Arkadiusz Chorobiński

Walka informacyjna, jako fundamentalny składnik działalności terrorystycznej w przyszłości

Abstrakt: W swoim artykule *„Punkt zapalny: Elektroniczna wojna w Internecie”* Andrzej Pająk zwraca uwagę, że walka informacyjna stosowana przez organizacje terrorystyczne, między innymi poprzez ataki na rządowe strony internetowe wielu państw świata, to nie tylko problem teoretyczny, ale jak najbardziej realny. FBI ma zamiar umieścić zagrożenie atakiem elektronicznym na trzecim miejscu (po ataku nuklearnym i broni masowego rażenia) listy największych zagrożeń bezpieczeństwa Stanów Zjednoczonych.[1] Dlatego też autor pracy, jako żołnierz zawodowy w Centralnej Grupie Działań Psychologicznych w Bydgoszczy, postanowił przybliżyć ten niewątpliwie poważny problem współczesnego świata.

Słowa kluczowe: terroryzm, cyberterroryzm, propaganda, Al Kaida, Hamas.

Wprowadzenie

Terroryzm jest jednym z największych problemów współczesnego świata. Aby móc skutecznie zwalczać to zagrożenie, niezbędne jest poznanie celów działalności terrorystycznej oraz środków stosowanych do ich osiągnięcia. Celem niniejszej pracy jest przedstawienie nowych strategii i taktyki terrorystów. Analiza tego zagadnienia ma na celu zrozumienie powagi zjawiska terroryzmu, co z kolei jest warunkiem niezbędnym do skutecznego radzenia sobie z tym zagrożeniem. Liczne organizacje terrorystyczne działają w wielu państwach, na różnych kontynentach, nieustannie werbując obywateli różnych narodowości w swoje szeregi, a w ciągu ostatniej dekady zauważalne jest dążenie nowego pokolenia terrorystów do prowadzenia działań odmiennego typu niż konwencjonalne. Wiążą się one z zagrożeniem wykorzystania środków chemicznych, biologicznych lub radiologicznych oraz elementów walki informacyjnej, mającej na celu wykorzystanie informacji, jako broni, która skuteczne osłabi wolę walki przeciwnika. Cele terrorystów, jakie sobie wyznaczą, są relatywnie łatwe do zrealizowania zważywszy na fakt uzależnienia niemalże każdego aspektu naszego życia od sieci informatycznych i telekomunikacyjnych. Ponadto terroryści zwrócili uwagę na siłę

[1] A. Pająk, *Punkt zapalny: Elektroniczna wojna w Internecie*, [Online], dostępne: http://chip.pl/artykuly/trendy/2009/11/punkt-zapalny-elektroniczna-wojna-w-internecie, 13.11.2009.

i skuteczność prowadzenia kampanii propagandowych i operacji psychologicznych poprzez wykorzystanie najnowszych zdobyczy techniki.

Zalety walki informacyjnej

Postęp naukowo-techniczny w dziedzinie elektroniki i informatyki spowodował zmianę charakteru walki informacyjnej poprzez przeniesienie fizycznych przedsięwzięć z nią związanych do sfery cybernetycznej. W nowoczesnej walce informacyjnej głównymi środkami rażenia stały się narzędzia informatyczne i urządzenia, za pomocą których można oddziaływać na wojskowe i cywilne systemy komputerowe przeciwnika w celu zakłócenia lub całkowitego uniemożliwienia ich użytkowania.

W związku z powyższym, z punktu widzenia terrorystów, wykorzystanie w ich działalności elementów walki informacyjnej ma wiele zalet. Umożliwia im rozszerzenie swoich działań o zasięg ogólnoświatowy. Dzięki wykorzystaniu globalnej sieci połączeń internetowych organizacje terrorystyczne koordynują swoje akcje z różnych części świata. Dodatkowo w porównaniu z bardzo drogimi technikami zabezpieczenia sieci, koszty przygotowania i przeprowadzenia ataku informatycznego są niewielkie. W najprostszych przypadkach wymagany jest jedynie komputer z dostępem do Internetu oraz zdolny haker. W związku z tym, iż Internet jest źródłem ogromu informacji stał się on dla terrorystów jednym z głównych narzędzi służących pozyskaniu niezbędnych danych o obiektach, które mają zamiar zaatakować. Kolejną zaletą walki informacyjnej jest znikome ryzyko dla zamachowców z uwagi na możliwość dokonania ataków z dużych odległości. Akcję można przeprowadzić z ogólnie dostępnego terminala znajdującego się np. w kawiarence internetowej, a szanse schwytania sprawcy na gorącym uczynku są nikłe. Natomiast zlokalizowanie miejsca, z którego dokonano ataku oraz ustalenie personaliów atakujących jest żmudne i długotrwałe, co pozwala na wystarczające zakonspirowanie się sprawcy. Nieocenionym elementem walki informacyjnej jest również propaganda, której zaletą jest szeroki wachlarz obiektów oddziaływania, na który składają się: społeczność państw islamskich oraz wojska własne, ale także wojska przeciwnika i światowa opinia publiczna.

Cyberterroryzm

Dotychczasowa liczba ataków cybernetycznych jest stosunkowo niewielka w porównaniu do konwencjonalnych aktów terroru. Obecnie ma to związek z dominacją w organizacjach terrorystycznych osób starszych pełniących funkcje kierownicze, które wychowane zostały z dala od techniki informatycznej. Ponadto wielu terrorystów uważa ataki

cybernetyczne za nieefektywne, ponieważ nie powodują one tak wielkich skutków propagandowych jak spektakularne zamachy metodą konwencjonalną, np. zamach na World Trade Center (WTC) w 2001 r. Organizacjom terrorystycznym brakuje w dalszym ciągu specjalistów, którzy mogliby się profesjonalnie zająć cyberterroryzmem. Wymaga on bowiem szerokiej wiedzy specjalistycznej i jest zarezerwowany dla osób wykształconych. Niemniej jednak podejrzewa się organizacje o szkolenie coraz większej ilości swoich członków z zakresu telekomunikacji i informatyki, co świadczy o tym, że jest to dziedzina walki, której ranga wzrasta w oczach terrorystów.

Jak wspomniane zostało na wstępie mojej pracy, terroryści stawiają sobie za cel zrujnowanie życia codziennego innowierców. Najbardziej prawdopodobne są więc ataki przeciw systemom informatycznym sfery cywilnej z uwagi na niższe poziomy zabezpieczeń w porównaniu do wojskowych. Ponadto systemy cywilne nie są fizycznie odseparowane od innych sieci komercyjnych i publicznych, co w znaczącym stopniu ułatwia do nich dostęp. Można przypuszczać, że szczególnie zagrożone są systemy wspomagające nadzór ruchu w sieciach transportowych, systemy używane w instytucjach państwowych, sektory bankowości i służb ratowniczych oraz produkcji dóbr strategicznych takich jak ropa naftowa, gaz czy energia elektryczna. Systemy, które wymieniłem zarządzają kluczową infrastrukturą wysokorozwiniętego państwa i poważne zakłócenie ich pracy mogłoby mieć nieobliczalne następstwa ekonomiczne oraz społeczne, chociażby w postaci wybuchu paniki. Terroryści mając tego świadomość dążą do wykorzystania charakterystycznych wad, które czynią każdy system informatyczny podatnym na ataki cybernetyczne. Władze państwowe i instytucje prywatne z kolei dokładają wszelkich starań, aby utrzymać wysoki poziom ochrony ważnych systemów poprzez wysokiej klasy sprzęt oraz regularne uaktualnianie oprogramowania. Operacje takiego typu niestety są bardzo kosztowne, dlatego też wiele instytucji nie stosuje najnowszych wersji używanych produktów zabezpieczających.

Na działalność cyberterrorystyczną składa się wiele technik. Część z nich może być stosowania 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. Takie zdarzenie chociażby miało miejsce w listopadzie 2000 r. po wybuchu powstania palestyńskiego, gdy witrynę IDF okupowało tygodniowo blisko 130 tys. osób, podczas gdy przed wybuchem zamieszek stronę odwiedzało ok. 7 tys. Internautów. Skuteczność kolejnej

techniki zwanej *flooding*[2] przedstawia atak separatystów tamilskich na serwery ambasad Sri Lanki w 1998 r. Polegał on na wysyłaniu ok. 1 tys. e-maili przez okres dwóch tygodni z oświadczeniem kwestii roszczeń niepodległościowych, zakończonych informacją mówiącą o celowości działań.[3] 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 na ok. 30 minut przed ich dokonaniem. Często dołączane jest również specjalistyczne oprogramowanie opracowane przez islamistyczne grupy hakerskie np. Al-Jihad czy Dorach War Engine. 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 ich prowadzenia i stale udoskonalają wykorzystywane oprogramowanie. O wysokich ambicjach ich działań świadczy planowany, zmasowany atak przeciw serwerom wybranych banków amerykańskich w grudniu 2006 r. pod nazwą „The Electronic Guantanamo Raid". Ostatecznie został on jednak odwołany najprawdopodobniej z powodu dekonspiracji. Kolejne zagrożenie wiąże się 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 r. 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 posiadają już specjalistów zdolnych do tworzenia szkodliwego oprogramowania. Agencja Bezpieczeństwa Narodowego Stanów Zjednoczonych (NSA) wskazuje, że tylko do końca 2001 r. ok. 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

[2] Termin stosowany w polskojęzycznej literaturze przedmiotu.

[3] Oryginalny tekst brzmiał „We are the Internet Black Tigers and we're doing his to disrupt your communications" ("Jesteśmy Internetowymi Czarnymi Tygrysami i robimy to w celu zdezorganizowania waszej łączności").

zatrudniona w wielu amerykańskich i zachodnich firmach oraz ośrodkach naukowo-badawczych. Ich wykorzystanie przez terrorystów mogłoby mieć katastrofalne skutki.

Propaganda i operacje psychologiczne

Propaganda jest równie stara jak sama cywilizacja. Już wczesne zapisy hieroglificzne w kulturze egipskiej i mezoamerykańskiej składały się z symboli i obrazów przedstawiających historię w sposób korzystny dla klasy panującej. Teksty i pomniki Majów często manipulowały datami historycznymi, długością życia władców, cyklami astronomicznymi i rzeczywistymi wydarzeniami, aby ukazać aktualnie panującego władcę w korzystnym świetle. Zważywszy, że odczytywać i sporządzać hieroglify umieli tylko przywódcy i ich kapłani, perswazja miała charakter jednokierunkowy, skierowany od przywódcy do mas. Chociaż termin propaganda po raz pierwszy użyto w sposób udokumentowany w 1622 r., do powszechnego obiegu wszedł dopiero na początku XX w., kiedy zaczęto nim określać techniki perswazyjne wykorzystywane w okresie I wojny światowej, a później przez reżimy totalitarne.[4] Przez propagandę rozumiano pierwotnie rozpowszechnianie stronniczych idei i poglądów, nierzadko przy użyciu kłamstwa i podstępu. Po poddaniu tego zjawiska głębszej analizie przez uczonych nabrało ono nowych cech. Od tamtej pory słowo propaganda objęło także sugestię i wywieranie wpływu przez manipulację symbolami i przy wykorzystaniu mechanizmów psychologicznych jednostki. Propaganda obejmuje zręczne posługiwanie się obrazami, sloganami i symbolami odwołujące się do naszych uprzedzeń i emocji. Jest komunikowaniem pewnego punktu widzenia, mającym na celu skłonienie odbiorcy do „dobrowolnego" przyjęcia tego punktu widzenia za swój.

Kierownictwa ugrupowań terrorystycznych przywiązują dużą wagę do prowadzenia kampanii propagandowych i operacji psychologicznych, obecnie głównie za pośrednictwem Internetu i popularnych sieci medialnych. Upowszechnienie Internetu i globalny zasięg programów informacyjnych umożliwiają dotarcie do szerokich rzesz odbiorców na całym świecie. Stwarza to możliwość prowadzenia działań mających na celu rozpowszechnienie fałszywych, lub w określony sposób spreparowanych, informacji i promowanie własnych ideologii na skalę globalną. Usługi oferowane przez Internet doskonale nadają się do realizacji wspomnianych celów i dlatego organizacje terrorystyczne wykorzystują je w coraz większym stopniu. Ponadto realizują swoje cele również przy użyciu tradycyjnego sposobu,

[4] E. Aronson, A. Pratkanis: *Wiek propagandy*, Warszawa 2004, s. 17.

jakim jest komunikacja bezpośrednia. Motywy przewodnie propagandy terrorystów to gloryfikacja wysiłku własnego, deprecjonowanie przeciwnika, dyskredytacja sił przeciwnika, budowanie wśród islamistów przeświadczenia o tym, że ich państwo, zwłaszcza obecnie Islamska Republika Afganistanu oraz Irak, są miejscem wojny globalnej, chrześcijaństwa z islamem, zepsutego zachodu ze światem muzułmańskim, grożeniu państwo zamachami terrorystycznymi, których armie są zaangażowane w konflikty na ziemiach muzułmańskich oraz nakłanianie rządów do wycofania swoich wojsk z Bliskiego Wschodu.[5] Działania te prowadzą miedzy innymi takie organizacje, jak: Al Kaida, terrorystyczne ugrupowania palestyńskie, separatyści kaszmirscy i tamilscy czy afgańscy Talibowie. Al Kaida wykorzystuje w działalności propagandowej przede wszystkim strony internetowe oraz nagrania audio i wideo, publikowane w arabskich telewizjach satelitarnych Al Jazzeera i Al Arabiya. Działalność w Internecie prowadzona jest za pośrednictwem wielu stron internetowych umiejscowionych na serwerach z całego świata. Przykładowymi stronami intensywnie wykorzystywanymi przez Al Kaidę i Talibów są Al Neda, Islamie Studies and Research (ISR) oraz Jihad Online. Natomiast w okresie poprzedzającym wkroczenie wojsk koalicji do Republiki Afganistanu w ramach operacji „Enduring Freedom" („Umacnianie Wolności") oraz w trakcie jej trwania, w której miałem okazję osobiście uczestniczyć, zauważono wzmożone korzystanie z serwerów pakistańskich jehad oraz alemarh.[6] Organizacje terrorystyczne koncentrowały się wówczas na umieszczaniu, na wspomnianych stronach, informacji mających na celu stworzenie u odbiorców wrażenia istnienia potężnego proislamskiego ruchu, walczącego przeciw zachodniej ekspansji w państwach muzułmańskich. Dlatego ich twórcy oprócz bieżących informacji o Al Kaidzie i poglądów Osamy bin Ladena, przedstawiali rzekome szczególne osiągnięcia innych radykalnych ruchów islamskich oraz wyrazy poparcia dla reżimu Talibów w Afganistanie. Gloryfikowali także zamachy samobójcze ich członków, jako akty poświęcenia godne naśladowania. Działalność propagandowa Al Kaidy w Internecie stale się zwiększa. Na początku roku 2004 organizacja rozpoczęła wydawanie magazynu internetowego pt. „Obóz Treningowy Al Battara", mającego na celu przygotowanie pod względem mentalnym i ideologicznym

[5] 25.09.2009 Talibowie opublikowali nagranie wideo „Wezwanie do prawdy" na tureckojęzycznej internetowej stronie dżihadystów., w którym grożą Niemcom zemstą za udział w misji w Afganistanie. Zamaskowany mężczyzna posługujący się imieniem Adżub ostrzegał po niemiecku, że Talibowie chcą, by Niemcy „zakosztowali cierpienia, jakie każdego dnia znosić musi lud w Afganistanie". „Poczucie bezpieczeństwa to iluzja. Jest tylko kwestią czasu, kiedy dżihad rozerwie niemieckie mury" - mówił terrorysta.

[6] Pełne nazwy serwerów to: www.jehad.net oraz www.alemarh.com.

przyszłych bojowników „Świętej Wojny”.[7] Idąc w tym kierunku, rok później, różne odłamy Al Kaidy i współpracujące z nimi organizacje w Iraku i Arabii Saudyjskiej również rozpoczęły wydawać magazyny internetowe. Koncentrowały się one na sytuacji lokalnej i regionalnej. Są one redagowane w sposób profesjonalny, zawierają dodatkowo kolorowe zdjęcia i ilustracje sformatowane zgodnie z wymogami wydawniczymi. Również Czeczeni publikują, za pośrednictwem Internetu, wiele oświadczeń i informacji przedstawiających ich komentarze na temat wydarzeń w republice i związanych z działalnością separatystów. Najbardziej spektakularną akcją była kampania dezinformacyjna na serwisie kavkaz.org związana z zatonięciem rosyjskiego strategicznego okrętu podwodnego „Kursk”. W miesiącach sierpniu i wrześniu 2000 r. Czeczeni sugerowali, że jednym z członków załogi był współpracujący z nimi, dagestański muzułmanin, który przemycił ładunek wybuchowy na pokład okrętu podwodnego, aby go zatopić. Al Kaida i organizacje palestyńskie prowadzą również operacje mające na celu dezinformowanie społeczeństw swoich przeciwników. Przykładem tego typu były informacje z lata 2002 r. zamieszczone na wspierającym bin Ladena serwerze Al Neda, sugerujące, że wielkie pożary lasów w Stanach Zjednoczonych były wynikiem zamachu terrorystycznego.[8] Jednak propagandę uprawianą przez Al Kaidę wyróżnia nacisk kładziony na uzasadnianie ideologiczne i merytoryczne działań prowadzonych przez organizację. Niemalże za każdym razem przywódcy tej organizacji odwołują się do wybranych fragmentów Koranu, przedstawiając jego własne, skrajnie radykalne interpretacje, które mają niezwykle silny wpływ na słabo wyedukowane społeczeństwo muzułmańskie. Terroryści Al Kaidy przedstawiają swoje działania, jako wojnę totalną ze światem zachodnim, a siebie, jako obrońców islamu i wszystkich „prawdziwych” muzułmanów. Aby uzmysłowić propagandę, jaką stosuje Al Kaida należy przytoczyć fragment odzewu organizacji, opublikowanego na serwerze Al Neda: „Krucjata, którą Ameryka i świat prowadzą przeciwko islamowi i muzułmanom, nie jest walką militarną, ekonomiczną, polityczną i kulturalną. Ta wojna jest wojną wszechstronną, odbywającą się na wszystkich poziomach, która różni się znacznie od poprzednich wojen toczonych przez muzułmanów, jak pierwsza wojna w Afganistanie, wojna w Bośni i Hercegowinie, pierwsza i druga wojna w Czeczenii lub druga wojna o Palestynę. Tę wojnę rozpoczął wróg, który uznaje ją za wojnę decydującą…”. W oświadczeniach Al Kaidy często używa się, typowych dla chwytów reklamowych, krótkich, łatwych do zapamiętania zwrotów emocjonalnych, jak

[7] Nazwa publikacji pochodzi od przezwiska Al Battar, jakie miał szejk Yousef al-Ayyiri, były osobisty ochroniarz bin Ladena.
[8] Spłonęło wówczas ok. 1,84 mln akrów lasów na terytorium 19 stanów.

„Ameryka przeciw Islamowi i Muzułmanom". Stosowanie takich zabiegów jak przykucie uwagi odbiorcy i umożliwienie mu łatwego zapamiętania kluczowych informacji, świadczy o ogromnej wiedzy terrorystów na temat socjotechnik masowego przekazu. Ugrupowania terrorystyczne, oprócz działań mających na celu rozbudzanie nienawiści do swoich przeciwników, prowadzą kampanie na rzecz ideologicznego uzasadnienia prowadzonej przez siebie walki. Przykładem takiej indoktrynacji jest opublikowany 9 grudnia 2001 r. na witrynie internetowej Azzam Publications tzw. list pożegnalny Osamy bin Ladena do muzułmanów. Powołując się na fakty historyczne i przykazania islamu, zachęcał on wszystkich muzułmanów na świcie do walki z USA i ich sojusznikami oraz apelował o ostateczne i całkowite odrzucenie kultury zachodniej.

Z początkiem XXI w. zauważalne jest dążenie organizacji terrorystycznych do prowadzenia skoordynowanej działalności propagandowej w Internecie. Czeczeni skoncentrowali się na prowadzeniu spójnej działalności propagandowej za pośrednictwem witryny kavkazcenter.com oraz jej 6 wersji, działających pod innymi adresami, redagowanych w językach rosyjskim, angielskim i tureckim. Natomiast Hamas zorganizował kilkustopniowy system dystrybuowania informacji w formie piramidy. Jej wierzchołek stanowi główna strona informacyjna organizacji,[9] wspomagana przez 6 stron bliźniaczych, redagowanych w językach angielskim, francuskim, rosyjskim, malajskim, urdu i farsi. Na stronach tych informacje są dystrybuowane do innych witryn internetowych, posegregowanych w zależności od związków z Hamasem i przydatności informacyjnej dla niego. Spójna polityka propagandowa umożliwia organizacji zarządzanie informacjami przekazywanymi do kilkudziesięciu witryn internetowych redagowanych w ok. 20 językach.

Niezależnie od Internetu terroryści wykorzystują również inne media, zapewniające dostęp do grupy odbiorców niemalże na całym świecie. Najbardziej znanymi przykładami takich działań są oświadczenia Al Kaidy, nagrywane na taśmach wideo i publikowane po ich otrzymaniu, przez satelitarną telewizję Al-Jazzeera działającą w Katarze.[10] Jednym z wielu takich wystąpień jest chociażby pierwsze po zamachach z 11 września 2001 r. przemówienie Osamy bin Ladena opublikowane 7 października 2001 r. Wówczas ubrany w mundur polowy, potępił rozpoczęcie nalotów przez amerykańskie myśliwce na Afganistan nazywając je atakami na islam oraz ogłosił początek „Świętej Wojny". Wezwał tym samym wszystkich muzułmanów do walki z niewiernymi. Ugrupowaniom terrorystycznym udaje się również incydentalnie wykorzystywać media zachodnie do działalności propagandowej.

[9] Główna witryna organizacji działała pod adresem: www.palestine-info.com.
[10] Arabski odpowiednik CNN.

Znakomitym przykładem tej tezy jest arabskojęzyczne radio Salaam, nadające z Brukseli. Jego główny prezenter zanim został aresztowany prze belgijskie służby specjalne w styczniu 2003 r., regularnie wygłaszał odezwy wzywające muzułmanów do „Świętej Wojny". Z kolei 3 lutego 2005 r. brytyjska telewizja Chanel 4 wyemitowała wywiad z Szamilem Basajewem, w którym stwierdził on, że konieczne jest przeprowadzanie większej liczby takich akcji jak w Biesłanie. Ta sama telewizja 27 lutego 2007 r. wyemitowała wywiad z wysokim dowódcą Talibów, mułłą Dadullahem, który mówił o setkach ochotników do przeprowadzania zamachów samobójczych w Afganistanie. Śmiało można to stwierdzenie zdyskredytować, gdyż podczas weryfikacji pochodzenia oraz dobrowolności wielu zamachowców-samobójców, w większości przypadków okazywało się, iż to rodzina poświęcała członka swojej rodziny, który często był niepełnosprawny i nie mógł zarabiać, a w przypadku udanego zamachu bliscy otrzymywali wynagrodzenie finansowe od organizacji terrorystycznej i byli okryci chwałą, że ich syn „odszedł" do Allaha zabijając przy tym innowierców.

Członkowie ugrupowań terrorystycznych są również specjalistami w prowadzeniu działań psychologicznych. Jak wspominano na wstępie pracy, obiektami oddziaływania terrorystów mogą być wojska własne oraz społeczność krajów islamskich, ale także wojska przeciwnika i światowa opinia publiczna. Pragną oni przy użyciu manipulacji, wzbudzić uczucie nieufność i irytacji w stosunku do legalnych władz, organów bezpieczeństwa czy też grup narodowościowych. Ponadto pozyskują w ten sposób nowych zwolenników, niezadowolonych z otaczającej ich rzeczywistości. Ostatnim z postawionych sobie celów przez organizacje terrorystyczne jest zastraszanie oponentów oraz tworzenie w społeczeństwie psychozy zagrożenia. Obecnie operacje tego typu są prowadzone głównie przez tworzenie stron internetowych z celowo spreparowaną zawartością.

Przykład działań, podejmowanych przez Al Kaidę, mających wzbudzić nieufność obywateli państw zachodnich do oficjalnej polityki informacyjnej stanowią próby prostowania lub dementowania informacji podawanych przez oficjalne ogólnoświatowe serwisy informacyjne. W artykule „Świadectwo Talibanu" z 2002 r. 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, dążenia do wywierania presji na władze, poprzez wywołanie poczucia zagrożenia wśród obywateli, była kampania psychologiczna prowadzona przez Al Kaidę w październiku i listopadzie 2001 r. Terroryści dążyli w Pakistanie do wywołania fali demonstracji i zamieszek przeciwko

udziałowi tego państwa w koalicji antyterrorystycznej oraz wspierania 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.[11] Było to niedługo po atakach na World Trade Center w 2001 r., 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 r., aby państwa Organizacji Traktatu Północnoatlantyckiego wycofały swoje wojska z Republiki Afganistanu i zaprzestali 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 ok. 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 miedzy innymi wystąpienia nagrane w Finsbury Park w Londynie i umieszczone na stronie haganah.[12] 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 r.

Wnioski

Palestyńskie ugrupowania terrorystyczne, Hamas i Hezbollah, uruchomiły własne programy edukacji komputerowej, co niewątpliwie sukcesywnie przyczynia się do wzrostu świadomości i wiedzy informatycznej ich członków i sympatyków. W rezultacie stale rośnie liczba islamistycznych grup hakerskich. Wkrótce będą one zdolne włamywać się do systemów oraz dokonywać ich penetracji, przy czym autoryzowany użytkownik

[11] Oświadczenie opublikowano głównie na serwerze Azzam Publications (www.azzam.com).
[12] Pełna nazwa witryny brzmi: www.haganah.org.il.

czy personel techniczny odpowiedzialny za jego obsługę, nawet nie zauważy tego faktu. Umożliwi to organizacjom terrorystycznym bardzo szczegółowe zaplanowanie i przeprowadzenie ataku cybernetycznego bez obaw o dekonspirację.

Należy pamiętać, że organizacje terrorystyczne nie są wyłącznie domeną islamskiego kręgu kulturowego. Europa jest również obszarem działania wielu organizacji stosujących przemoc w imię wyznawanych przez siebie poglądów. Najbardziej znanymi są Irlandzka Armia Republikańska (IRA) oraz hiszpańska organizacja walcząca o niepodległość kraju Basków (ETA).

Wreszcie należy liczyć się z ewentualnością powstania całkowicie nowej formy terroryzmu, jaką może być broń psychotroniczna. Stany Zjednoczone prowadziły już nad nią badania w połowie XX wieku. Ma ona za zadanie oddziaływać na psychikę i podświadomość człowieka, a w konsekwencji wpływanie na jego wolę i wywołanie stanu niezdolności do działania. W charakterze broni psychotronicznej mogą być zastosowane środki pochodzenia chemicznego, np. psychofarmakologiczne, antydepresyjne i halucynogenne oraz nietypowe narkotyki. Jednak prawdziwe zagrożenie związane z tą bronią wynika z możliwości wykorzystania przez terrorystów technologii teleinformatycznych i telekomunikacyjnych. Chodzi przede wszystkim o specjalnie przygotowane informacje ukryte między właściwymi obrazami, przekazywane za pośrednictwem filmów wideo, telewizji i programów komputerowych. Techniki takie umożliwiają przekazywanie sygnałów i informacji bezpośrednio do podświadomości w celu wywołania np. stanów lękowych. Można je stosować również do podnoszenia ciśnienia krwi i wywoływania epilepsji. Dobrą wiadomością jest, że wiele państw stworzyło specjalne oddziały do obrony przed przestępczością elektroniczną – tylko USA w latach 2009–2014 przeznaczą na ten cel 30 miliardów dolarów. Tym bardziej cieszy, że problem dostrzegło Wojsko Polskie. Generał Franciszek Gągor, szef Sztabu Generalnego WP, wypowiedział się na łamach dziennika „Rzeczpospolita", twierdząc, że „cyberprzestrzeń – po lądzie, morzu, powietrzu i przestrzeni kosmicznej – stała się faktycznie piątym polem, na którym prowadzone są działania wojenne".[13] Wojsko Polskie, świadome zagrożeń pochodzących z sieci planuje powołać jednostkę, której zadaniem będzie przeciwdziałanie cyberatakom. Idea utworzenia takiej jednostki powstała całkiem niedawno w Departamencie Transformacji MON.

[13] E. Żemła, *„Żołnierze na cyberwojnę"*, [Online], dostępne: http://www.rp.pl/artykul/339842.html, 25.07.2009.

Literatura.

Druki zwarte:

1. Adamski J., Nowe technologie w służbie terrorystów, Warszawa 2007.
2. Aronson E., Pratkanis A., Wiek propagandy, Warszawa 2004.
3. Barnas R., Terroryzm. Od Asasynów do Osamy bin Laden, Wrocław 2001.
4. Białek T., Terroryzm - manipulacja strachem, Warszawa 2005.
5. Borkowski R., Terroryzm ponowoczesny, Toruń 2006.
6. Kosta R., Terroryzm jako zagrożenie dla bezpieczeństwa cywilizacji zachodniej w XXI wieku, Toruń 2007.

Artykuły.

1. Pająk. A., Punkt zapalny: Elektroniczna wojna w Internecie, [Online], dostępne: http://chip.pl/artykuly/trendy/2009/11/punkt-zapalny-elektroniczna-wojna-w-internecie, 13.11.2009.
2. E. Żemła, „Żołnierze na cyberwojnę", [Online], dostępne: http://www.rp.pl/artykul/339842.html, 13.11.2009.

Strony internetowe.

1. Centrum Badań nad Terroryzmem [Online], dostępne: http://cbnt.collegium.edu.pl/index.php?option=com_content&view=article&id=83:suby-specjalne-w-wojskowych-misjach-stabilizacyjnych-w-rejonach-wzmoonej-aktywnoci-terrorystycznej--zarys&catid=34:analizy-i-raporty&Itemid=49, 16.11.2009.
2. Wszystko o terroryzmie, [Online], dostępne: http://terroryzm.com/article/490/Strategia-i-taktyka-terrorystw.html, 21.11.2009.