DOI:10.17951/h.2016.50.2.31

A N N A L E S
UNIVERSITATIS MARIAE CURIE-SKŁODOWSKA
LUBLIN – POLONIA

VOL. L, 2 SECTIO H 2016

Uniwersytet Warszawski. Wydział Zarządzania

JERZY KISIELNICKI

jkisielnicki@wz.uw.edu.pl

Po drugiej strony mocy, czyli ciemne strony informatyki

On the Other Site of the Power that is the Dark Side of Science

Słowa kluczowe: cyberwojny; cyberkonflikt; terroryzm; technologia informacyjno-komunikacyjna; informatyka

Keywords: cyber-wafare; cyber-conflict; terrorism; Information and Communication Technology; computer science

Kod JEL: M15

Wstęp

Prezydent Rzeczypospolitej Polskiej Bronisław Komorowski w dokumencie z dnia 22 stycznia 2015 r. przedstawił problematykę zagrożenia Polski przez cyberterroryzm. Napisał w specjalnym przesłaniu do przyjętej przez Rząd RP doktryny cyber-bezpieczeństwa RP: „Cyberprzestrzeń jest polem konfliktu, na którym przychodzi nam zmierzyć się nie tylko z innymi państwami, ale także z wrogimi organizacjami, jak choćby z grupami ekstremistycznymi, terrorystycznymi czy zorganizowanymi grupami przestępczymi. Dlatego jednym z istotnych priorytetów polskiej strategii stało się bezpieczeństwo tego nowego środowiska".

Jeżeli nasze społeczeństwo jest świadome możliwości, jakie daje zastosowanie systemów informatycznych i umie je wykorzystać dla wzbogacenia się i wspomagania procesów podejmowania decyzji, to na pewno będzie szczęśliwsze (w potocznym słowa tego rozumieniu). Współczesna cywilizacja, która często bywa nazywana

cywilizacją informacyjną, to jednak nie tylko pozytywy, ale także nowe zagrożenia. J. Ryan stwierdził nawet, że „Ataki informacyjne są największą innowacją w dziedzinie prowadzenia wojen od czasu wymyślenia prochu" [cyt. za: Bartoszek, 2008]. Ataki na infrastrukturę państwa, które potencjalnie mogłyby spowodować trwałe szkody, są uznawane za jedno z największych zagrożeń dla bezpieczeństwa narodowego Stanów Zjednoczonych. W wywiadzie dla telewizji Fox News szef połączonych sztabów sił zbrojnych USA, generał Martin Dempsey, ostrzegł, że cyberprzestrzeń jest obszarem, w którym Amerykanie mogą mierzyć się z równorzędnymi przeciwnikami, mimo że w innych dziedzinach dysponują znaczną przewagą militarną [za: Defensy24, 2015].

Na podstawie analizy dostępnych raportów, przeprowadzonych rozmów z osobami odpowiadającymi za problematykę bezpieczeństwa kraju i dyskusji na seminarium dotyczącym współczesnych zagrożeń cyberterrorystycznych i bioterrorystycznych w kontekście bezpieczeństwa narodowego Polski [Sienkiewicz, 2015] została postawiona teza, że szczególnie wrażliwe na atak cybernetyczny są państwa o rozwiniętych systemach informacyjnych. Ich rozwój gospodarczy spowodował, że cechują się dużym stopniem zależności od systemów informatycznych. Wrażliwe są szczególnie systemy wspomagające funkcjonowanie telekomunikacji, systemów energetycznych, transportu, systemu zaopatrzenia, systemów bankowych i finansowych, produkcji (w szerokim znaczeniu tego słowa), służb ratowniczych i szpitali. Wymienione systemy tworzą tzw. krytyczną infrastrukturę państwa. Zniszczenie jej lub uszkodzenie może osłabić zdolność obronną oraz bezpieczeństwo funkcjonowania państwa, przerwać ciągłość funkcjonowania władzy i służb publicznych. W nomenklaturze anglosaskiej są określane jako SCADA (*Supervisory Control and Data Aquisition*). Jak pisze G.J. Ratrray [2006]: „Im bardziej określone państwo jest uzależnione od swoich infrastruktur informacyjnych, w tym większym stopniu infrastruktury te stają się środkami ciężkości wartymi atakowania i obrony".

1. Portale społecznościowe jako narzędzie rekrutacji i propagowania idei terroryzmu

Wstępny i pozornie niedoceniany etap przygotowań do cyberwojny to bezkrwawa wojna informacyjna. Musimy uznać, iż informacja we współczesnym świecie jest wykorzystywana jako broń. P. Sienkiewicz [2015] określa walkę informacyjną jako całokształt działań ofensywnych i defensywnych mających na celu uzyskanie przewagi informacyjnej nad przeciwnikiem. Potencjał militarny państwa tworzą również zasoby informacyjne pozwalające na działania zgodne z przyjętą strategią obronną. Przykładów takich działań jest wiele: konflikt rosyjsko-ukraiński i rosyjsko-gruziński, ataki przeprowadzone przez Kalifat islamski w Afryce, działania Al-Kaidy. Szczególnie działania tej ostatniej organizacji są bardzo niebezpieczne. „Dżihad dla każdego" – demokracje zachodnie, zwłaszcza w Europie, stoją dziś przed poważnym zagrożeniem terrorystycznym ze strony własnych obywateli. Chodzi nie

tylko o potomków muzułmańskich imigrantów ulegających radykalizacji religijnej i ideologicznej, ale również o młodych ludzi zafascynowanych nową religią i nową ideologią. Minister bezpieczeństwa USA, Michael Chertoff, składając wyjaśnienia przed senacką Komisją Bezpieczeństwa Wewnętrznego i Spraw Rządowych, powiedział, że internet jest obecnie głównym medium, przez które Al-Kaida zdobywa zwolenników w USA.

Rys. 1. Goście audycji propagującej przez internet terroryzm

Źródło: [www.bing.com/images/search?q=Al+Kaida+werbowanie+przez+Internet+t&FORM=HDRSC2#view=detail&id=64338AF9F021D3398370C00EE210B6263BA5A78A&selectedIndex=6].

Jedna z organizacji terrorystycznych, jak informuje Daily Mail [MailOnline, 2010], wydała magazyn internetowy zatytułowany „Inspire", ukazujący się w języku angielskim. Zdaniem specjalistów ma rekrutować bojowników w krajach zachodnich. W środku znalazł się m.in. artykuł *Jak zmontować bombę ze składników dostępnych w kuchni twojej matki*. Jest on wyraźnie skierowany do rodzącego się dżihadu w USA i Europie. Szefem pisma jest Jemeńczyk, Anwar al-Awlaki. Jego kazania w internecie przyczyniły się do zwerbowania terrorystów – obywateli USA: Bryanta Neala Vinasa i Najibullaha Zazi. Al-Awlaki poza tym prowadzi własny blog, ma profil na Facebooku i z dużą częstotliwością umieszcza filmiki propagandowe na YouTubie. Dzięki tej działalności został okrzyknięty „bin Ladenem internetu" – informuje „Chip".

2. Cyberwojna (*cyber-wafare*)

Pod pojęciem cyberwojny rozumiemy konflikt w skali międzypaństwowej lub globalnej, który będzie prowadzony przede wszystkim z użyciem technologii infor-

macyjno-komunikacyjnej (*Information – Comunication Technology*, ICT). Często w literaturze na określenie cyberwojny używa się też pojęcia *cyber-warfare*. Jest to użycie systemów informatycznych, czyli hardweru, softweru, internetu i innych środków przechowywania lub rozprzestrzeniania informacji w celu przeprowadzenia ataków na systemy informacyjne i informatyczne przeciwnika.

Wojnę cybernetyczną od tzw. klasycznych wojen odróżnia środowisko pola walki. Tu nie jest ściśle określony teren w znaczeniu fizycznym, ale wirtualna przestrzeń, np. chmury komputerowe, sieci teleinformatyczne. Rozwój *cloud computingu* stwarza warunki do prowadzenia takiej wojny. W cyberwojnach strona atakująca byłaby zdolna sparaliżować kluczową infrastrukturę zarządzania, a w konsekwencji – gospodarkę państwa przeciwnika. Ten paraliż jest oparty na systemach komputerowych przeciwnika. Wojna cybernetyczna to atak w dużym stopniu asymetryczny, co pozwala na prowadzenie tego rodzaju wojen państwom militarnie i gospodarczo słabszym przeciwko tym silniejszym. L. Janczewski z Uniwersytetu w Auckland [2015], zajmujący się problematyką bezpieczeństwa informacyjnego i konfliktami w cyberprzestrzeni, stawia wprost pytanie: czy trzecia wojna światowa to cyberwojna? W tym zakresie możemy tylko przypuszczać, iż najbardziej prawdopodobny scenariusz to wojna hybrydowa. W takiej wojnie obok działań klasycznych udział będą miały też działania określane terminem cyberwojny i cyberkonfliktów. Relacje między tymi elementami będą różne, ale na pewno działania te będą się wspomagały. „Czysta" cyberwojna oznacza, że tylko technologia informatyczna byłaby stosowana przez obie strony konfliktu. Można przypuszczać, że w praktyce cyberwojna będzie stosowana jako technika wspierająca [Kisielnicki, 2014a; Kisielnicki, 2014b].

Przestrzeń kosmiczna i internet (cyfrowa przestrzeń) to według Han Xudonga z pekińskiej uczelni wojskowej kolejne fronty działań militarnych w czymś, co można określić mianem zbliżającej się „III wojny światowej" [według serwisu interia.pl, 2015].

Jak podają różne źródła prasowe, to Edward Snowden ujawnił, jako jeden z pierwszych, fakty o sposobie, w jaki Amerykanie przygotowują się do ewentualnej cyberwojny. I tak Agencja Bezpieczeństwa Narodowego (NSA) nie będzie brała cyfrowych jeńców, ale będzie niszczyła komputery, routery i sprzęt przeciwnika. W razie konieczności zostaną zaatakowane elektrownie, oczyszczalnie wody, lotniska. Wiemy również z ujawnionych materiałów, że cały czas narzędzia informatyczne zbierają informacje o praktycznie każdym obywatelu kuli ziemskiej, nie wyłączając inwigilacji szefów rządów zaprzyjaźnionych państw. Mamy do czynienia ze śledzeniem każdego kroku (znają hasła, loginy) inwigilowanej osoby. Te rozwiązania nie są niczym nowym, ale według informacji E. Snowdena NSA i podobnego typu organizacje specjalizują się w takich działaniach. Zgodnie z tymi materiałami NSA jest przekonana, że „III wojna światowa rozpocznie się w internecie". W 2013 r. Agencja Bezpieczeństwa Stanów Zjednoczonych miała otrzymać miliard dolarów na przygotowanie strategii cyberobrony, w tym również na „niekonwencjonalne działania". Nie wiadomo dokładnie, co kryje się pod tym terminem, ale takie plany budzą spory niepokój.

W przygotowaniach do nowego rodzaju wojny pojawiają się różnego typu nowe rozwiązania, np. zdobywanie nowych informacji z użyciem samolotów bezzałogowych (dronów). Drony są przecież sterowane z użyciem technologii informatycznej. W Polsce na straży naszych wschodnich granic będą natomiast stać bezzałogowe samoloty.

Problematyka cyberwojny i cyberkonfliktów jest analizowana zarówno przez władze polityczne, jak i wojskowe [por. Clarke, Knake, 2012]. Krajowe polityki w tej dziedzinie zostały przygotowane w wielu państwach, między innymi w Polsce i krajach NATO. I tak administracja USA ujawniła swoją politykę w maju 2012 r. [Howard, 2012]. Podobny dokument został opublikowany w grudniu 2012 r. w Wielkiej Brytanii. System obrony cyfrowej został upubliczniony w czerwcu 2012 r. w Holandii pt. *Strategia Cyber Defence* (2012). Dokument ten zaproponował zupełnie nowe podstawy do obrony państwa obejmującego współpracę z komercyjnym sektorem prywatnym. Wiele rządów uzupełnia istniejące struktury organizacyjne (sił lądowych, marynarki i sił powietrznych itp.) nowymi jednostkami, jakimi są siły obrony cybernetycznej. W październiku 2010 r. w Stanach Zjednoczonych zostały powołane specjalne siły pod nazwą United States Cyber Command (USCC). Rozwijają się organizacje międzynarodowe, które zajmują się problematyką obrony cyberprzestrzeni. Jeden z nich, dość znany na całym świecie, to tzw. OBIEG NATO (NATO Computer Incident Response). W 2014 r. prezydent USA Barack Obama wezwał Kongres do przyjęcia ustawy, która zmusi firmy do powiadamiania klientów, jeśli w ataku hakerskim zostaną skradzione ich dane osobowe. Można przypuszczać, jak podaje Onet [*Hakerzy…*, 2015], że jest to propozycja, która wynika z cyberataku na Sony Pictures, za którym – jak podejrzewa rząd USA – stała Korea Północna, oraz ataków na sieci handlowe Target i Home Depot w 2015 r., w których wykradziono dane o kartach kredytowych milionów Amerykanów.

Cybernetyczni napastnicy mają do wyboru wiele narzędzi ataku. W ich arsenałach są tysiące różnego rodzaju złośliwego oprogramowania, malware (*malicious software*), czyli wszelkie aplikacje, skrypty itp. mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera (w tym między innymi: wirusy, robaki, trojany, programy szpiegujące, keyloggery). Mogą też użyć mechanizmu *Distributed Denial of Service* (DDoS), który został zastosowany w ataku na Estonię[1]. Groźba ataku DDoS bywa czasami używana do szantażowania firm, np. serwisów aukcyjnych, firm brokerskich i podobnych, gdzie przerwa w działaniu systemu

[1] DDoS (*Distributed Denial of Service* – rozproszona odmowa usługi) – atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania przez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów (np. zombie). Do przeprowadzenia ataku służą najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania (różnego rodzaju tzw. robaki i trojany). Na dany sygnał komputery jednocześnie zaczynają atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług, jakie oferuje. Dla każdego takiego wywołania atakowany komputer musi przydzielić pewne zasoby (pamięć, czas procesora, pasmo sieciowe), co przy bardzo dużej liczbie żądań prowadzi do wyczerpania dostępnych zasobów, a w efekcie – do przerwy w działaniu lub nawet zawieszenia systemu.

transakcyjnego przekłada się na bezpośrednie straty finansowe firmy i jej klientów. W takich przypadkach osoby stojące za atakiem żądają okupu za odstąpienie od ataku lub jego przerwanie. Szantaż taki jest przestępstwem. Szczególnie niebezpieczne są ataki osób z wewnątrz. Osoba taka może przeprowadzić atak cyberterrorystyczny, aby się zemścić na instytucji, dla której pracuje lub pracowała, na rozkaz swoich mocodawców. Dla strony szykującej atak cybernetyczny posiadanie takiej osoby w szeregach przeciwnika jest warte więcej niż brygada wojsk pancernych. Jej działalność znacznie zwiększa zdolność do strategicznego uderzenia cybernetycznego.

Liczba ataków cybernetycznych na systemy komputerowe obsługujące sieci infrastruktury w USA wzrosła od 2009 r. niemal 17-krotnie – poinformowała amerykańska Agencja Bezpieczeństwa Narodowego (NSA), która po raz pierwszy opublikowała dane na ten temat.

Jak stwierdza G.J. Ratrray [2006]: „Im bardziej określone państwo jest uzależnione od swoich infrastruktur informacyjnych, w tym większym stopniu infrastruktury te stają się środkami ciężkości wartymi atakowania i obrony". Departament Obrony USA już w 1999 r. uznał, że „naród będący obiektem ataku na sieci komputerowe, finansowanego przez inne państwo, może legalnie odpłacić się tym samym, a w szczególnych przypadkach usprawiedliwiona może być obrona własna przy użyciu tradycyjnych środków wojskowych". G.J. Ratrray postuluje, aby w prawie międzynarodowym uregulować kwestię cyberwojny i uznać ją za akt agresji usprawiedliwiający użycie do obrony wszelkich dostępnych środków.

Zmienia się świat, a wraz z nim zmienia się działanie największej plagi XXI w., jaką jest terroryzm. To nie brodaty anarchista z bombą, ale wykształcony/a, siedzący/a przy komputerze osoba potrafi wywołać panikę i przerażenie świata.

W 2013 r. szef amerykańskiej Agencji Bezpieczeństwa Narodowego wyraził zaniepokojenie rosnącą liczbą zagranicznych cybernetycznych ataków wymierzonych w „krytyczną infrastrukturę" oraz brakiem dostatecznego przygotowania Stanów Zjednoczonych na takie działania. Stopień przygotowania kraju ocenił na „około 3" w skali od 1 do 10 [Forbes, 2012].

Polska wielokrotnie była obiektem cyberataków. W dniach od 30 listopada do ok. 3 grudnia 2006 r. miał miejsce atak na portal Gazeta.pl. Innym głośnym celem ataków DDoS stał się w maju 2007 r. serwis policja.pl. Według przypuszczeń miał to być odwet za policyjny nalot na jeden z serwisów udostępniających napisy do filmów w internecie. W połowie września 2009 r. ABW udaremniła zorganizowany atak na kilka polskich serwerów rządowych, który pochodził prawdopodobnie ze Wschodu. Sprawa była na tyle poważna, że w Departamencie Bezpieczeństwa Teleinformatycznego ABW powołano Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. Na bieżąco zbiera on i analizuje informacje o atakach i zagrożeniach. Jednym z zadań CERT-u jest nadzór nad systemem wczesnego ostrzegania o incydentach sieciowych ARAKIS-GOV. Dodatkowo CERT prowadzi rutynową akcję monitorowania bezpieczeństwa rządowych witryn internetowych [Pietryga, 2009].

W związku z planowanym podpisaniem przez Polskę porozumienia ACTA 21 stycznia 2012 r. ok. godziny 19:00 rozpoczął się szereg ataków na strony polskich instytucji parlamentarnych i rządowych. Do ataku przyznała się grupa Anonymous. To, czy pierwsze problemy (przestała działać strona Sejmu) były wynikiem DDoS, nie jest do końca jasne. W prasie pojawiły się też opinie, że była to zwykła usterka techniczna niezwiązana z działalnością hakerów. Po ich wystąpieniu w sieci zaczęły krążyć niepotwierdzone informacje, co mogło wywołać efekt ataku DDoS w sposób naturalny (duża liczba internautów sprawdzających, czy strona rzeczywiście nie działa). Rzecznik rządu podał, że przyczyną późniejszych problemów mogło być duże zainteresowanie treścią porozumienia, które zostało zamieszczone na serwerach ministerstwa w pliku pdf. o wielkości ponad 20 MB, zawierającym zeskanowany oryginał dokumentu. Później jednak przestały działać witryny innych ministerstw i instytucji rządowych, czego najbardziej prawdopodobną przyczyną jest właśnie atak DDoS. Przemawia za tym również fakt, że wkrótce po tym, jak rzecznik rządu Paweł Graś zaprzeczył doniesieniom na temat ataku hakerskiego, przestała działać jego strona www. W styczniu 2015 r. hakerzy zablokowali stronę internetową Salezjańskiego Wolontariatu Misyjnego. Współpracownicy salezjan wskazywali, że prawdopodobnie przyczyną wyboru przez Państwo Islamskie zakonników z tego wolontariatu jest ich działalność promująca chrześcijańskich męczenników. Są oni producentem serialu o aktach męczeństwa na Wschodzie, uchodźcach z Syrii, prześladowaniach chrześcijan we Francji. Gdy planowali wyemitować odcinek o prześladowaniach w Iraku, ich strona została „zhakowana". Mówiono wówczas o pierwszym w Polsce przypadku cyberterroryzmu islamskiego.

W 2015 r. między innymi hakerzy z Państwa Islamskiego zaatakowali stronę małopolskiej firmy Michalus. „Jesteśmy wszędzie" – napisali na głównej stronie firmy. Właściciele zastanawiają się, dlaczego to właśnie oni znaleźli się na celowniku. Do ataku doszło w drugiej połowie marca, ale szczegóły firma ujawniła dopiero teraz. „Zostaliście zhakowani przez Państwo Islamskie. Jesteśmy wszędzie" – taki podpis, umieszczony pod flagą Państwa Islamskiego (sztandaru sławiącego Allaha), pojawił się na stronie internetowej tej firmy przewozowej.

W styczniu 2015 r. grupa hakerów, która przedstawia się jako CyberKalifat, ostrzegła, że zdążyli już przeniknąć „do każdego komputera, w każdej bazie wojsk USA". Według informacji amerykańskich mediów armia USA potwierdziła, że konto USCENTCOM zostało przejęte.

3. Rewolucja informacyjna i jej społeczne reperkusje w budowie systemu zabezpieczenia kraju

W nowym społeczeństwie na plan pierwszy wysuwa się informacja. Człowiek staje się wolny, ponieważ posiada informacje i wiedzę. Rewolucja informacyjna, w którą wchodzi rozwinięty świat, stwarza niezwykłe szanse dla jednostki i społe-

czeństwa [Zacher, 2007]. Wynika to z faktu, iż zwiększając znacząco możliwości przekazu informacji, stwarza się całkowicie nowe warunki dla komunikowania się i współdziałania. Obdarzeni ogromną wyobraźnią futurolodzy H. i A. Toffler [1997] piszą o konieczności rozwiązania różnorodnych problemów, takich jak elektroniczna autostrada, powstanie monopoli informacyjnych, totalna wojna informacyjna.

Według L. Groffa [1997] „cały świat – w różny sposób i różnymi sposobami – ulega restrukturyzacji oraz wpływowi rewolucji informacyjnej". Polska również ulega tym przekształceniom. Jako nowy członek Unii Europejskiej dążymy do zacieśnienia współpracy gospodarczej, kulturalnej i turystycznej z krajami starej Unii Europejskiej, musimy jak najszybciej przystąpić do budowy wspólnej przestrzeni informacyjnej. Przestrzeń informacyjna obejmuje między innymi bazy: danych, wiedzy, modeli, obrazów, dźwięku, wraz z odpowiednim oprogramowaniem i środkami technicznymi, które umożliwiają użytkownikom korzystanie z tych zasobów w sposób bezpieczny i zgodny z przeznaczeniem. Dla osiągnięcia tych celów musimy wydatkować odpowiednie kwoty na technologię informacyjną.

Jak wielkie powinny być te kwoty? Na pewno powinny proporcjonalnie odpowiadać kwotom wydatkowym w tych krajach, których poziom życia pragniemy osiągnąć. W krajach rozwiniętych gospodarczo nakłady na infrastrukturę zarządzania są w większości pokrywane przez prywatnych przedsiębiorców. Jednak to od państwa zależy, czy dla tego celu zostaną stworzone odpowiednie warunki makroekonomiczne. Wydaje się, iż polityka gospodarcza w Polsce nie jest skoordynowana z działaniami zarówno Unii Europejskiej, jak i naszych bezpośrednich sąsiadów. Przeprowadzone badania pod kierunkiem W. Cellarego [2002] wykazały, że Polska jest w grupie krajów o najniższym poziomie informatycznej infrastruktury. Sytuacja się nie poprawiła, wręcz przeciwnie. Jak pisze się w „Gazecie Wyborczej": „Polska to technologiczny zaścianek Europy" [„Gazeta Wyborcza", 09.04.2008]. Według Global Information Technology [2015] Polska w 2014 r. była na 43. pozycji, zaraz za Litwą i Łotwą, a daleko w tyle za Republiką Czeską. Natomiast jeżeli wziąć pod uwagę samo wykorzystanie ICT w administracji państwowej i samorządowej, to jesteśmy na 103. miejscu wśród wszystkich 130 ujętych w raporcie państw. Z analizy zamieszczonych w opracowaniach danych statystycznych European Information Technology Observatory (roczniki 2000–2014) wynika, że mimo iż dynamika wydatków na ICT w Polsce i krajach byłego bloku RWPG jest wysoka, to jednak bezwzględna ich wysokość jest o wiele niższa niż w rozwiniętych krajach Unii Europejskiej. I tak, mimo że w Polsce w ciągu ostatnich 10 lat wydatkowano znaczne środki na ICT, jest to o wiele mniej niż w większości krajów Unii Europejskiej. Polska należy w Europie do krajów najbardziej opóźnionych w zakresie wydatków na infrastrukturę zarządzania.

Konsekwencją posiadania przestarzałej infrastruktury zarządzania jest powstanie nowego typu barier związanych z brakiem informacji o możliwościach rozwoju poszczególnych branż i przedsiębiorstw. Efekty negatywne takiej informacyjnej bariery to między innymi spadek konkurencyjności firm polskich w stosunku do

firm pochodzących z tych krajów, które taką nowoczesną infrastrukturę posiadają. Problematyka ta jest przedmiotem obrad między innymi w Information Society Forum (ISF). Forum to zostało powołane w 1995 r. jako niezależne ciało doradcze Komisji Europejskiej, a jego zadaniem jest wyciąganie wniosków i formułowanie zaleceń dla wszystkich instytucji europejskich. Według prac Komisji i opracowanego przez nią raportu wydatki na ICT są niezbędne dla realizacji Europejskiej Drogi do Społeczeństwa Informacyjnego. Europejska Droga to stawianie na silny rynek, nieustanną innowacyjność oraz wolny przepływ informacji i wiedzy jako pochodną przepływu kapitału i siły roboczej. Wolne przepływy informacji to również pole do manipulacji i nadużyć.

Tworzenie przestrzeni informacyjnej jako podstawowego elementu gospodarki informacyjnej wymaga przeznaczenia dość znacznych środków na budowę bezpiecznej infrastruktury zarządzania, a więc na technologię informacyjną.

W warunkach Polski możliwości, jakie niesie ze sobą zastosowanie ICT są dużą szansą dla rozwoju przedsiębiorczości i przyspieszenia procesu gospodarczej integracji krajów Unii Europejskiej. Globalne strategie organizacji mogą być w pełniejszy i łatwiejszy sposób realizowane dzięki gospodarce elektronicznej. Polska i inne kraje Europy Środkowo-Wschodniej, korzystając z gospodarki elektronicznej, mają większe możliwości stania się konkurencyjnymi i kreatywnymi niż w przypadku tradycyjnej gospodarki rynkowej. Powstanie gospodarki elektronicznej jest wynikiem rozwoju informacyjnej technologii. Dzięki gospodarce elektronicznej organizacje pochodzące z krajów Europy Środkowo-Wschodniej mają możliwość funkcjonowania zarówno w wymiarze lokalnym, jak i globalnym. Rozwój gospodarki elektronicznej to szansa wzrostu konkurencyjności tak małych, jak i dużych organizacji na rynku globalnym.

Jednak czy takie organizacje nie będą bardziej wystawione na atak terrorystyczny? Szansa taka nie jest związana z lokalizacją organizacji. Obok szans pojawiają się też nowe zagrożenia. Jak stwierdza G. Yip [2006], „umiejętność opracowania i realizacja strategii globalnej jest prawdziwym testem sprawności zarządzania organizacją". Na całym świecie poszczególne organizacje dążą w stronę globalizacji rozumianej jako ekspansja na rynki zagraniczne. Problematyka ta jest tym bardziej aktualna, że niezależnie od tego, czy poszczególne osoby chcą globalizacji czy też są jej przeciwne, jest to naturalna droga rozwoju niemal wszystkich działów i gałęzi gospodarki narodowej.

4. Cyberterroryzm jako zagrożenie budowy społeczeństwa informacyjnego

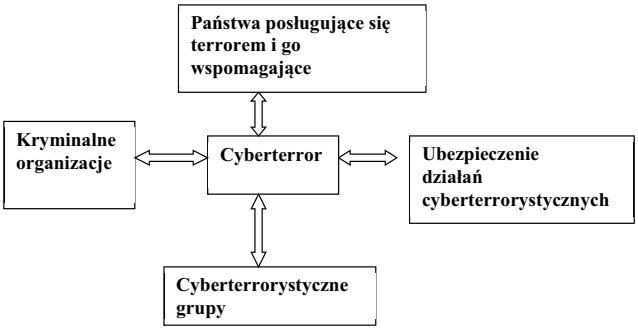
Jak już wspomniano, budowa społeczeństwa informacyjnego niesie różnego rodzaju niebezpieczeństwa. Ze względu na ograniczoną objętość artykułu skoncentrowano się na analizie cyberterroryzmu. Jest on bardzo silnie związany z rozwojem ICT w kontekście budowy społeczeństwa informacyjnego. Powstanie cyberterrory-

zmu łączy się z kluczowymi zagrożeniami bezpieczeństwa państwa i jego obywateli. Analizując tzw. piramidę potrzeb Maslowa, widzimy, że dla ludzi – zaraz po zaspokojeniu potrzeb fizjologicznych – najważniejsze jest zaspokojenie potrzeb obronnych.

Dzięki rozwojowi ICT z terroryzmu powstał cyberterroryzm. Według eksperta w dziedzinie bezpieczeństwa cyberprzestrzeni i nowych technologii na Uniwersytecie Georgetown w Waszyngtonie, D.E. Denninga [2002], „Cyberterroryzm jest konwergencją cyberprzestrzeni i terroryzmu. Dotyczy nielegalnych ataków i gróźb ataków przeciwko komputerom, sieciom komputerowym i informacjom przechowywanym w nich, by zastraszyć lub wymusić na rządzie lub społeczeństwie polityczne lub społeczne cele. Zakwalifikowanie ataku jako cyberterroryzm powinno wynikać z faktu zastosowania przemocy przeciwko ludziom lub ich mieniu". Cyberterroryzm wywołuje strach. W Wikipedii pod tym hasłem można znaleźć następujące stwierdzenie: „Cyberterroryzm – spotykane w mediach oraz literaturze określenie opisujące posługiwanie się zdobyczami technologii informacyjnej w celu wyrządzenia szkody z pobudek politycznych lub ideologicznych, zwłaszcza w odniesieniu do infrastruktury o istotnym znaczeniu dla gospodarki lub obronności atakowanego kraju. W szerszym, ogólnym znaczeniu jest to terroryzm". A. Bógdał-Brzezińska i M.F. Gawrycki [Bógdał-Brzezińska, Gawrycki, 2003; Bógdał-Brzezińska, 2007; Gawrycki, 2006] piszą, że cyberterroryzm jest najbardziej nieprzewidywalnym sposobem oddziaływania zorganizowanych grup na funkcjonowanie i stabilność struktur państwowych. Systemy te, określane jako SCADA (*Supervisory Control and Data Aquisition*) – jak piszą L. Janczewski i A. Colarik [Janczewski, Colarik, 2007; Colarik, Janczewski, 2011; Colarik, 2006] – są znakomitym celem ataków cybeterrorystów ze względu na rolę, jaką pełnią, ale nie tylko dlatego. Systemy SCADA są pochodną automatycznych systemów sterowania obiektami przemysłowymi. Dawniej, w erze przedinformatycznej, fizyczny dostęp do sterowania obiektami przemysłowymi był utrudniony. Wysiłek konstruktorów był ukierunkowany głównie na ich niezawodne działanie. Zastosowanie komputerów i telekomunikacji spowodowało, że funkcje sterownicze są realizowane zdalnie z wykorzystaniem ogólnodostępnych łączy i komputerów. Nie opracowano do tej pory właściwego zabezpieczenia systemów SCADA od zagrożeń zewnętrznych (np. hakerów) i to stanowi ich zasadniczą wadę. Dla cyberterrorystów jest to łatwy cel do likwidacji.

K. Kumalski (2006) zwraca uwagę na fakt, że wielu ludzi nie widzi różnicy pomiędzy terroryzmem lub cyberterroryzmem a innymi formami zbrodni. Tymczasem różnica jest ogromna. Powoduje on bowiem reperkusje psychologiczne w społeczeństwie. Przy pomocy rozgłosu zdobytego w wyniku przemocy terroryści dążą do zdobycia wpływów i władzy. Jest to akt kryminalny, ale jego skutki najczęściej znacznie wykraczają poza granice klasycznego przestępstwa kryminalnego. Posługując się typologią podaną przez T. Mockatisa [2008], możemy głównych aktorów działań cyberterrorystycznych przedstawić jak na rys. 2.

Wiele krajów powołało specjalne ośrodki zajmujące się ochroną systemów krytycznych (np. USA, Anglia, Australia, Norwegia, Nowa Zelandia). Ośrodki te nie



Rys. 2. Aktorzy działalności terrorystycznej

Źródło: [Mockatis, 2008].

tylko są aktywne wewnątrz krajów, w jakich działają, ale też bardzo ściśle ze sobą współpracują. Na przykład w marcu 2008 r. miały miejsce międzynarodowe ćwiczenia obejmujące wyżej wymienione kraje i mające na celu zbadanie wspólnych zdolności tych krajów do zwalczania ataków ukierunkowanych na systemy krytyczne. Ćwiczenia te nie są typu „sztuka dla sztuki". Przykładem rzeczywistych zagrożeń mogą być wspomniane wcześniej wydarzenia z Estonii z maja 2007 r. W wyniku konfliktowej decyzji władz estońskich (przesunięcia pomnika upamiętniającego żołnierzy radzieckich poległych na tych terenach w czasie II wojny światowej) nastąpił zmasowany atak cybernetyczny na sieć informatyczną tego kraju. Wiele centralnych urzędów Estonii, wliczając ministerstwa i bank centralny, było odciętych od świata przez wiele godzin. Atak ten był przeprowadzony spoza granic Estonii przez elementy pro-rosyjskie, przeciwne rządowi tego państwa. W wyniku tych wydarzeń na terenie Estonii powołano ośrodek NATO-wski zajmujący się cyberterroryzmem i wojnami cybernetycznymi.

Terroryści z Al-Kaidy w wydanym oświadczeniu wzięli odpowiedzialność za działania podjęte w 2003 r., w konsekwencji których nastąpiła przerwa w dostawie zasilania w północnych częściach Stanów Zjednoczonych i południowych Kanady (władze amerykańskie zaprzeczają udziałowi Al-Kaidy w tych zakłóceniach), a także za dokonaną w tym samym roku (nieskuteczną zresztą) „elektryczną blokadę Wielkiej Brytanii". Jak uspokajają w internecie takie organizacje, jak CIA i FBI, infrastruktura obronna Stanów Zjednoczonych (broń atomowa i inne systemy wojskowe, a także systemy informatyczne FBI i CIA) są izolowane od internetu, co czyni je niedostępnymi dla działających „z zewnątrz" hakerów czy cyberterrorystów. Działania hakerów lub innych osób posługujących się tzw. narzędziami szpiegującymi mają na celu przygotowanie ataku cyberterrorystycznego. Te uzasadnienia są dosyć wątpliwego znaczenia, ponieważ statystyka ataków na systemy informacyjne pokazuje, że praktycznie połowa z nich jest inicjowana wewnętrznie [Janczewski, Colarik, 2007]. Warto dodać, że wiele „tradycyjnych" konfliktów ma swoje odpowiedniki cybernetyczne, między innymi w czasie nasilenia konfliktów (takich jak palestyński, indyjsko-pakistański, bałkański) odnotowuje się nasilenie ataków cybernetycznych (z obu stron).

O czyhającym na nas niebezpieczeństwie napisano wiele powieści, pojawiło się wiele filmów. Mimo przytoczonych faktów nasuwa się pytanie, czy osoby wskazujące na cyberterroryzm jako realne zagrożenie dla bezpieczeństwa narodowego i międzynarodowego, wkładają tylko swoją cegiełkę do „histerii terrorystycznej", jaka ma miejsce po 11 września 2001 r.? A może jednak cyberterroryzm w niedługim czasie ma szansę stać się jednym z największych wyzwań współczesnego świata? Pytania te możemy postawić każdemu członkowi społeczności. Zabezpieczenie przed takim rodzajem ataku jest bardzo kosztowne i ogranicza naszą „wolność" w budowie społeczeństwa informacyjnego. Jednak bardzo często jest ono konieczne.

Wynika to z faktu, iż w przypadku takiego ataku skutki mogą mieć niewyobrażalne konsekwencje. Od 11 września 2001 r. wszyscy żyjemy w obawie następnych ataków. I nie buntujemy się, jak musimy zdejmować buty przed bramkami kontroli na lotnisku. Obawiamy się „Fatwe", czyli wypowiedzenia świętej wojny przez zwolenników Osamy bin Ladena. Ekstremiści, nie tylko muzułmańscy, są rozproszeni po niemal całym świecie, a ich przesłania to zachęcanie do przyłączenia się do wspólnej walki. Internet może być efektywną drogą do realizacji tych celów. Dzięki sieci ekstremiści mają dostęp z dowolnego punktu na świecie. Takie możliwości są przez nich wykorzystywane do szybkiego przesyłania nieograniczonej ilości tekstów propagandowych. Internet pomaga im się jednoczyć i motywować wzajemnie.

Sprawa nie jest taka prosta. B. Schneier opublikował w 2007 r. artykuł, którego myślą przewodnią było to, że uczucie zagrożenia bardzo często nie jest związane z rzeczywistym zagrożeniem. Jak to napisano powyżej, transport lotniczy wydał wiele miliardów dolarów na ochronę pasażerów. Nastąpiło to w wyniku śmierci ok. 3000 ludzi w wypadkach lotniczych w ostatnim 10-leciu. Z drugiej strony od zatruć żywnością umiera rocznie w USA około 5000 ludzi, ale roczne wydatki agencji zajmującej się tymi sprawami liczy się w dziesiątkach milionów dolarów, a nie w miliardach, jak to jest w przypadkach zapobiegania katastrofom lotniczym. Uczucie zagrożenia jest złym motywem działania. Dodatkowo dużą negatywną rolę spełniają mass media nagłaśniające jakiekolwiek działania terrorystyczne. Terroryzm jest zbudowany na działaniach mających wywołać przerażenie wśród ludzi. Doniesienia prasowe oraz telewizyjne, pokazujące rezultaty działań ekstremistów, stanowią znakomite paliwo do podsycania tego uczucia. Informatyczna infrastruktura tworzona w budowie społeczeństwa informacyjnego nie jest uodporniona na ataki z zewnątrz. W konsekwencji cyberterrorysta ma szansę dostępu do wybranego celu z dowolnego punktu na ziemi czy też z przestrzeni. Charakteryzując zagrożenia cyberterrorystyczne, należy zwrócić uwagę na sieciową organizację działań i bezterytorialność.

Zależność społeczeństwa od ICT stworzyła nowy rodzaj zagrożenia, którego świadomość zwróciła uwagę mass mediów, naukowców i informatyków. W warunkach Polski zagadnienie zabezpieczeń jest tym bardziej trudne, że informatyczna kultura w społeczeństwie nie jest zbyt wysoka.

Istnieje wiele publikacji przestrzegających społeczeństwo przed cyberterroryzmem i zwracających uwagę na konieczność podejmowania działań ochronnych.

I tak w jednym z nich cyberterrorystyczny atak na system komputerowy kontrolujący elektrownię prowadzi do katastrofy skażenia radioaktywnego, a w efekcie – do śmierci wielu niewinnych ludzi. W innym scenariuszu cyberterroryści włamują się do systemu kierowania przestrzenią powietrzną i powodują kolizję cywilnych samolotów. Powstaje więc pytanie, czy zagrożenie przestrzeni cybernetycznej działalnością cyberterrorystów czy też cyberwojskowych jest realne czy też nie? Naszym zdaniem sytuacja jest prawie identyczna z pojawieniem się słynnego wirusa Y2K Bug. Wirus ten pojawił się na przełomie 1999 i 2000 r. Zagrożenie było realne w skali światowej i wiele wysiłków zostało dokonanych, by nie uaktywnił się on na szerszą skalę. I rzeczywiście, z wybiciem zegara Nowego Millenium można było stwierdzić: „Polacy, nic się nie stało". Niektórzy nawet odczuwali zawód z tego powodu, np. pewni obywatele USA, którzy w przewidywaniu chaosu socjalnego z tego powodu kupowali żywność (i oczywiście broń) i wypełniali nią zaparkowane przed ich domami kontenery. Nie ulega wątpliwości, że bez tych środków zapobiegawczych nie odnotowano by większych zakłóceń. Podobne zagrożenie istnieje ze strony ataków cyberterrorystów, ponieważ ich działania mogą mieć szeroki zasięg, jeżeli nie podejmie się środków zapobiegawczych. Są już one coraz częściej podejmowane w skali światowej i prawdopodobieństwo skutecznych ataków cyberterrorystów nie rośnie.

W wielu scenariuszach filmowych cyberterroryści włamują się do systemu bankowego i kontrolują międzynarodowe transakcje finansowe i giełdy papierów wartościowych. System ekonomiczny załamuje się, społeczeństwo traci zaufanie do państwa i cel cyberterrorystów, jakim jest destabilizacja państwa, zostaje osiągnięty.

Zagrożenie cyberterroryzmem wielu ludziom może się wydawać wyolbrzymione i w ich opinii może nie opłaca się wydatkować środki na walkę z nim. Pragniemy jednak zwrócić uwagę, że nie powinniśmy jego istnieniu zaprzeczać czy go ignorować. Nie możemy być uśpieni tym, że do tej pory nie było żadnych większych wojen cybernetycznych między narodami, ponieważ widzieliśmy wiele przypadków, które zawierały niemal wszystkie składniki takiej formy konfliktu.

R. Clarke i R. Knake w swojej książce [2012] zaproponowali następującą liczbę zagadnień związanych ze strategicznymi aspektami cyberwojny: odstraszanie, prawo do pierwszego użycia, preparaty bitwy. Można zauważyć, że kwestie te są typowe dla każdej postaci konfliktu. W opinii autora jednym z najważniejszych elementów planów wojskowych jest odstraszanie. Jeśli jest to działanie skuteczne, to można będzie uniknąć dalszych konfliktów.

Podsumowanie

Odpowiedź na podstawowe pytanie, czy musimy się obawiać globalnej cyberwojny – jest trudna i odpowiedzialna. Optymistyczne stanowisko wynika z faktu, że prawdopodobieństwo poważnego konfliktu światowego z wykorzystaniem ICT jest w chwili obecnej bardzo niskie. Czy rzeczywiście tak jest? Analiza czynników,

które należy brać pod uwagę w analizie prawdopodobieństwa wybuchu cyberwojny pokazuje, że czynnikami, które zwiększają prawdopodobieństwo światowego cyberkonfliktu i cyberwojny są:

1. Uzależnienie od informacji. Informacje dotyczą wszystkich aspektów naszego życia. W tych państwach, które mają wysoki stopień rozwoju, mieszkańcy nie mogą żyć bez ICT. W konsekwencji atak na infrastrukturę informacyjną zarządzania może skutecznie sparaliżować kraj.
2. Cyberwojna jest konfliktem, w którym strona atakująca może nie ponieść strat materialnych (to nie jest wojna nuklearna). Cyberataki są zazwyczaj o wiele mniej kosztowne niż tradycyjne działania wojskowe.
3. ICT rozwija się bardzo szybko i praktycznie wszystkie duże organizacje są z nim związane. Dostęp do informacji wewnętrznych może być ograniczony, ale hakerzy nie mają najmniejszych problemów z pokonaniem stosowanych zabezpieczeń.
4. Zawsze znajdą się takie siły, które zechcą, nie patrząc na koszty, wygrać konflikt.

Istnieją czynniki, które zmniejszają prawdopodobieństwo takiej wojny [por. Janczewski, 2015]. Konflikty zbrojne w przeszłości były prowadzone na podstawie niewystarczającej ilości informacji na temat planów wroga. Obecnie wszystkie główne mocarstwa dzięki systemom „szpiegującym" wspieranym przez ICT mają dość szczegółowe informacje o swoich przeciwnikach. Zaskakujący atak jest bardzo trudny do przeprowadzenia. W ciągu ostatnich dziesięcioleci handel międzynarodowy rośnie w zawrotnym tempie. Pomimo znacznych różnic ideologicznych mocarstwa uczestniczą w międzynarodowym handlu. Oznacza to, że konflikt z takim państwem, który jest dostawcą kluczowych elementów do gospodarki, nie znajduje się na liście priorytetów politycznych potęg światowych. Konflikt na Ukrainie jest najlepszym przykładem tego problemu. Zarówno Unia Europejska, jak i Rosja wyraźnie ograniczają uruchomienie głównych działań wojskowych i ekonomicznych wobec drugiej strony z powodów gospodarczych.

Jak przedstawiono w artykule, jesteśmy świadkami wielu lokalnych cyberkonfliktów. Wybuchają one zazwyczaj w krajach mniej rozwiniętych, jednak i one mogą być źródłem cyberzagrożeń. Do przeprowadzenia cyberataku nie są wymagane duże środki. Cyberwojna nie wymaga tysięcy okrętów, samolotów i rakiet. Należy również mieć na uwadze fakt, że większość konfliktów jest wywoływana przez różnego typu fanatyków (Nowy York[2], Londyn[3], Madryt[4]).

Na podstawie dostępnych materiałów przypuszczamy, że w najbliższej przyszłości nie będzie „czystej" globalnej cyberwojny, lecz działania cyberterrorystyczne

[2] Zamach z 11 września 2001 r. – seria czterech ataków terrorystycznych przeprowadzonych rano we wtorek 11 września 2001 r. na terytorium Stanów Zjednoczonych za pomocą uprowadzonych samolotów pasażerskich.

[3] Trzy eksplozje w metrze i jedna eksplozja w miejskim autobusie sparaliżowały 7 lipca 2005 r. w porannych godzinach szczytu centrum Londynu w Wielkiej Brytanii.

[4] Zamach w Madrycie 11 marca 2004 r. – seria ataków terrorystycznych na pociągi w Madrycie.

będą wspomagały działania destrukcyjne w czasie różnego rodzaju konfliktów. Nie można w związku z tym wykluczać, iż w najbliższym czasie możemy jako kraj brać udział w takich hybrydowych działaniach wojennych.

Budowa społeczeństwa informacyjnego jest faktem. Polska musi wejść do tego „pociągu", jeżeli ma ambicje bycia liczącym się krajem w Unii Europejskiej. Innych dróg nie ma dla stania się państwem nowoczesnym. Musimy zdawać sobie jednak sprawę z konieczności poniesienia znacznych nakładów na realizację polityki „Bezpieczna Polska". Konieczny kierunek działań to praca nad wzrostem kultury informatycznej społeczeństwa i praca od podstaw nad przeprowadzeniem zmian w mentalności dość dużej grupy naszych obywateli. Polska w zakresie ICT nie należy do liderów i bez nowoczesnej infrastruktury informatycznej na pewno będziemy pomijani przez zagranicznych inwestorów. Wraz z naszym uzależnieniem się od ICT należy zdawać sobie sprawę z pojawiających się nowych zagrożeń. Jednym z najbardziej istotnych jest cyberterroryzm w różnych postaciach. Przeznaczając coraz większe środki na ICT i tworzenie społeczeństwa informacyjnego, winniśmy również pamiętać o przeznaczeniu części dysponowanych środków na działania antycyberterrorystyczne.

Bibliografia

Bartoszek B., *Cyberwojna – wojna XXI wieku*, 2008, www.mojeopinie.pl/cyberwojna_wojna_xxi_wieku,3,1215862210 [data dostępu: 10.02.2015].

Bógdał-Brzezińska A., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Fundacja Studiów Międzynarodowych, Oficyna Wydawnicza ASPRA-JR, Warszawa 2007.

Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Fundacja Studiów Międzynarodowych, Oficyna Wydawnicza ASPRA-JR, Warszawa 2003.

Cellary W. (red.), *Polska w drodze do globalnego społeczeństwa informacyjnego*, UNDP, Warszawa 2002.

Clarke R.A., Knake R., *Cyber War: the Next Threat to National Security and What to Do about it Paperback*, HarperCollins Pub. 2012.

Colarik A., *Cyber Terrorism: Political and Economic Implications*, Idea Group, 2006, **DOI: http://dx.doi.org/10.4018/978-1-59904-021-9**.

Colarik A., Janczewski L., *Developing a Grand Strategy for Cyber War. Proceedings of the 7th International Conference on Information Assurance and Security, IAS2011*, Melaka, Malaysia, 5–8 December 2011, **DOI: http://dx.doi.org/10.1109/isias.2011.6122794**.

Defensy24, *Ćwiczebna cyberwojna między USA a Wielką Brytanią*, 2015, www.defence24.pl/news_cwiczebna-cyberwojna-miedzy-usa-a-wielka-brytania [data dostępu: 10.02.2015].

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

Forbes, *Coraz więcej cyberataków na infrastrukturę w USA*, 2012, www.forbes.pl/artykuly/sekcje/Wydarzenia/coraz-wiecej-cyberatakow-na-infrastrukture-w-usa,29113,1 [data dostępu: 10.05.2015].

Gawrycki M.F., *Globalizacja w służbie antyglobalistów – „zapatyści" i rewolucja informacyjna*, [w:] I. Łęcka (red.), *Społeczne skutki globalizacji – globalizacja a bezpieczeństwo i zdrowie publiczne*, Wydawnictwa Uniwersytetu Warszawskiego, Warszawa 2006.

„Gazeta Wyborcza", 09.04.2008.

Global Information Technology (The Global Competitiveness Index 2014–2015 Rankings), www3.weforum.org/docs/WEFUSA_DigitalInfrastructure_Report2015.pdf, 2015 [data dostępu: 10.02.2015].

Groff L., *Rewolucja informacyjna, globalne trendy restrukturyzacyjne, wizje i decyzje*, „Transformacje" 1997, nr 3–4.

Hakerzy z Państwa Islamskiego przejęli konto na Twitterze należące do dowództwa armii USA, 2015, http://wiadomosci.onet.pl/swiat/hakerzy-z-panstwa-islamskiego-przejeli-konto-na-twitterze-nalezace-do-dowodztwa-armii/93xg2 [data dostępu: 10.05.2015].

Howard A., *White House Launches New Digital Government Strategy*, O'Reilly Radar, May 2012, http://radar.oreilly.com/2012/05/white-house-launches-new-digit.html [data dostępu: 10.09.2014].

Janczewski L., *3rd World War: Cyber War?*, [w:] W. Chmielarz, J. Kisielnicki, T. Parys (red.), *Informatyka 2 przyszłości*, Wydawnictwo Naukowe WZ UW, Warszawa 2015.

Janczewski L., Colarik A., *Cyber Warfare and Cyber Terrorism*, "Information Science Reference" 2007, **DOI: http://dx.doi.org/10.4018/978-1-59140-991-5**.

Kisielnicki J., *Zarzadzanie*, PWE, Warszawa 2014a.

Kisielnicki, J., *Zarządzanie i informatyka*, Placet, Warszawa 2014b.

Kumalski K., *Problemy definicyjne pojęcia terroryzmu*, 2006, www.psz.pl/124-polityka/karol-kumalski--problemy-definicyjne-pojecia-terroryzm [data dostępu: 10.02.2015].

MailOnline, *"Make a bomb in the kitchen of your Mom": Al Qaeda launches its first online magazine in English*, 2010, www.dailymail.co.uk/news/article-1291143/Al-Qaeda-launches-Inspire-online-magazine-English.html#ixzz3WF9GFi4b [data dostępu: 10.02.2015].

Mockatis T., *The New Terrorism: Myths and Realists*, Stanford University Press 2008.

Pietryga T., *Wrześniowy cyber atak na Polskę*, 2009, http://etarcza.pl/jezyk_pl/artykuly/2009-09-15%20cyberatak%20na%20Polsk%C4%99.pdf [data dostępu: 10.05.2015].

Ratrray G.R., *Wojna strategiczna w cyberprzestrzeni*, WNT, Warszawa 2006.

Schneier B., *The Psychology of Security – Draft*, "CRYPTO-GRAM" 2007, February 28.

Sienkiewicz P., *Wyzwania i zagrożenia w sieci: inwigilacja, dezinformacja, cyberterroryzm*, [w:] *Współczesne zagrożenia cyberterrorystyczne i bioterrorystyczne a bezpieczeństwo narodowe Polski*, Wydawnictwo WSP Szczytno, Warszawa – Dęblin 2015.

Toffler H., Toffler A., *Wojna i antywojna*, Warszawskie Wydawnictwo Literackie Muza, Warszawa 1997.

Yip G.S., *Strategia globalna – światowa przewaga konkurencyjna*, PWE, Warszawa 2006.

Zacher L.W., *Transformacje społeczeństw od informacji do wiedzy*, C.H. Beck, Warszawa 2007.

On the Other Site of the Power that is the Dark Side of Science

The article discusses the issues to take under consideration when dealing with information technology that may become threats. We draw special attention to the new threat of modern civilization, namely the cyberwar, as a hybrid form of war, and cyberterrorism. Poland, along with the progress of civilization and development of information management infrastructure is increasingly vulnerable to cyberattacks. Terrorist activity in cyberspace is particularly dangerous to people. The article was justified by the need to allocate adequate resources to combat this phenomenon. Attention was drawn to the fact that the era of information society and information systems can be both a weapon and a target.

Po drugiej strony mocy, czyli ciemne strony informatyki

Artykuł jest poświęcony problematyce spojrzenia na technologię informacyjną od strony zagrożeń. Szczególną uwagę pragniemy zwrócić na nowe zagrożenia współczesnej cywilizacji, jakimi są cyberwojny i cyberterroryzm. W opracowaniu przedstawiono formy wojny hybrydowej. Jedną z nich jest cyberwojna. Polska wraz z postępem cywilizacyjnym i rozwojem informatycznej infrastruktury zarządzania jest coraz bardziej narażona na ataki w cyberprzestrzeni. Szczególnie niebezpieczna dla społeczeństwa jest działal-

ność terrorystyczna w cyberprzestrzeni. W pracy uzasadniono konieczność przeznaczenia odpowiednich środków na walkę z tym zjawiskiem. Zwrócono też uwagę na fakt, że w erze społeczeństwa informacyjnego systemy informacyjne mogą być zarówno bronią, jak i celem ataku.