ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2015
Seria: ORGANIZACJA I ZARZĄDZANIE z. 85 Nr kol. 1943

Urszula SOLER
Katolicki Uniwersytet Lubelski Jana Pawła II
Wydział Nauk Społecznych
Instytut Socjologii

TECHNOLOGIE SIECIOWE VS. TERRORYZM – CZY MOGĄ BYĆ SPOŁECZNIE SZKODLIWE?

Streszczenie. Rewolucja technologiczna przyniosła zmiany we wszystkich sferach ludzkiego życia. Szczególnie są one widoczne w komunikacji. Technologie sieciowe (Internet, łączność satelitarna etc.) przyspieszyły rozwój komunikacji społecznej w niespotykany dotąd sposób. Ich ewaluacja nie jest jednak łatwa, gdyż z jednej strony dobrze służą one milionom ludzi w ich codziennym życiu, z drugiej jednak w analogiczny sposób dostęp do nich mają grupy społecznie szkodliwe, m.in. terroryści, pozwalając im na niezwykle niebezpieczne działania. Zatem, czy społeczna ocena technologii sieciowych jest jednoznaczna?

Słowa kluczowe: technologie sieciowe, nowoczesne technologie, terroryzm, społeczeństwo, wartościowanie technologii, technology assessment

NETWORK TECHNOLOGIES VS. TERRORISM – COULD THEY BE SOCIALLY HARMFUL?

Summary. The technological revolution brought changes in all spheres of human life. In particular, they are visible in communication. Network technologies (Internet, satellite communications, etc.) accelerated in an unprecedented way the development of social communication. However their evaluation is not simple, because on the one hand, they serve to millions of people in their daily lives, on the other, in the same way the access to them have also groups socially harmful – among others – terrorists. It allowed them to act in very dangerous way. Is their social assessment unequivocal?

Keywords: network technologies, modern technologies, terrorism, society, technology evaluation, technology assessment

Koniec XX wieku przyniósł ogromne zmiany technologiczne w wielu sferach ludzkiego życia. Niezwykle szybki rozwój nowych technologii wpłynął na rozwój przemysłu, sektora usług, ale przede wszystkim przyniósł niespotykane do tej pory zmiany w ludzkiej komunikacji. W ciągu jednego wieku szybkość komunikacji zwielokrotniła się do tego stopnia, że odległości przestrzenne przestały mieć jakiekolwiek znaczenie. W XXI wieku normą staje się tworzenie międzynarodowych firm, których pracownicy mieszkają w różnych krajach, „spotykają się" i pracują przez nowoczesne technologie komunikacyjne. Te, które wprowadziły w ostatnich dziesięcioleciach szczególną rewolucję, nazywane są technologiami sieciowymi. Ich narodziny i rozwój w niezwykły sposób wpłynęły na życie społeczne przynosząc ze sobą wiele społecznego dobrodziejstwa. Z ich możliwości korzystają zarówno rządy, organizacje pozarządowe, świat biznesu, jak i zwykli ludzie w ich codziennej komunikacji. Czy jednak technologie sieciowe są jedynie wielkim społecznym dobrodziejstwem? Czy ich narodziny jedynie służą czy także szkodzą społeczeństwu? Nieograniczony do nich dostęp sprawił, że bardzo szybko zaczęły się nimi posługiwać także grupy społecznie szkodliwe – świat przestępczy czy szerzej – międzynarodowy terroryzm. Czy w świetle działań terrorystycznych wartościowanie technologii sieciowych jest społecznie jednoznaczne?

1. O technologiach sieciowych słów kilka

Pojęcie t*echnologie sieciowe* po raz pierwszy pojawiło się w końcu lat 90. XX wieku w związku z rozwojem komunikacyjnych możliwości Internetu. Jego powstanie, w połączeniu z nowymi osiągnięciami w telekomunikacji i informatyce, doprowadziło do innej wielkiej technologicznej zmiany – przejścia od rozrzuconych, izolowanych mikro-komputerów i superkomputerów do szerokiej informatyzacji za pośrednictwem połączonych urządzeń przetwarzających informację, wykorzystujących wielorakie formaty[1]. Z czasem urządzenia komputerowe rozpowszechniły się we wszystkich możliwych sferach życia oraz działalności – w: domu, pracy, sklepach, rozrywce, transporcie etc. Urządzenia, w wielu przypadkach przenośne, mogły komunikować się między sobą nie korzystając z własnego systemu operacyjnego. Podstawowa technologia, aplikacje i dane są przechowywane na serwerach sieciowych, a informatyczna inteligencja mieści się w samej sieci: witryny komunikują się ze sobą i mają do dyspozycji niezbędne oprogramowanie, pozwalające włączyć dowolne urządzenie do uniwersalnej sieci komputerowej. Logika sieci, ucieleśniana

[1] Castells M.: Społeczeństwo sieci. PWN, Warszawa 2007, s. 63.

przez Internet, zaczęła być stosowana w każdej dziedzinie działalności, w każdym kontekście i w każdym miejscu, które mogło być połączone elektronicznie[2].

Technologie sieciowe nazywane są często informacyjnymi, komunikacyjnymi lub ICT. Jest to szerokie pojęcie, obejmujące wszystkie środki techniczne, służące przekazywaniu informacji. Innymi słowy ICT dotyczy zastosowania technologii cyfrowych, które pomagają ludziom w przetwarzaniu i przekazywaniu informacji. Te technologie mają szeroki zakres – od komputerów osobistych do PDA (Personal Digital Assistant), od telefonów komórkowy do telefonów satelitarnych czy od faksów do robotów. Zapotrzebowanie na bardziej zaawansowane technologie komunikacyjne doprowadziło do ogromnego postępu w późnych latach 70. W tym czasie inżynierowie telekomunikacyjni marzyli o jednej rzeczy – „the death of distance"[3] (śmierci odległości). To marzenie stało się rzeczywistością i pojawiły się takie technologie, jak Internet czy telefony satelitarne.

Nowoczesna komunikacja technologiczna bardzo zmieniła życie zwykłego człowieka. Obecnie mówi się, że żyjemy w globalnej wiosce, gdzie informacja jest na usługach każdego człowieka. To wszystko stało się dzięki rewolucji teleinformatycznej. Technologie informacyjne i komunikacyjne zdecydowanie zmieniły nasze życie. Ludzie wykorzystują je w komunikacji społecznej, edukacji czy biznesie. Wspólne środowiska wirtualne (CVE) dostarczyły biznesmenom okazji do uruchomienia ich działalności na całym świecie – w różnych geograficznie miejscach, pozwalając im równocześnie na zachowanie biura w ich naturalnym miejscu pracy i życia. Telefony satelitarne zmniejszyły dystans w relacjach międzyludzkich. Dość powszechne i nikogo niedziwiące stały się związki na odległość osób z różnych miast, krajów, a czasem nawet kontynentów. Marzenie dwudziestowiecznych inżynierów o „the death of distance" spełniło się.

2. Terroryzm i jego młodszy brat – cyberterroryzm

To jeden z najbardziej kontrowersyjnych terminów w nowoczesnym świecie. Nie istnieje jedna, powszechnie akceptowana jego definicja. Różne rządy i różne agencje używają własnych definicji terroryzmu. Według badań przeprowadzonych w 2003 roku przez Jeffreya Recorda z armii amerykańskiej istnieje ich ponad 100. Swoim zasięgiem objęły łącznie 22 różne elementy definicyjne[4]. Termin stał się kontrowersyjny ze względu na mieszanie interesów różnych krajów i narodów. Na ten problem wskazuje m.in. Organizacja Narodów Zjednoczonych (United Nations). Organizacja ta, ze względu na konflikt interesów

[2] The Economist, 1997, http://economist.com, p. 33.
[3] Cairncross F.: The Death of Distance: How the Communications Revolution Will Change Our Lives. Harvard Business School Press, Boston 1997, p. 118.
[4] Record J.: Bounding the global war on Terrorism. Strategic Studies Institute, December 2003.

suwerennych państw, które określają, w każdym przypadku indywidualnie, jaki podmiot jest terrorystą, a jaki bojownikiem o wolność, nie jest w stanie podjąć decyzji w sprawie definicji terroryzmu[5]. Często zdarza się, że ta sama osoba w jednym kraju uważana jest za bojownika o wolność, a w drugim za terrorystę.

Zdaniem Todda Sandlera i Waltera Endersa terroryzm jest użyciem z premedytacją lub zagrożeniem stosowania przemocy przez osoby lub grupy narodowe, w celu uzyskania politycznych lub społecznych celów przez zastraszanie dużej grupy odbiorców bezpośrednimi ofiarami[6]. Według tych badaczy istnieją dwa podstawowe składniki charakteryzujące każdą nowoczesną definicję terroryzmu: obecność lub zagrożenie przemocą i polityczny/społeczny motyw. Bez przemocy lub jej groźby terroryści nie mogą wpływać na decyzje polityczne, będące odpowiedzią na ich żądania, natomiast w przypadku braku politycznego/społecznego motywu akt przemocy jest przestępstwem, a nie aktem terroryzmu[7]. Inna, uproszczona definicja terroryzmu przyjęta została przez Narodowe Konsorcjum Studiów nad Terroryzmem i Odpowiedzi na Terroryzm (National Consortium for Study of Terrorism and Responses to Terrorism – START) Departamentu Stanu USA. W tym ujęciu terroryzm to grożenie lub rzeczywiste wykorzystanie nielegalnej siły i przemocy niepaństwowych aktorów do osiągnięcia celu politycznego, gospodarczego, religijnego lub społecznego przez strach, przymus lub zastraszanie[8].

3. Cyberterroryzm

Najprościej rzecz ujmując jest to mariaż technologii i terroryzmu. Jest to typ terroryzmu, który bezpośrednio jest związany z postępem w dziedzinie technologii. Sam termin został wprowadzony po nagłym i niekontrolowanym rozwoju w dziedzinie techniki. Podobnie jak terroryzm, termin cyberterroryzm jest kontrowersyjny i nie ma powszechnie przyjętej jego definicji. Niektórzy naukowcy twierdzą, że wykorzystanie komputerów i zasobów technologii informatycznych dla dowolnego działania terrorystycznego może być określane mianem cyberterroryzmu. Inni twierdzą, że cyberterroryzm jest nadużyciem systemów informatycznych i baz danych, jak hakowanie baz danych organizacji i uzyskiwanie informacji do nielegalnych celów. Jedną z definicji podaje Dorothy E. Denning. Jej zdaniem jest to zbieżność terroryzmu i cyberprzestrzeni. Są to generalnie rozumiane bezprawne ataki i groźby ataku na komputery, sieci i informacje w niej zapisane, służące temu, by zastraszyć

[5] Kochler H.: The United Nations, International Rule of Law and Terrorism, in: The Supreme Court Centenary Lecture Series. I: July 2000 – June 2001; II. September 2001 – June 2002. Manila: Supreme Court of the Philippines / Philippine Judicial Academy, 2002, pp. 550–571.
[6] Sandler T., Enders W.: The Political Economy of Terrorism. Cambridge University Press, New York 2006.
[7] Ibidem.
[8] International Institute for Counter-Terrorism, www.ict.org.il/.

lub zmusić rząd lub jego ludzi do osiągnięcia określonych celów politycznych lub społecznych. Ponadto, aby atak zakwalifikować jako cyberterroryzm, powinien on spowodować przemoc wobec osób lub mienia, lub przynajmniej spowodować tyle szkód, aby wywołać strach. Będą to więc ataki, które prowadzą do śmierci lub cielesnej szkody, wybuchy, katastrofy lotnicze, zanieczyszczenie wody lub ciężkie straty gospodarcze. Ciężkie ataki na kluczową infrastrukturę mogą być, w zależności od wielkości ich wpływu, aktami cyberterroryzmu. Nie będą nimi natomiast ataki, które zakłócają nieistotne usługi lub są uciążliwe finansowo[9].

Czysty cyberterroryzm

Istnieje również inny termin związany z cyberterroryzmem – czysty cyberterroryzm (*pure cyber-terrorism*). Nazywa się go również czasem bezkrwawym terroryzmem (*bloodless terrorism*). Dotyczy on działań terrorystycznych, które dzieją się całkowicie w wirtualnym świecie. Przykładem tego mogą być włamania do banków. Organizacje terrorystyczne potrzebują funduszy na prowadzenie swojej działalności w realnym świecie, a dzięki współczesnym systemom bankowości online i wielu internetowych usług finansowych mają możliwość (przez cyberterroryzm) wykradania pieniędzy z banków i następnie wykorzystywania ich do finansowania innych działań terrorystycznych. Idea ta była już podejmowana w 1991 roku i opisana w raporcie „Computers at Risk", stworzonym przez zarząd amerykańskiego The Computer Science and Telecommunications. Autorzy tego raportu wskazywali na niebezpieczeństwo związane z tym, że funkcjonowanie państwa zależy w zbyt dużym stopniu od komputerów. Kontrolują one dostawy energii, komunikację lotniczą, usługi finansowe, są wykorzystywane do przechowywania ważnych informacji, rejestrów medycznych, rejestrów karnych, wykorzystywane przez biznes. I mimo że darzone są one powszechnym, społecznym zaufaniem, narażone są – z powodu złej konstrukcji i niedostatecznych kontroli jakości – na ataki terrorystyczne. Współczesny złodziej może ukraść więcej za pomocą komputera niż pistoletu. Ich zdaniem terrorysta jutra może uczynić więcej szkód przy użyciu klawiatury niż bomby[10]. Niestety te prognozy się sprawdziły.

4. Technologie sieciowe – społecznie użyteczne czy szkodliwe?

Z założenia nowe technologie zawsze służyć mają dobru społeczeństwa i ludzi, ale z powodu braku ograniczeń i łatwej dostępności nie ma gwarancji, że technologie te są zawsze używane zgodnie z przeznaczeniem. Przykładem może być technologia Google Earth

[9] Denning, D.: Cyberterrorism. Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services. US House of Representatives, 23 May 2000.
[10] National Research Council: Computers at Risk. National Academy Press, 1991.

(program komputerowy umożliwiający wyświetlanie na trójwymiarowym modelu kuli ziemskiej zdjęć satelitarnych, lotniczych, panoram zrobionych z poziomu ulicy oraz różnego rodzaju informacji geograficznych i turystycznych), która jest jedną z wielu nowoczesnych technologii, z której korzystają naukowcy różnych dziedzin. Używa się jej m.in. do tworzenia map do pomiaru podatność powierzchni na powodzie i trzęsienia ziemi czy inne klęski żywiołowe. Równocześnie jednak ta sama technologia może być również wykorzystywana do zabicia setek niewinnych ludzi. Przykładem tego jest jej wykorzystanie przez terrorystów zaangażowanych w ataki w Mumbaju w Indiach w 2008 roku[11].

Bardzo pożytecznymi społecznie i jednymi z najbardziej dynamicznie rozwijających się działów teleinformatyki są narzędzie biometryczne, wykorzystywane przede wszystkim do kontroli dostępu do chronionych pomieszczeń lub autoryzacji użytkowników korzystających z określonych danych, programów czy urządzeń (nieautoryzowane próby dostępu do bankomatów, komputerów osobistych, sieci komputerowych, telefonów komórkowych, domowych systemów alarmowych etc). Niektóre kraje wprowadziły rozwiązania biometryczne na granicach. Funkcjonują one już z powodzeniem m.in. na lotniskach w Stanach Zjednoczonych czy w Australii. Australia zdecydowała się na zastosowanie systemu rozpoznawania twarzy (Smart Gate[12]), który dział równolegle z tradycyjnymi punktami odprawy paszportowej. Odprawa z zastosowaniem czytnika twarzy trwa jedynie 6 sekund. Systemy biometryczne chcą wprowadzić u siebie także Francja (rozpoznawanie twarzy) i Wielka Brytania (odczytywanie tęczówki oka). Równocześnie jednak terroryści doskonalą sposoby pozwalające na obejście biometrii lub jej zafałszowanie (jak choćby przy fałszowaniu pieniędzy).

Kolejnym przykładem technologii sieciowych jest *Visual Surveillance*, czyli monitorowanie zachowań, działań, zwyczajów ludzi w celu wywarcia na nich wpływu, zarządzania, kierowania i ich ochrony[13]. Może obejmować obserwacje z odległości za pomocą urządzeń elektronicznych (takich jak kamery CCTV) lub przechwycenia informacji przesyłanych drogą elektroniczną (takich jak Internet lub telefon)[14]. System ten jest wykorzystywany przez rządy do wywiadu, zapobiegania przestępczości, ochrony procesów, osób, grupy lub do badania zbrodni. Ale nie tylko. Jest również stosowany przez organizacje przestępcze do planowania i popełniania przestępstw, takich jak napady czy porwania.

Bardzo często używany jest obecnie także *Tracking of personal data* (śledzenie danych osobowych), a więc pozyskiwania z różnych źródeł informacji o osobach, zestawiania ich i wyciągania na ich podstawie kolejnych wniosków w celu stworzenia profilu za pomocą

[11] The Washingtonpost, www.washingtonpost.com/wpdyn/content/article/2008/12/02/AR2008120203519.html.
[12] Wikipedia, http://en.wikipedia.org/wiki/SmartGate.
[13] Lyon D.: Surveillance Studies: An Overview. Polity Press, Cambridge 2007.
[14] Minsky M., Kurzweil R., Mann S.: The Society of Intelligent Veillance. Proceedings of the IEEE ISTAS 2013. Toronto, Ontario, Canada 2013, p. 13-17.

nowoczesnych narzędzi komunikacyjnych. Zastosowanie dużych zbiorów danych może przynieść wiele korzyści zarówno dla biznesu, rządów, jak i organizacji non profit. Jednak podkreśla się przy tym, że biorąc pod uwagę ogólne zasady ochrony danych i prywatności, zjawisko profilowania powinno być ograniczone do niezbędnego minimum. Niebagatelną rolę odgrywa także informowanie użytkowników o tym, że podlegają profilowaniu, nawet w przypadku, gdy profilowanie odbywa się na podstawie powszechnie dostępnych źródeł. Do walki z terroryzmem używa się wielu typów profilowania[15] (profile oparte na konkretnych informacjach wywiadowczych, profile nieoparte na konkretnych informacjach wywiadowczych, profilowanie przez „eksplorację danych"), jednak w ostatnich latach dużo mówi się o profilowaniu etnicznym[16]. Jego używaniem zaniepokojone są jednak organizacje międzyrządowe, takie jak ONZ, Rada Europy i Unia Europejska, a także organizacje pozarządowe, działające w dziedzinie ochrony praw człowieka. Wysuwa się w szczególności argument, że profilowanie etniczne nie tylko koliduje z prawem w zakresie dyskryminacji, ale ma także niekorzystne skutki społeczne. Jednak terroryści często wykorzystują fałszywe profile, by ukryć swą prawdziwą tożsamość.

Inną, nowoczesną technologią sieciową są *spy satellites* – satelity rozpoznawcze, często potocznie nazywane satelitami szpiegowskimi. Ich zadaniem jest obserwowanie obiektów na Ziemi oraz przechwytywanie sygnałów z Ziemi, w celach wojskowych lub wywiadowczych. Często obserwacja ta związana jest z wykonywaniem fotografii o dużej rozdzielczości (do poniżej 1 m), które można wykorzystać na wiele sposobów (na przykład śledzić przemieszczenia wojsk przeciwnika lub uzyskiwać informacje o potencjalnych celach na jego terytorium). Istnieją również satelity zdolne zdobywać informacje przez chmury lub w nocy, wykonując zdjęcia w podczerwieni lub używając radaru. Ich podstawowym celem jest dostarczanie danych dotyczących potencjału gospodarczo-militarnego ewentualnego przeciwnika, struktur i wyposażenia oraz dyslokacji jego sił zbrojnych i stopnia przygotowania do obrony kraju[17]. Przykładem użycia satelity jest operacja Allied Force przeprowadzona przez siły Sojuszu Północnoatlantyckiego (NATO) między 24 marca i 20 czerwca 1999 roku w Federalnej Republice Jugosławii, mająca doprowadzić do zakończenia czystek etnicznych na terenie Kosowa i przywrócenia wieloetnicznego charakteru tej prowincji oraz wymuszenia procesu demokratyzacji w Jugosławii. Do rozpoznania sytuacji użyto głównie środków rozpoznania powietrznego oraz

[15] Podniesienie skuteczności działań policji. Rozumienie dyskryminującego profilowania etnicznego i zapobieganie mu. Przewodnik. Urząd Publikacji Unii Europejskiej, Luksemburg 2010.

[16] Nie jest ono nową praktyką w państwach członkowskich Unii Europejskiej. Na znaczeniu zyskało w reakcji na zamachy terrorystyczne w Stanach Zjednoczonych (2001), Madrycie (2004) i Londynie (2005) oraz na zwiększone obawy dotyczące nielegalnej imigracji.

[17] Nowacki G.: Rozpoznanie satelitarne USA i Federacji Rosyjskiej. Akademia Obrony Narodowej, Warszawa 2002, s. 57-64.

kosmicznego[18]. Podczas całej operacji satelity rozpoznawcze (satelity IMINT (Imagery Intelligence) wyposażone w aparaturę elektrooptyczną i sensory podczerwieni o dużej rozdzielczości (IR), satelity Lacrosse służące do sporządzania radarowego obrazu obszaru operacji oraz satelity ELINT/SIGINT typów Merkury, Mentor, Trumpet i Orion, przeznaczone do przechwytywania sygnałów elektronicznych w szerokim zakresie częstotliwości) śledziły przede wszystkim lokalizację serbskich sił zbrojnych oraz ich komunikację, przechwytując sygnały radiowe oraz fotografując stanowiska bojowe przeciwnika. Satelity teoretycznie nie mogą być wykorzystywane do celów niezgodnych z prawem, jednak w praktyce bywa inaczej. Podobnie jak w przypadku innych technologii także satelity mogą być wykorzystywane przez terrorystów do analogicznych, jak w przypadku wojska, celów.

Komputery i Internet to kolejny przykład nie najnowszej już technologii sieciowej, pomagającej z jednej strony walczyć z terroryzmem, z drugiej jednak służący terroryzmowi. O cyberterroryzmie wspominano już było w poprzednim paragrafie. Tu jednak jeszcze kilka przykładów. Komputery powstały pierwotnie jako maszyny służące do liczenia, z czasem stały się medium służącym we wszystkich niemal sferach życia człowieka. W połączeniu z Internetem (powstałym pierwotnie na potrzeby wojska w postaci sieci ARPANET) ich moc nieobliczalnie wzrosła służąc zarówno walce z przestępczością i terroryzmem, jak i samemu terroryzmowi. Dość wspomnieć o włamaniach na konta bankowe, nielegalnych transakcjach w sieci, aż do Dark Web (Deep Web, Deepnet, Invisible Web, Hidden Web).

Dark Web[19] to termin odnoszący się do konkretnej kolekcji witryn, które teoretycznie są widoczne dla wszystkich, ale ich adresy IP i serwery, na których są prowadzone są ukryte. W ten sposób mogą być odwiedzane przez każdego użytkownika sieci, ale jest bardzo trudno dojść kto stoi za daną witryną. Stron tych nie można również znaleźć za pomocą wyszukiwarek. Prawie wszystkie strony Dark Web ukrywają swoją tożsamość przy użyciu narzędzia szyfrowania Tora, dzięki któremu można ukryć właściwości końcowego użytkownika, ukryć tożsamość i sfałszować lokalizację. Aby wejść na stronę na Dark Web, który jest szyfrowana przy użyciu Tora, należy użyć Tora. Przykłady ciemnych stron internetowych to Silk Road (Jedwabny Szlak) i jego potomstwo. Silk Road służy do kupna i sprzedaży narkotyków, ale istnieją także inne zastosowania Dark Web. Osoby działające w zamkniętych społeczeństwach totalitarnych mogą korzystać z Dark Internetu do komunikowania się ze światem zewnętrznym. Najogólniej rzecz ujmując, Dark Internet służy przede wszystkim szeroko pojętemu terroryzmowi.

[18] Marszałek M.: Sojusznicza operacja "Allied Force": przebieg – ocena – wnioski. Adam Marszałek, Toruń 2009.

[19] Egan M.: What is the Dark Web? How to access the Dark Web – How to turn out the lights and access the Dark Web (and why you might want to) ALL OF THE INTERNET IS DRUGS AND PORN AND GUNS AND TERRORISTS, www.pcadvisor.co.uk/how-to/internet/3593569/what-is-dark-web-how-access-dark-web/.

Podobnemu celowi służą także telefony komórkowe i satelitarne (komunikacja, detonacja etc.), telewizja (głównie jako forma komunikacji i zastraszania – pokazowe ścinanie głów etc.) oraz inne niewspomniane tutaj nowoczesne wynalazki. W ostatnich latach przestępcy zaczęli też z powodzeniem wykorzystywać media społecznościowe. Pojawiło się już nawet pojęcie *Twitter terrorism*[20]. Uważa się, że Państwo Islamskie ma ponad 50 tys. kont na Twitterze wykorzystywanych głównie do komunikacji. Powszechnie używana jest również steganografia (nauka o komunikacji w taki sposób, by obecność komunikatu nie mogła zostać wykryta). Za jej pomocą umieszcza się ukryty przekaz w innej treści, która wcale nie wygląda jak ukryty przekaz. Bardzo często wykorzystywane są do tego zdjęcia, których w sieci są miliony.

5. Zakończenie

Technologie informacyjne i komunikacyjne mają wpływ na każdego człowieka i na każdą dziedzinę jego życia. Upraszczając komunikację uczyniły one nasze życie łatwiejszym. Ostatnie dwadzieścia lat przyniosło ogromne zmiany w świecie technologicznym. Najbardziej widocznym tego przykładem jest ewolucja telefonu komórkowego, który na początku lat dziewięćdziesiątych uważany był za luksus, a dzisiaj ludzie używają sprzętu PDA jako ułatwienia w prawie każdym procesie komunikacji. Ta zmiana, którą niektórzy autorzy nazywają „rozwojem technologii", stała się powodem do wyścigu gospodarczego pomiędzy krajami i organizacjami. Stała się jednak także powodem do wyścigu pomiędzy światem przestępczym a tymi, którzy go zwalczają.

Czy więc technologie sieciowe są społecznie użyteczne? Odpowiedź na to pytanie nie jest prosta. Z jednej strony zdecydowanie tak, z drugiej jednak niosą ze sobą poważne ryzyko wykorzystania ich przez niepowołane osoby w niewłaściwy sposób. Ten dylemat dotyczy jednak każdego typu technologii od zarania jej dziejów. Ich społeczne wartościowanie nie jest łatwe, jednak niezmiernie potrzebne, gdyż rozwój technologiczny, idący w parze z rozwojem społecznym, nie zawsze musi temu społeczeństwu dobrze służyć. Przy ich ocenie trzeba wziąć pod uwagę ich swoisty dualizm, gdyż te same technologie mogą równocześnie służyć dobrym, a także złym sprawom. Takie technologie jak telefon czy Internet bardzo ułatwiają życie. Wielu ludzi nie wyobraża sobie życia codziennego bez ich udziału. To w Internecie wyszukujemy wszystkie potrzebne nam informacje o dostępie, do których do tej pory mogliśmy tylko pomarzyć. Książkowe encyklopedie i słowniki pozostają już zwykle na półkach. Równocześnie jednak Internet służy terrorystom do komunikacji, ale również jako źródło potrzebnej wiedzy. To w Internecie można na przykład znaleźć przepis na to,

[20] BBC News, Europol chief warns on computer encryption, www.bbc.com/news/technology-32087919.

jak zrobić bombę domowego użytku. To także w sieci szukają porad chorzy próbujący się sami zdiagnozować i wyleczyć, często bardzo sobie szkodząc. Technologie, jak telefon, mogą służyć ratowaniu życia (przez wezwanie pomocy) lub jego odebraniu (detonacja bomby). Pomagają walczyć z przestępczością, jak wspomniane wyżej satelity lub *Tracking of personal data*, ale także tej przestępczości służą. Jednocześnie ułatwiają komunikacją, a także ją utrudniają i służą manipulacji (jak *Twitter terrorism*, zakłócanie przekazu informacji, szum informacyjny etc.). Mają nas chronić, jak kamery monitoringu, równocześnie jednak nas szpiegując. Czy więc o technologiach sieciowych można i czy warto mówić w jednoznaczny społecznie sposób?

Mnogość ich wykorzystania potwierdza tezę, że ich społeczne wartościowanie jest niezmiernie trudne, co nie znaczy, że niepotrzebne. Wykorzystanie nowoczesnych technologii zarówno w dobrych, jak i złych społecznie celach wydaje się być nieuniknione. W dziejach ludzkości prawdopodobnie żadna nowość techniczna nie służyła tylko dobrym celom, bardzo często wbrew intencjom ich twórców. Wystarczy tu przywołać historię Alfreda Nobla i jego niezwykłego wynalazku[21]. Społeczne doświadczenie pokazuje, że z tą sytuacją ludzkość musi nauczyć się żyć. W przeciwnym razie, jakie inne ma możliwości? Nie tworzyć wynalazków? Nie rozwijać technologicznych umiejętności człowieka? Nowe technologie, także sieciowe, i tak będą powstawać i będą rozwijane także przez świat przestępczy. Ważne jednak jest to, aby ich wykorzystanie było zawsze jak najbardziej społecznie użyteczne i by były one w miarę możliwości chronione przed niewłaściwym wykorzystaniem. Tu pojawia się jednak kolejne pytanie – czy mamy jeszcze nad tym kontrolę? Odpowiedź przyniosą prawdopodobnie kolejne lata wykorzystania technologii sieciowych.

Bibliografia

1. BBC News, Europol chief warns on computer encryption, www.bbc.com/news/technology-32087919.
2. Bjørgo T.: Root causes of terrorism: myths, reality and ways forward. Routledge, London and New York 2005.
3. Castells M.: Społeczeństwo sieci. PWN, Warszawa 2007.
4. Cairncross F.: The Death of Distance: How the Communications Revolution Will Change Our Lives. Harvard Business School Press, Boston 1997.
5. Denning D.: Cyberterrorism. Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services. US House of Representatives, 23 May 2000.

[21] The Official Web Site of the Nobel Prize, http://www.nobelprize.org/alfred_nobel/will/.

6. Kochler H.: The United Nations, International Rule of Law and Terrorism, [in:] The Supreme Court Centenary Lecture Series. I: July 2000 – June 2001; II. September 2001 – June 2002. Manila: Supreme Court of the Philippines / Philippine Judicial Academy, 2002, p. 550-571.
7. Lyon D.: Surveillance Studies: An Overview. Polity Press, Cambridge 2007.
8. Marszałek M.: Sojusznicza operacja "Allied Force": przebieg – ocena – wnioski. Adam Marszałek, Toruń 2009.
9. Minsky M., Kurzweil R., Mann S.: The Society of Intelligent Veillance. Proceedings of the IEEE ISTAS 2013. Toronto, Ontario, Canada 2013.
10. National Research Council: Computers at Risk. National Academy Press, 1991.
11. Nelson B., Choir R., Iacobucci M., Mitchell M.: USA, Captain Greg Gagnon, USAF. White paper, Cyberterror Prospects and Implications.
12. Nowacki G.: Rozpoznanie satelitarne USA i Federacji Rosyjskiej. Akademia Obrony Narodowej, Warszawa 2002.
13. Podniesienie skuteczności działań policji. Rozumienie dyskryminującego profilowania etnicznego i zapobieganie mu. Przewodnik. Urząd Publikacji Unii Europejskiej, Luksemburg 2010.
14. Record J.: Bounding the global war on Terrorism. Strategic Studies Institute, 2003.
15. Sandler T., Enders W.: The Political Economy of Terrorism. Cambridge University Press, New York 2006.
16. Egan M.: What is the Dark Web? How to access the Dark Web – How to turn out the lights and access the Dark Web (and why you might want to) ALL OF THE INTERNET IS DRUGS AND PORN AND GUNS AND TERRORISTS, www.pcadvisor.co.uk/how-to/internet/3593569/what-is-dark-web-how-access-dark-web/, access 15.03.2015.
17. International Institute for Counter-Terrorism, www.ict.org.il/, access 15.03.2015.
18. Study of terrorism and responses to terrorism (START), www.start.umd.edu/start/, access 16.03.2015.
19. The Economist, 1997, http://economist.com, access 14.03.2015.
20. The Official Web Site of the Nobel Prize, http://www.nobelprize.org/alfred_nobel/will/, access 10.08.2015.
21. The Washingtonpost, www.washingtonpost.com/wpdyn/content/article/2008/12/02/AR2008120203519.html, access 14.03.2015.
22. Wikipedia, http://en.wikipedia.org/wiki/SmartGate, access 14.03.2015.

Abstract

The last twenty years have brought very big changes in the world of technology. This change, which some authors call "technology development", has become a cause for the economic race between countries and organizations. But also it became the reason of the race between the criminal world and those who oppose him. So does the network technologies are socially useful? The answer to this question is not simple. On the one hand, definitely yes, on the other, they bring with them a serious risk of their use by unauthorized users or in the wrong way. This dilemma, however, has brought each type of technology since the dawn of its history. Their social evaluation is not easy but very required because technological development, going hand in hand with social development, does not always serve this society well.