Tadeusz Dmochowski, Jamil Absi

Cyberterroryzm i cyberataki a społeczeństwo informacyjne na Bliskim Wschodzie

1. Wprowadzenie

Wraz z rozwojem technologii informacyjnych na całym świecie pojawiło się i rozwija zagrożenie atakami cybernetycznymi i cyberterroryzmem, co z kolei wpływa na spadek bezpieczeństwa państwa i obywateli. Region Bliskiego Wschodu, ze względu na nasilenie trwających tam konfliktów politycznych, religijnych i cywilizacyjnych, wzmocnionych jeszcze po „arabskiej wiośnie", a także z uwagi na brak lub niewielką świadomość społeczną i społecznego poczucia zagrożeń sieciowych oraz poczucia konieczności zapewnienia bezpieczeństwa, stał się łatwym celem dla hakerów i agencji wywiadowczych państw tego regionu oraz spoza niego. Dopóki nowoczesne technologie bezpieczeństwa na Bliskim Wschodzie będą ograniczały się głównie do struktur bezpieczeństwa państw, a regulacje prawne będą miały na celu przede wszystkim tłumienie wolności słowa i praw obywatela, dopóty zagrożenie atakami cybernetycznymi oraz cyberterroryzmem będzie wzrastać.

2. Cyberterroryzm

Samo pojęcie „cyberterroryzm" funkcjonuje w źródłach od stosunkowo niedawna. Jako pierwszy terminu tego użył w latach osiemdziesiątych XX w. Barry Hollin, określając w ten sposób połączenie terroryzmu z przestrzenią wirtualną (cyberprzestrzenią). Cyberterroryzmem według niego jest „jakiekolwiek użycie sieci bądź systemu komputerowego w akcji terrorystycznej", również w sensie komunikowania się czy zbierania informacji niezbędnych do przeprowadzenia aktów terroru[1]. Federalne Biuro Śledcze (FBI; ang. Federal Bureau of Investigation) stoi

[1] R. Hennig, *Czym naprawdę jest cyberterroryzm*, Krajowe Stowarzyszenie Bezpieczeństwa Teleinformacyjnego i Ochrony Informacji Niejawnych, http://www.ksbtioin.pl/index.php?option=com_

natomiast na stanowisku, że za cyberterroryzm należy uznawać każdy „obmyślony, politycznie umotywowany akt przemocy wymierzony przeciwko informacjom, programom, systemom komputerowym lub bazom danych, który mając charakter niemilitarny, jest przeprowadzony przez ponadnarodowe lub narodowe grupy terrorystyczne”[2]. Inną definicję cyberterroryzmu przytacza polska Agencja Bezpieczeństwa Wewnętrznego, określając go jako (celowe) „wykorzystywanie zdobyczy technologii informacyjnej w celu wyrządzenia szkody”, zauważając przy tym, że „atak na jeden z elementów systemu może zakłócić funkcjonowanie pozostałych («efekt domina»), ponieważ są one ściśle ze sobą powiązane”[3].

Z kolei prof. Abdullah Bin Abdulaziz Alajlan z Islamskiego Uniwersytetu Imama Muhammada Bin Sauda w Rijadzie w Arabii Saudyjskiej zdefiniował cyberterroryzm jako agresję, terroryzowanie lub szantażowanie materialne lub psychiczne osób, z pogwałceniem uczuć religijnych, nietykalności cielesnej, godności i intelektu, przy użyciu instrumentów technologii informacyjnej i środków elektronicznych wszelkiego rodzaju przez państwa, grupy zorganizowane lub osoby. Opiera się on na wykorzystaniu możliwości naukowych i technicznych oraz środków komunikacji i technologii informacyjnej w celu zastraszania, terroryzowania i szkodzenia innym[4].

Analiza powyższych definicji pozwala zaobserwować charakterystyczne dla nich wspólne mianowniki: położenie nacisku na hipotetyczną możliwość wykorzystania systemów komputerowych i telekomunikacyjnych do przeprowadzenia samego ataku, jak również wskazanie na bezpośredni cel tego ataku w postaci newralgicznych końcówek terminalowych, komputerów, serwerów czy w szerszym zakresie całych systemów informatycznych. Aby atak posiadał znamiona cyberterroryzmu, a nie tylko cyberataku, musi się opierać na akcji (działaniu) terrorystycznej oraz wiązać się ze świadomym wykorzystaniem dowolnego systemu informatycznego lub urządzenia elektronicznego w takim celu.

W związku z rozwojem technologicznym i uzależnieniem wszystkich aspektów życia od nowoczesnych technologii w obecnych czasach dla wywarcia presji i zmiany niektórych aspektów otaczającej nas rzeczywistości nie potrzeba już wielotysięcznej armii i przeprowadzenia skomplikowanych działań wojennych, lecz wystarczyć może grupa dobrze przygotowanych i kompetentnych hakerów,

content&view=article&id=30:terroryzm-w-sieci-czym-naprawd-jest-cyberterroryzm&catid=1:stowarzyszenie [dostęp: 10.10.2015].

[2] A. Kozłowski, *Cyberterroryzm w amerykańskiej wojnie z terroryzmem w XXI wieku*, http://www.academia.edu/7673885/Cyberterroryzm_w_ameryka%C5%84skiej_wojnie_z_terroryzmem_w_XXI_wieku, s. 3 [dostęp: 10.10.2015].

[3] *Cyberterroryzm*, https://www.abw.gov.pl/pl/zadania/zwalczanie-terroryzmu/cyberterroryzm/306,Cyberterroryzm.html [dostęp: 10.10.2015].

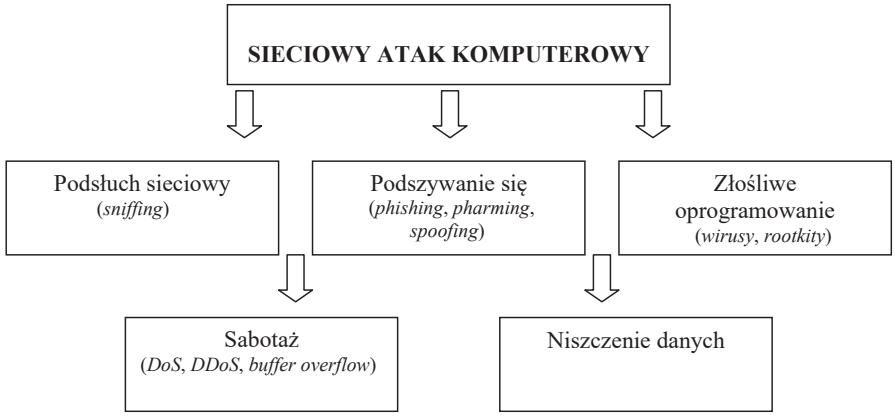
[4] A. Bin Abdulaziz Alajlan, *Cyberterroryzm w epoce technologii informacyjnych*, Pierwsza Międzynarodowa Konferencja o Ochronie Bezpieczeństwa Technologii Informacyjnych i Danych Osobowych w Prawie Internetowym, Kair 2–4.06.2008.

gotowych do prowadzenia ataków wymierzonych w newralgiczne elementy struktur informatycznych i informacyjnych oraz w same informacje, których wartość – jako towaru rynkowego – rośnie wraz ze zmianami wprowadzonymi przez rewolucję technologiczną. W przestrzeni wirtualnej (cyberprzestrzeni) połączone ze sobą siecią komputery i inne media cyfrowe komunikują się ze sobą za pośrednictwem najczęściej systemu połączeń internetowych. W tejże przestrzeni (w zasadzie informatycznej) powstają nieograniczone wręcz możliwości oddziaływań, w tym także terrorystycznych, co powoduje, że zagadnienie bezpieczeństwa w cyberprzestrzeni stało się jednym z najczęściej podejmowanych tematów w zakresie bezpieczeństwa, a stabilność i bezpieczeństwo funkcjonowania przestrzeni wirtualnej stały się priorytetami w działaniach rządów, organizacji międzynarodowych czy gospodarczych (np. banków).

W ramach ataków na sieci komputerowe można wyróżnić m.in. następujące typy działań szkodliwych:

- nieuprawnione wejście do systemu komputerowego poprzez naruszenie zastosowanych zabezpieczeń w celu kradzieży bądź manipulacji danych,
- niszczenie informacji, czyli naruszenie jej integralności poprzez bezprawne wymazywanie, uszkodzenie, usuwanie bądź utrudnianie czy wręcz uniemożliwienie zapoznania się z nią osobie do tego uprawnionej,
- sabotaż komputerowy – polegający na paraliżowaniu bądź zakłócaniu pracy systemów komputerowych o istotnym znaczeniu. Ten typ ataku może wystąpić w połączeniu z niszczeniem informacji lub uszkodzeniem fizycznym urządzeń służących do zapisu, przetwarzania czy gromadzenia informacji[5].

[5] W polskim kodeksie karnym przestępstwa „komputerowe" ujęto w kilku rozdziałach: przeciwko ochronie informacji w rozdz. XXXIII, art. 267 § 1 (hacking komputerowy), art. 267 § 2 (podsłuch komputerowy – nieuprawnione przechwycenie informacji), art. 268 § 2 (bezprawne niszczenie informacji), art. 269 § 1 i 2 (sabotaż komputerowy); przeciwko mieniu w rozdz. XXXV, art. 278 § 2 i 5, art. 285 § 1, art. 287 § 1, art. 293 § 1 (dotyczą: nielegalnego uzyskania programu komputerowego, oszustwa telekomunikacyjnego, oszustwa komputerowego, paserstwa programu komputerowego); przeciwko bezpieczeństwu powszechnemu w rozdz. XX – art. 165 § 1 ust. 4 (sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo mienia w znacznych rozmiarach), art. 165 § 2 (nieumyślne zakłócenie automatycznego przetwarzania informacji związane za sprowadzeniem niebezpieczeństwa powszechnego), art. 167 § 2 (zamach terrorystyczny na statek morski lub powietrzny); przeciwko Rzeczypospolitej Polskiej w rozdz. XVII, art. 130 § 2 i 3 (szpiegostwo komputerowe albo wywiad komputerowy), art. 138 § 2 (szpiegostwo albo wywiad komputerowy na szkodę państwa sojuszniczego); przeciwko wiarygodności dokumentów w rozdz. XXXIV (art. 270 § 1 (fałszerstwo komputerowe).



DoS (*denial of service*) – odmowa usługi, DDoS (*distributed denial of service*) – rozproszona odmowa usługi

Rysunek 1. Rodzaje najczęściej przeprowadzanych ataków komputerowych

Źródło: Opracowanie własne.

Region Bliskiego Wschodu jest łatwym celem dla cyberataków przede wszystkim ze względu na brak lub niską świadomość zagrożeń ze strony użytkowników internetu oraz brak uregulowań prawnych. Elementem generującym liczbę ataków jest obecność licznych konfliktów politycznych, ekonomicznych i społecznych, a przede wszystkim religijnych i cywilizacyjnych. Jako najbardziej reprezentatywne należy wymienić wojnę domową w Syrii, konflikt saudyjsko-irański oraz arabsko-izraelski.

Wiele cyberataków czy aktów cyberterroryzmu spowodowanych było przez strony-uczestników wojny domowej w Syrii. Prorežimowa Syryjska Armia Elektroniczna, używając różnych metod socjotechnicznych i złośliwego oprogramowania, atakuje użytkowników i organizacje antyrządowe w Syrii i innych krajach. Dla przykładu 8 września 2013 r. grupa ta zamieściła na stronie Polskiego Związku Wędkarskiego w Bydgoszczy apel do polskiego rządu o zaprzestanie wysyłania broni terrorystom[6]. Z kolei grupy opozycyjne atakują i niszczą syryjskie strony prorządowe.

Na początku 2012 r. haker z Arabii Saudyjskiej o pseudonimie OxOmar włamał się na izraelskie strony sportowe i zdobył dane osobowe i dane kart kredytowych tysięcy Izraelczyków. W odpowiedzi izraelscy hakerzy zwani Obrońcami Izraela (ang. *Israel Defenders*) ujawnili informacje osobowe oraz dotyczące kart kredytowych ponad 50 tys. Arabów, głównie z Arabii Saudyjskiej i innych państw Zatoki Perskiej. Z kolei OxOmar włamał się na stronę izraelskich linii lotniczych

[6] Syryjscy hakerzy zaatakowali… wędkarzy z Bydgoszczy!, 10.09.2013, http://www.se.pl/wiadomosci/polska/syryjscy-hakerzy-zaatakowali-wedkarzy-z-bydgoszczy_353725.html [dostęp: 30.10.2015].

El Al oraz zablokował na pewien czas działanie strony informacyjnej giełdy walutowej w Tel Awiwie[7].

W Iranie najbardziej znany był atak na infrastrukturę energetyczną państwa. Doszło do niego w czerwcu 2010 r., wirus Stuxnet zniszczył wówczas wirówki używane w procesie wzbogacania paliwa jądrowego, co zagroziło katastrofą ekologiczną w regionie. Kolejny wirus odkryty przez władze Iranu – Flame – zaatakował komputery irańskich urzędników, stworzono go w celu atakowania systemu operacyjnego Microsoft Windows i wykorzystywano do szpiegowania cyberprzestrzeni krajów Bliskiego Wschodu. Za tymi działaniami stały Stany Zjednoczone i Izrael[8].

Międzynarodowa grupa hakerów Anonymous organizuje od czasu do czasu cyberataki na portale i izraelskie zasoby internetowe, zwłaszcza gdy zaostrzają się stosunki pomiędzy stronami tamtejszego konfliktu[9]. W sierpniu 2012 r. izraelska grupa Cutting Sword of Justice zaatakowała wirusem Shamoon największy saudyjski koncern naftowy – Saudi Aramco, uszkadzając 30 tys. komputerów[10]. Dwa tygodnie później podobny atak nastąpił na katarską spółkę RasGas, giganta na rynku gazu, o co wywiad amerykański oskarżał Iran[11]. W 2013 r. cyberkryminaliści ukradli 45 mln USD z Bank of Muscat w Omanie i z RAKBANK (National Bank of Ras Al-Khaimah) w Zjednoczonych Emiratach Arabskich[12].

Cyberszpiegowanie na Bliskim Wschodzie odgrywa i będzie nadal odgrywało bardzo dużą rolę w lokalnych konfliktach. Głównymi aktorami na tej scenie są regionalne i zagraniczne agencje wywiadowcze. Przykładem ich działań była sprawa 43 rezerwistów izraelskiego wojskowego wywiadu elektronicznego, którzy

---

[7] S. Frenkiel, *Israeli and Arab hackers square off in cyberbattle*, http://www.npr.org/2012/01/20/145522079/israeli-and-arab-hackers-square-off-in-cyberbattle [dostęp: 30.10.2015]; T. Ben Gedalyahu, *Round two in hacker war: El Al site attacked*, http://www.israelnationalnews.com/News/News.aspx/151773#.Vj3e5F4bLyY [dostęp: 30.10.2015].

[8] D.E. Sanger, *Obama order sped up wave of cyberattacks against Iran*, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all [dostęp: 10.10.2015].

[9] *Nie udał się atak Anonymous na izraelskie zasoby internetowe*, http://wolnemedia.net/swiat-komputerow/nie-udal-sie-atak-anonymous-na-izrael/ [dostęp: 30.10.2015]; *Hack attack! Anonymous strikes at Israeli govt over Gaza*, http://rt.com/news/182520-anonymous-attack-israeli-government/ [dostęp: 30.10.2015]; *OpIsrael: Anonymous attacks hundreds of Israeli websites*, http://rt.com/news/anonymous-israel-cyber-attack-737/ [dostęp: 30.10.2015]; E. Terry, *Anonymous threatens cyber attack on Israel over Al Aqsa*, http://www.jspacenews.com/anonymous-threatens-cyber-attack-israel-al-aqsa/ [dostęp: 30.10.2015].

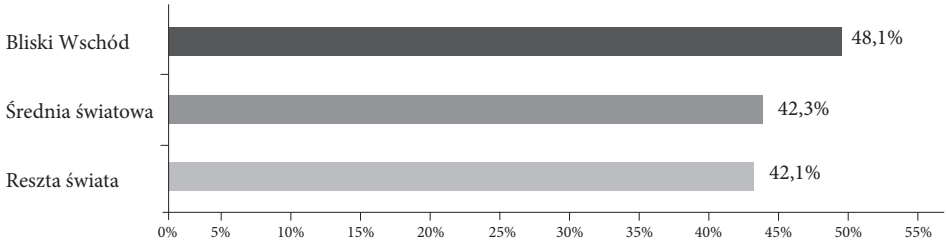
[10] *Aramco says cyberattack was aimed at production*, http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0 [dostęp: 30.10.2015]; N. Perlroth, *In cyberattack on Saudi firm*, *U.S. sees Iran firing back*, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html [dostęp: 30.10.2015].

[11] N. Perlroth, *In cyberattack on Saudi firm…*

[12] *Six arrested in $45m global cybercrime involving RAKBANK*, *Bank of Muscat*, http://gulfbusiness.com/articles/industry/finance-and-investment/six-arrested-in-45m-global-cybercrime-involving-rakbank-bank-of-muscat/ [dostęp: 30.10.2015].

złożyli na ręce premiera Benjamina Netanjahu list z deklaracją odmowy szpiegowania Palestyńczyków na okupowanych terytoriach.

Według raportu Internet World Space w 2014 r. liczba użytkowników internetu na Bliskim Wschodzie wynosiła 113 609 510, czyli 48,1% ogółu ludności regionu[13] (rys. 2).



Rysunek 2. Zasięg internetu na Bliskim Wschodzie (stan na 31 grudnia 2014 r.) w procentach użytkowników w stosunku do ogółu ludności regionu, w porównaniu z resztą świata i średnią światową. Liczbę użytkowników internetu w 2014 r. szacowano na 3 073 028 193 osób

Źródło: Internet World Space, http://www.internetworldstats.com/stats5.htm [dostęp: 30.10.2015].

Stale rośnie liczba użytkowników telefonów komórkowych, smartfonów i internetu mobilnego. Szacuje się, że do końca 2014 r. liczba użytkowników telefonów komórkowych na Bliskim Wschodzie i w Afryce może osiągnąć 525,08 mln (dając temu regionowi drugie miejsce na świecie po regionie Azji i Pacyfiku z 2,43 mld telefonów). Użycie smartfonów na Bliskim Wschodzie i w Afryce wzrośnie z 5,1% do 8,3% (na samym Bliskim Wschodzie do 2015 r. spodziewany jest wzrost o 39% liczby użytkowników). Dotychczas w Katarze jest najwięcej użytkowników smartfonów w regionie (75%). Na drugim miejscu znajdują się Zjednoczone Emiraty Arabskie (73%)[14].

Według raportu producenta oprogramowania antywirusowego Kaspersky Lab za pierwszy kwartał 2014 r. program antywirusowy Kaspersky zneutralizował na Bliskim Wschodzie ponad 34,9 mln cyberataków i złośliwych programów na komputerach i urządzeniach mobilnych, co świadczy o blisko 10-procentowym wzroście liczby ataków w stosunku do 2013 r. Najwięcej cyberataków dokonano w Arabii Saudyjskiej – 9,8 mln, 80% z nich miało charakter wewnętrzny. W Zjednoczonych Emiratach Arabskich było ich do tej pory ok. 8,7 mln. Następne miejsca pod względem liczby cyberataków zajmują kolejno Egipt, Katar, Irak, Oman, Kuwejt, Liban i Bahrajn[15].

[13] Internet World Space, http://www.internetworldstats.com/stats5.htm [dostęp: 30.10.2015].

[14] *Smartphone usage in the Middle East. Statistics and trends*, http://www.infinitemonkeys.mobi/blog/smartphone-usage-in-the-middle-east-statistics-and-trends-infographic/ [dostęp: 10.10.2015].

[15] *Kaspersky Lab reports on cyber threats in the Middle East in the first quarter of 2014*, http://me.kaspersky.com/en/about/news/virus/2014/Kaspersky_Lab_reports_on_cyber_threats_in_the_Middle_East_in_the_first_quarter_of_2014 [dostęp: 10.10.2015].

W raporcie zamieszczonym w „Kaspersky Security Bulletin" odnotowano, że w latach 2012–2013 miały miejsce następujące incydenty[16]:

- zniszczenie przy pomocy szkodliwego oprogramowania systemów komputerowych kilku platform wiertniczych na Bliskim Wschodzie,
- infiltracja systemów komputerowych na Bliskim Wschodzie wymierzona głównie przeciwko Iranowi i Izraelowi (złośliwe oprogramowanie Mahdi),
- ataki wymierzone przeciwko Saudi Aramco – jednemu z największych na świecie koncernów naftowych. W wyniku ataku całkowicie zniszczono ponad 30 tys. komputerów (wirus Shamoon),
- zakrojone na szeroką skalę próby nieautoryzowanego dostępu do urządzeń mobilnych (głównie telefonów komórkowych) własnych obywateli przez rządy Egiptu i Indii,
- działania szkodliwego oprogramowania znanego pod nazwą Flame, a także Gauss, sponsorowanego przez państwo trojana bankowego mającego na celu wykradanie danych uwierzytelniających transakcje bankowe *online* (zwłaszcza w Libanie).

Złożoność ataków i możliwości oprogramowania nie pozostawiają wątpliwości, że za tymi atakami stoi któryś z rządów (podejrzewa się Stany Zjednoczone i Izrael), a ślady prowadzą do twórców Stuxneta).

3. Społeczeństwo informacyjne

Społeczeństwo informacyjne to według Urzędu Komitetu Integracji Europejskiej „nowy typ społeczeństwa, które ukształtowało się w krajach, w których rozwój nowoczesnych technologii teleinformatycznych osiągnął bardzo szybkie tempo. Podstawowymi warunkami, które muszą być spełnione, aby społeczeństwo można było uznać za informacyjne, jest rozbudowana nowoczesna sieć telekomunikacyjna, która swoim zasięgiem obejmuje wszystkich obywateli oraz rozbudowane, dostępne dla wszystkich zasoby informacyjne. Społeczeństwo informacyjne nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz środki te są podstawą tworzenia dochodu narodowego i dostarczają źródła

[16] „Kaspersky Security Bulletin" 2012; „Kaspersky Security Bulletin" 2013. Zob. też K. Zetter, *Mahdi, the Messiah*, *Found Infecting Systems in Iran*, *Izrael*, http://www.wired.com/2012/07/mahdi/ [dostęp: 10.10.2015]; „Kaspersky Security Bulletin" 2012. *Ewolucja szkodliwego oprogramowania*, securelist.pl/threats/detect/7097,kaspersky_security_bulletin_2012_ewolucja_szkodliwego_oprogramowania.html [dostęp: 10.10.2015]; *GReaT*, *Gauss: Nation-state cyber-surveillance meets banking Trojan*, https://securelist.com/blog/incidents/33854/gauss-nation-state-cyber-surveillance-meets- banking- trojan-54/ [dostęp: 10.10.2015]; *Kaspersky Lab Discovers 'Gauss' – A New complex cyber-threat designed to monitor online banking accounts*, 2012,http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Discover_Gauss_A_New_Complex_Cyber_Threat_Designed_to_Monitor_Online_Banking_Accounts [dostęp: 10.10.2015].

utrzymania większości społeczeństwa. Ważnym aspektem jest również kształcenie społeczeństwa w kierunku dalszego rozwoju, tak by wszyscy mogli w pełni wykorzystywać możliwości, jakie dają środki masowej komunikacji i informacji"[17].

Sieć już dawno przestała być jedynie środkiem łączności. Dominują w niej strumienie ruchu złożonego, integrujące różne media transmisyjne umożliwiające komunikację interaktywną, realizowaną w czasie rzeczywistym. Współczesna technika teleinformacyjna umożliwia tworzenie zdalnie funkcjonujących systemów dających możliwość ingerencji w przebieg realizowanych procesów, pozwala również tworzyć systemy szybkiego reagowania na zagrożenia, awarie i katastrofy oraz ostrzegania przed potencjalnymi możliwościami ich wystąpienia[18].

„Powszechność, wielostronność i dynamika rozwoju w dziedzinie techniki informacyjnej spowodowały kształtowanie się nowych jakości określanych jako proces powstawania społeczeństwa informacyjnego, którego bazę rozwojową stanowi – obok informatyki – telekomunikacja". A sama informacja stała się jednym z podstawowych zasobów gospodarczych, który ze względu na swoje specyficzne cechy, takie jak wszechstronne oddziaływanie na masową skalę oraz szeroki obieg w czasie rzeczywistym, silnie oddziałuje na rozwój gospodarczy i społeczny[19].

Z analizy ankiety przeprowadzonej wśród mieszkańców Bliskiego Wschodu oraz Polski, dotyczącej wiedzy na temat cyberterroryzmu, wynika, że zauważalne są różnice w postrzeganiu tego typu zagrożeń przez obie grupy. Wiedza polskich ankietowanych w tym zakresie jest tylko nieco pełniejsza. Ale różnice nie są duże, zwłaszcza w świetle obecnej sytuacji na Bliskim Wschodzie, gdzie konflikty wyniszczają kraje regionu, a większość rządów jest bardziej zainteresowana kontrolą internautów niż ich kształceniem w tej dziedzinie.

Wiedza mieszkańców Bliskiego Wschodu na temat ochrony danych osobowych wynika raczej z powszechnego zainteresowania urządzeniami mobilnymi, korzystania z internetu na dużą skalę oraz chęci poszerzania wiedzy na temat cyberataków i cyberterroryzmu, które stały się elementem codziennego życia, co wymusza konieczność zwiększenia ochrony prywatności, tradycyjnie odgrywającej istotną rolę w obyczajowości społeczeństw regionu.

[17] Definicja społeczeństwa informacyjnego, Urząd Komitetu Integracji Europejskiej, http://archiwum-ukie.polskawue.gov.pl/www/serce.nsf/0/6A1F328341480FEAC1256F6A0038762F?Open [dostęp: 10.10.2015].

[18] Zob. *Rozwój technologii oraz infrastruktury teleinformatycznej warunkiem budowy społeczeństwa informacyjnego. Opracowanie przygotowane przez Centralne Kolegium Sekcji Telekomunikacyjnej SEP*, http://www.sep.com.pl/aktualnosci/rozwtech.html [dostęp: 10.10.2015].

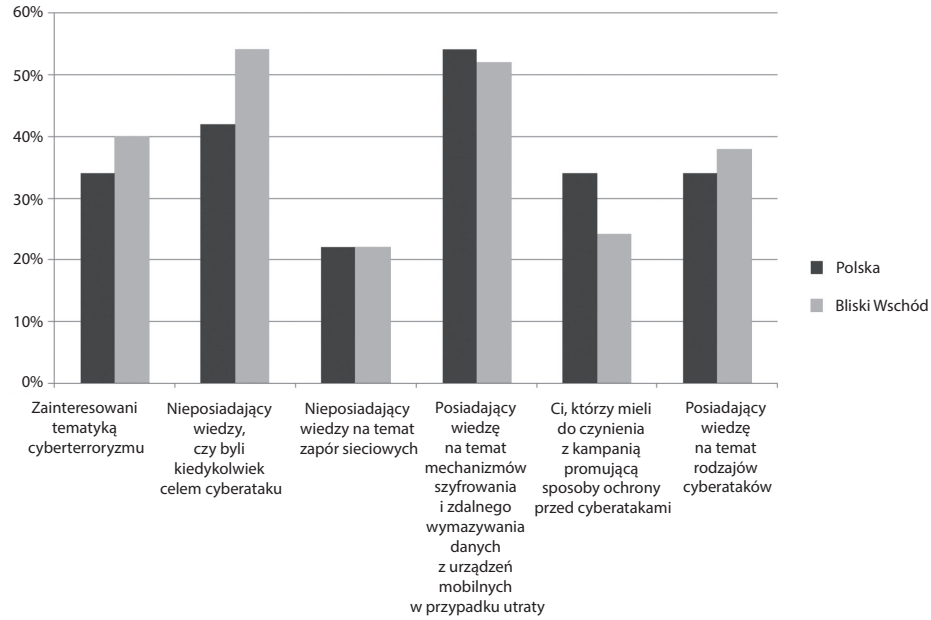
[19] *Ibidem*.

Tabela 1. Elementy wiedzy mieszkańców Polski i Bliskiego Wschodu na temat cyberataków i cyberterroryzmu i możliwości im zapobiegania

Pytania	Pochodzenie ankietowanych	Odpowiedzi		
		tak		nie
1. Czy interesuje Cię tematyka cyberterroryzmu?	Polska	34		38
	Bliski Wschód	40		50
2. Czy byłeś kiedykolwiek celem cyberataku?	Polska	14		44
	Bliski Wschód	12		34
3. Czy w swoim komputerze masz zainstalowaną zaporę sieciową (*firewall*)?	Polska	56		22
	Bliski Wschód	58		20
4. Czy znane Ci są mechanizmy szyfrowania i zdalnego wymazywania danych z urządzeń mobilnych w przypadku ich utraty/kradzieży?	Polska	tak, stosuję je na co dzień 24	tak, ale nie widzę potrzeby ich stosowania 30	46
	Bliski Wschód	22	30	48
5. Czy spotkałeś się z kampanią promującą sposoby obrony przed cyberatakami?	Polska	34		66
	Bliski Wschód	24		76
6. Czy znane Ci są pojęcia DDoS, *malware*, *flooding*, *spoofing*?	Polska	34		66
	Bliski Wschód	38		62

Źródło: Opracowanie własne na podstawie: J. Absi, niepublikowane ankiety i ich analiza. Materiały do pracy doktorskiej *Zastosowanie cyberinstrumentów w konfliktach politycznych na Bliskim Wschodzie*. W ankiecie wzięło udział 100 osób (po 50 osób pochodzenia polskiego i arabskiego: 17 z Omanu, 12 z Arabii Saudyjskiej, 10 z Palestyny, 6 z Jordanii, po 2 z Syrii i Sudanu, 1 z Iraku).

Na rysunku 3 porównano stan wiedzy społeczeństwa na temat zapobiegania cyberatakom w Polsce i na Bliskim Wschodzie, z analizy wynika, że w obu analizowanych grupach jest on zbliżony.



Rysunek 3. Porównanie wiedzy społeczeństwa na temat zapobiegania cyberatakom w Polsce i na Bliskim Wschodzie. Uwzględniono dane 100 osób (po 50 osób pochodzenia polskiego i arabskiego: 17 z Omanu, 12 z Arabii Saudyjskiej, 10 z Palestyny, 6 z Jordanii, po 2 z Syrii i Sudanu, 1 z Iraku)

Źródło: Opracowanie własne.

4. Podsumowanie

W obliczu zagrożeń związanych z aktami cyberterroryzmu i cyberatakami najistotniejsze dla zapewnienia bezpieczeństwa sieci staje się powszechne stosowanie i ciągła aktualizacja systemów i mechanizmów zabezpieczeń. Muszą one mieć charakter wszechstronny i dotyczyć wszystkich poziomów przesyłania, przetwarzania i przechowywania informacji, w tym[20]:

- na poziomie sieciowym m.in. poprzez:
  - blokowanie określonych połączeń wychodzących i przychodzących według portu, domeny, adresu IP czy protokołu,
  - analizę ruchu sieciowego w celu wykrycia anomalii i ich zbadania,
  - wykrywanie i blokowanie podejrzanego ruchu sieciowego (poleceń, plików przychodzących z internetu, transmisji poufnych danych z wewnątrz instytucji),

[20] *Polityki dotyczące bezpieczeństwa: nadużywanie zasobów*, http://securelist.pl/analysis/7234,polityki_dotyczace_bezpieczenstwa_naduzywanie_zasobow.html [dostęp: 10.10.2015].

– na poziomie aplikacji ich kontrola powinna:
  - blokować uruchamianie i pobieranie niezaufanych programów,
  - uniemożliwiać zaufanym programom implementację złośliwego kodu,
  - ograniczać dostęp aplikacji systemowych zasobów i plików,
  - blokować potencjalnie niebezpieczne zaimplementowane funkcje, niestanowiące funkcji domyślnej aplikacji,
– integralnym elementem zabezpieczającym informacje powinno być również szyfrowanie plików/dysków oraz przesyłanie zaszyfrowanych danych.

Przedstawione powyżej elementy nie będą w stanie same w sobie zapewnić bezpieczeństwa i zapobiegać atakom sieciowym, w szczególności atakom ukierunkowanym na określoną osobę, instytucję, usługę, lub określone zasoby. W celu skutecznej ochrony przed cyberterroryzmem oraz cyberatakami na kluczowe dla funkcjonowania państwa instytucje polityczne, militarne i gospodarcze, w tym bankowe, niezbędna jest nie tylko współpraca i koordynacja działań instytucjonalnych w powiązaniu ze specjalistami do spraw bezpieczeństwa, systemów komputerowych, sieci itd., lecz również podjęcie szeroko zakrojonych działań w zakresie edukacji użytkowników – zarówno pracowników firm i instytucji, jak i zwykłych „cywilnych" użytkowników komputerów i internetu.

Istotnymi zatem zadaniami stają się nie tylko rozwijanie informatycznych systemów bezpieczeństwa, lecz również opracowanie, wdrożenie i egzekwowanie nowoczesnej i dostosowanej do zagrożeń polityki bezpieczeństwa; edukacja pracowników i użytkowników w zakresie potencjalnych zagrożeń i przestrzegania procedur; kontrola przyznanych uprawnień na poziomie pracownika i użytkownika; wdrożenie bezpiecznych mechanizmów i procedur uwierzytelniających; bieżące i wyprzedzające eliminowanie potencjalnie szkodliwych działań pracowników i użytkowników.

W zwalczaniu zagrożeń w cyberprzestrzeni kluczową rolę zawsze będzie odgrywał czynnik ludzki, dotyczy to zarówno strony atakującej (haker lub grupa hakerów), jak i atakowanej (pracowników instytucji lub zwyczajnych użytkowników, będących w polu zainteresowania atakujących). Często to pracownicy są najsłabszym ogniwem zabezpieczeń systemów informatycznych, których świadome lub nieświadome działania, w tym podatność na zewnętrzną manipulacje (*phishing*, socjotechniki), umożliwiają rozpoczęcie penetracji i przełamywania barier obronnych systemu, umożliwiając dostęp do danych wrażliwych.

Streszczenie

W artykule skupiono się na cyberterroryzmie i cyberatakach w regionie Bliskiego Wschodu jako nowoczesnych metodach prowadzenia walki i wojny w cyberprzestrzeni, służących niszczeniu zarówno infrastruktury elektronicznej przeciwnika, jak i osłabianiu go we wszystkich aspektach – politycznym, militarnym, społecznym i gospodarczym

poprzez penetrację, sianie zamętu i zdobywanie oraz usuwanie lub zamianę danych. Z przeprowadzonej ankiety wynika, że stan wiedzy o zagrożeniach związanych z cyberterroryzmem i cyberatakami oraz o sposobach zapobiegania im w Polsce i wybranych krajach Bliskiego Wschodu jest podobny.

Słowa kluczowe: cyberterroryzm, cyberatak, społeczeństwo informacyjne, Bliski Wschód

Cyberterrorism, cyberattacks, and the information society in the Middle East

Summary

The article describes the cyberattacks and cyberterrorism in the Middle East as modern warfare in the cyber space which serve not only weakening of electronic infrastructure of the enemy, but also weakening him in every aspect – political, military, social and economic – through penetration, wreaking havoc, gathering, destroying or modifying data. On the base of survey data one may notice a similar level of knowledge about cyberattack and cyberterrorism threats and countering them in Poland and some states in the region.

Keywords: cyberterrorism, cyberattack, the information society, Middle East