10.2016]

W celu monitorowania mediów społecznościowych wypracowano gotowe narzędzia, z których można skorzystać, aby dokonać analizy i syntezy danych:

- Buzzsumo – umożliwi wgląd w treści szybko zyskujące popularność oraz użytkowników, którzy chętnie je między sobą współdzielą (szczególnie przydatne przy analizie danych z: Twittera, Facebooka, LinkedIn, Google+ oraz Pinteresta).
- Social Mention – to wyszukiwarka danych dotyczących mediów społecznościowych. Aplikacja ma ponad 100 funkcji wyszukiwania dla takich portali, jak Twitter, Facebook, YouTube, Digg oraz Google.

- Mention – dostępna w aż 42 językach, umożliwia analizowanie danych z mediów społecznościowych, portali informacyjnych, blogów oraz stron firmowych.
- HowSociable – umożliwia szybkie oszacowanie widoczności i rozpoznawalności danego hasła w mediach społecznościowych.
- Addict-o-matic – gromadzi dane poprzez skanowanie plików RSS witryn informacyjnych oraz silników wyszukiwania, m.in.: Google, Yahoo, Technorati, Ask, YouTube, Truveo, Flickr, Blinkx, IceRocket, Digg, Topix, Newsvine oraz Tweetscan.
- Topsy – umożliwia wyszukiwanie działające w czasie rzeczywistym dedykowanym mediom społecznościowym. Indeksuje oraz ocenia wyniki wyszukiwania w oparciu o najpopularniejsze konwersacje prowadzone przez miliony użytkowników na dany temat, przykładowo – o danej stronie, domenie czy zagadnieniu.
- SumAll – umożliwia dostęp do wszystkich danych portali społecznościowych: Facebook, Instagram, Twitter, LinkedIn i Google Analytics z poziomu jednej aplikacji. Pozwala na śledzenie statystyk ponad 30 kont.
- Sprout Social – pozwala na monitorowanie oraz zarządzanie działaniami prowadzonymi w mediach społecznościowych.
- WhosTalkin – jest narzędziem do przeszukiwania zawartości mediów społecznościowych zorientowanym na wyszukiwanie konwersacji prowadzonych na określony temat. Dane zbierane są z 60 najpopularniejszych źródeł.
- Pluggio – to aplikacja do zarządzania kontami prowadzonymi na platformach Twitter oraz Facebook. Pluggio automatycznie śledzi oraz generuje wykresy dla nawet kilku kont, a więc możliwe jest określenie wydajności prowadzonej kampanii oraz oszacowanie wzrostu bazy klientów. Opcjonalna integracja z witryną Bit.ly daje użytkownikowi szansę analizy liczby odwiedzin współdzielonych linków – pozwala to na dokładną ocenę popularności publikowanych postów.
- SharedCount – usługa sprawdzająca liczbę udostępnień danego adresu URL w głównych mediach społecznościowych, takich jak: Facebook, Twitter, Pinterest, LinkedIn, Google+ oraz StumbleUpon.
- Social Searcher – ułatwia przeszukiwanie oraz analizę kanałów społecznościowych w czasie rzeczywistym. Gromadzi informacje bez konieczności logowania się na portale, takie jak: Twitter, Google+ bądź Facebook. Zapisuje wyniki wyszukiwania oraz ustaw powiadomienia dla konta.

- Edgerank Checker – aplikacja analizująca oraz oceniająca jakość prowadzonej strony na platformie Facebook. Sprawdzi, kiedy twoi fani są online, aby lepiej oszacować najlepszy moment publikacji materiałów promocyjnych. Sprawdza wydajność dla określonych dat, aby sprawdzić, kiedy użytkownicy byli najbardziej zainteresowani twoją stroną.
- Aplikacja Followerwonk – pozwala na pozyskanie zaawansowanych danych statystycznych dotyczących portalu Twitter.
- NutshellMail – zbiera informacje o najnowszych wydarzeniach na kontach założonych na różnych portalach społecznościowych, a następnie przesyła podsumowanie mailem.

PODSUMOWANIE

Zwalczanie terroryzmu informatycznego stało się nie tylko ważnym zagadnieniem natury politycznej, ale również, a może przede wszystkim, problemem natury ekonomicznej. Cyberterroryści mogą również dostosować swoje działania tak, aby zmaksymalizować pozytywny dla siebie wynik. Ponadto cyberterroryzm nie wymaga treningu fizycznego ani dużego zabezpieczenia logistycznego. Nie wymaga poza tym podróżowania. Ataki w cyberprzestrzeni nie stwarzają ryzyka poniesienia śmierci lub obrażeń fizycznych, ograniczają więc konieczność narażania życia – zamachy w sieci nie wymagają bowiem ataków samobójczych[11]. Aby przeprowadzić taki atak, nie potrzeba posiadać praktycznie żadnych umiejętności – można wynająć crackerów, którzy łamiąc zabezpieczenia (często nie zdając sobie sprawy ze skutków swojego działania), za pieniądze przeprowadzą atak terrorystyczny.

Dotychczasowe przykłady przestępstw informatycznych pokazują, jak wielka liczba ludzi może być dotknięta skutkami takiego działania; wynika to z globalnego charakteru informatyzacji. Tym samym jeden z zasadniczych celów terrorystów – medialność ataku – jest przeogromna[12].

Terroryści zdają sobie również sprawę, iż walka z cyberterroryzmem wymaga o wiele większej koordynacji działań niż w przypadku klasyczne-

[11] National Research Council, Computer at Risk, Washington, DC, 1991, s. 36.

[12] Devost M.G., Brian K.H., Neal A.P., *Information terrorism: Can you trust your toaster?*, [w:] *San Tzu and Information Warfare*, Washington, DC, 1997, s. 51.

go ataku. Dysponując różnymi możliwościami zastosowania sankcji – nie wiadomo, w jaki sposób odpowiedzieć na taki atak. W konsekwencji można stwierdzić, że cyberterrorystą może zostać każdy, dlatego kwestia cyberterroryzmu może stanowić kluczowy problem bezpieczeństwa międzynarodowego w XXI wieku. Ryzyko cyberterroryzmu będzie wzrastać w społeczeństwie wraz ze wzrostem znaczenia Internetu w naszym życiu. Cyberwojnę już dziś można prowadzić niezależnie od konfliktu na lądzie i morzu, w dodatku mniejszym nakładem kosztów. Systemy informacji w podstawowych dziedzinach gospodarki – bankowości, finansach, telekomunikacji, handlu – już dziś stały się nadrzędne, dlatego dostęp do nich lub ich blokada mogłyby skutecznie sparaliżować działanie instytucji i państwa. Wiele racji miał zatem sekretarz generalny NATO Jaap de Hoop Scheffer, mówiąc, że „cyberataki nie wymagają użycia ani jednego żołnierza czy naruszenia granic – mogą jednak sparaliżować działanie państwa".

Strach informatyczny jest zjawiskiem coraz powszechniejszym, jednak jest on wyolbrzymiony. Pomimo faktu, że pozaprawne ataki informatyczne na newralgiczne składniki narodowej infrastruktury informatycznej stają się coraz powszechniejsze, to nie są one, jak dotychczas, przeprowadzane przez terrorystów. Poziom ich niszczycielskiej siły nie jest ponadto na tyle znaczny, by można go zakwalifikować jako terroryzm informatyczny. Jakkolwiek strach przed tym zagrożeniem jest przesadzony, to nie może być lekceważony czy ignorowany.

Bibliografia

Adamski J. (2007). *Nowe technologie w służbie terrorystów*. Warszawa.

Adamski A. (2002). *Cyberterroryzm*, [w:] Materiały z konferencji na temat terroryzmu, 11.04.2002 r. Wydział Prawa UMK Toruń.

Adkins B. (2001). *The spectrum of cyber conflikt from hacking to information warfare: What is law enforcament's role?* Maxwell AFB, Alabama.

Aronson E., Pratkanis A. (2004). *Wiek propagandy*. Warszawa.

Barnas R. (2001). *Terroryzm. Od Asasynów do Osamy bin Laden*. Wrocław.

Białek T. (2005). *Terroryzm – manipulacja strachem*. Warszawa.

Borkowski R. (2006). *Terroryzm ponowoczesny*. Toruń.

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

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

Denning D.E. (2001). *Activism, hacktivism and cyberterrorism: The Internet as a tool for influencing foreign policy*, [w:] J. Arquilla, D. Ronfeldt, Networks and Netwars, Santa Monica.

Doroziński D. (2001). *Hakerzy. Technoanarchiści cyberprzestrzeni*. Helion.

El Ghamari M. (2016). *Cool Jihad*. Wydawnictwo Difin.

Gawrycki M.F. (2003). *Cyberterroryzm*. Fundacja Studiów Międzynarodowych. Warszawa.

Kerr K. (2003). *Putting cyberterrorism into contex*. AusCERT.

Kosta R. (2007). *Terroryzm jako zagrożenie dla bezpieczeństwa cywilizacji zachodniej w XXI wieku*. Toruń.

Lawson S.M. (2002). *Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure*. SANS Institute.

Monge P., Janet F., *Communication technology for global network organizations*, [w:] Shaping Organizational Form: Communication, Connection and Community, red. G. Desanctis, J. Fulk, Thousand Oaks, Calif., 1999.

Pollitt M., Cyberterrorism: Fact or Fancy? Proceedings of 20-th National Information Systems Security Conference, październik 1997.

Münkler H., *Terrorismusheute. Die Asymmetrisierung des Krieges*, „Internationale Politik", nr 2, 2004.

Organised Crime Situation Report 2004, *Focus on the Threat of Cybercrime*, Council of Europe, Strasburg, 23.12.2003.

Reeve S. (1999). *The New Jackals: Ramzi Yousef, Osama Ben Laden and the Future of Terrorism*. Mass, Boston.

Serwiak S. (2005). *Cyberprzestrzeń jako źródło zagrożenia terroryzmem*, [w:] E. Pływaczewski, *Przestępczość zorganizowana*. Kraków.

Staten C. (24.02.1998). *Subcommitte of Technology*. Terrorism and Government Information, U.S. Senate Judiciary Committee.

Stern J. (listopad/grudzień 2000). *Pakistan's Jihad Culture*.„Foreign Affairs".

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

Whine M., *Islamist organizations on the Internet*, „Terrorism and Political Violence", t. 11, nr 1, 1999.

Zanini M., Edwards S.J.A. *(2001). The networking of terror in the information age,* [w]:
J. Arquilla, D. Ronfeldt, Networks and Netwars. Santa Monica.

Źródła internetowe

Garrison J., Grand M., *Cyberterrorism: An evolving concept*, NIPC Highlights, http://www.nipc.gov/publications/highlights/2001/ highlight-01-06.html [data dostępu: 15.06.2012].

http://niezalezna.pl/84940-twitter-na-wojnie-z-terroryzmem.

http://technologie.gazeta.pl/ internet/1,104530,9036923,Mobilny_Internet_na_swiecie___Polacy_na_ni echlubnym.html [data dostępu: 15.06.2012].

https://www.quintly.com/.