Potencjalne zagrożenia społeczeństwa informacyjnego

świetna praca magisterska o społeczeństwie informacyjnym

Zagrożeniem dla społeczeństwa informacyjnego, zmuszającym do wprowadzenia ograniczeń i cenzury do sieci, mogą stać się akcje przestępców i terrorystów. Przed upowszechnieniem się internetowej sieci komputerowej, największym problem światowych służb specjalnych było ściganie handlarzy narkotyków, nielegalnych imigrantów i przemytników. Obecnie dzięki nowej technologii przestępcy i terroryści mogą pozwolić sobie na bezpieczne działanie na odległość. Patrolowanie lachy sieciowych w poszukiwaniu danych pozostawionych przez przestępców jest znacznie trudniejsze i wymaga od stróży prawa specyficznych umiejętności.

Obecnie łatwy dostęp do informacji zawartych w międzynarodowej sieci komputerowej sprawia, ze głównym instrumentem używanym do przeprowadzania przestępczych i terrorystycznych akcji staja się rożnego rodzaju bomby „domowej roboty”. Jeszcze do niedawna nielegalne zdobycie broni, szczególnie w Stanach Zjednoczonych było znaczne łatwiejsze niż uzyskanie informacji o sposobach konstruowania lądunków wybuchowych. Dziś sytuacja uległa zmianie. Korzystając z wysyłkowych księgarni internetowych bez trudu można nabyć w cenie 4 dolarów instrukcje US Ramy „Improvised Munitions, Handbook”, która uczy, jak sporządzać bomby domowym sposobem, lub „Anarchist’s Cookbook”. Liczba sprzedanych egzemplarzy wyżej wymienionych pozycji sięga milionów sztuk. Książki te, zawierają wiele błędów, co doprowadziło już do niejednego wypadku śmiertelnego przy sporządzaniu ładunków wybuchowych. Wystarczy jednak skontaktować się z licznie znajdującymi się w sieci

specjalistami od konstrukcji bomb, aby zweryfikować informacje i przedsięwzięcie zakończyć sukcesem. Koszt zdobycia „przepisu na bombę" równa się kilku minutom polaczenia do biuletynowej sieci internetowej i wydrukowi z domowej drukarki.

Z reguły w zamachach terrorystycznych używane są najprostsze bomby, do których wszystkie elementy można zakupić w ogólnie dostępnych sklepach chemicznych i technicznych wydając niecałe 100 dolarów. Wystarczy tylko połączyć wszystkie części zgodnie z instrukcja, przy czym można nieustannie korzystać z pomocy internetowych fachowców. Zazwyczaj już w kilka godzin po wielkich terrorystycznych zamachach można znaleźć w Internecie szczegółowe instrukcje, jak skonstruować użyte niedawno bomby domowym sposobem, ewentualnie również jak uniknąć błędów, które przydarzyły się zamachowcom.

Wzrasta również liczba internetowych stron World Widea Web (WWW), na lamach, których jawnie propaguje się:

- nazizm,
- nienawiść rasowa,
- terroryzm.

W ciągu ostatniego roku, jak podaje raport przygotowany przez Centrum Szymona Wiesenthala, liczba tego rodzaju publikacji wzrosła dwukrotnie. Dzięki internetowi entuzjaści wielu nielegalnych idei mogą bezpiecznie propagować swoje poglądy, leczyć się w międzynarodowe organizacje, wzajemnie wspierać się finansowo i informować o działaniach. Łatwość komunikowania się i docierania do bardzo dużych grup odbiorców pozwala również w sposób zamaskowany szerzyć idee rasistowskie i fundamentalistyczne wśród młodych internautów. Istnieje zagrożenie, ze mniej odporna na tego typu argumenty cześć młodzieży może stać się łatwym lupę agresywnych demagogów. *„Strony takie, promujące rasizm i terroryzm, są bardzo łatwe i tanie do stworzenia -powiedział Marc Knobel z Centrum Szymona Wiesenthala podczas prezentacji przygotowanej na konferencje ONZ poświęconej rasizmowi w Internecie*"(28).

Kneble twierdzi, ze odpowiedzialnością za treść stron WWW powinno obciążyć się dostawców usług internetowych, którzy powinni sprawdzać swój serwer pod katem informacji, które mogłyby urazić uczucia innych ludzi. Byłaby to pewnego rodzaju cenzura zawartości sieci. Trudno jednak stworzyć instytucje, które decydowałyby, które materiały są w Internecie niepożądane i jak należy z nimi postępować (kasować, blokować, prosić o usuniecie). Dla dużych dostawców usług internetowych dokładne sprawdzenie wszystkich treści znajdujących się na ich serwerach może okazać się wprost niemożliwe, ponadto istnieją tysiące sposobów na obejście przepisów i oszukanie kontrolujących.

Internet zawsze postrzegany był jako medium zapewniające całkowita wolność słowa i anonimowość, co często wykorzystywane jest przez organizacje terrorystyczne. Bardzo często tego typu działalność ukrywa się pod egida szanowanych organizacji, takich jak AANA (Algieria American Nasiona Association) albo IANA (Islamic Assembly of North America). Terrorysci i międzynarodowi przestępcy bardzo często korzystają z list dyskusyjnych do rozsyłania informacji o swoich ideach i zadaniach. Dzięki technologii listy dyskusyjnej w całkowicie legalny sposób przesyłają tysiącom ludzi swoje informacje. Korzystają również z serwerów uczelni, gdzie wolno jest zakładać strony i listy dyskusyjne o dowolnej tematyce, bądź tam, gdzie nie jest to dostatecznie kontrolowane. Ze sposobów tych najczęściej korzystają grupy fundamentalistów islamskich bądź skrajnych faszystów.

Istnieją organizacje studenckie, które specjalizują się w zwalczaniu przestępczej działalności w sieci. Gdy znajda w Internecie listę z wiadomościami o treściach zdecydowanie niedemokratycznych – „zasypują” zidentyfikowana grupę dyskusyjna setkami listów (tzw. śmieci), co w rezultacie uniemożliwia korzystanie z niej. Często docierają do serwera mieszczącego tego rodzaju grupę i niszczą go w „pirackim stylu”. Jednym za znanych centrów „polowania” na terrorystów

(w tym wypadku faszyzujących), jest Simon-Wiesenthal w Los Angeles pod kierownictwem rabina Abrahama Coopera. Zwalczają wszelkiego rodzaju internetowe grupy, szczególnie jednak spadkobierców Ku-Kluć-Klanu i John Birch Socjety.

Dyskusje o potrzebie ocenzurowania wiadomości znajdujących się i przesyłanych w sieci trwają od wielu lat. Wcześniej większe znaczenie przykładano do ochrony przed zalewem pornografia i finansowymi oszustwami, dziś na pierwszy plan wysuwa się walka z terroryzmem. Zdecydowana większość użytkowników sieci nie życzy sobie jakiejkolwiek kontroli. Sytuacja taka ma miejsce szczególnie w Stanach Zjednoczonych, gdzie wolność słowa jest gwarancja wolności obywatelskiej i jest wysoko ceniona. Coraz więcej ludzi wydaje się być przekonanych o konieczności wprowadzenia ograniczonej cenzury – w tym również coraz więcej zwykłych użytkowników Internetu. Przyczynia się do tego zastraszająca statystyka stron, prowadzona przez liczne centra zajmujące się zwalczaniem przejawów terroryzmu, w tym nazizmu, faszyzmu i fundamentalizmu islamskiego. Na wszystkich zarejestrowanych stronach na przykładowym serwerze w Stanach Zjednoczonych w 1997 roku 16% promuje wprowadzenie hierarchii opartej na pochodzeniu rasowym, 14,5% głosi hasła neonazistowskie, 6% przekonuje o wyższości białych, a 8,5% otwarcie propaguje terroryzm(29).

Podsumowując 45% stron to strony, które zawierają elementy uznawane za niebezpieczne. Na jednej ze stron, znajdującej się do dziś w Internecie umieszczono „wirtualny Auschwitz", w którym umieszcza się wszystkich, którzy sprzeciwiają się poglądom „rasy panów". Ludzie zawodowo zajmujący się zawartością Internetu twierdza, ze tendencji tej nie da się powstrzymać bez wprowadzenia cenzury blokującej dostęp do tego typu informacji. Nawet przy wprowadzeniu takich ograniczeń szybki rozwój technologii będzie dawał szanse terrorystom i ideologom dla przemycania szkodliwych informacji.

Coraz częściej problem terroryzmu i przestępczości postrzegany jest jako priorytetowy przez organizacje europejskie.

Ministrowie służb zagranicznych i spraw wewnętrznych siedmiu najbardziej uprzemysłowionych państw świata (G-7) oraz Rosji stworzyli w 1996 roku listę 25 sposobów skutecznej walki z terroryzmem i przestępczością międzynarodowa. Jednym z najważniejszych stal się nadzór nad nowymi środkami liczności, a przede wszystkim nad Internetem. Europa odmiennie podchodzi do problemu ocenzurowania sieci komputerowej. Niektóre kraje m.in. Niemcy i Szwecja postanowiły wprowadzić przepisy ograniczające wolność słowa w Internecie i dziś można już zauważyć pewne efekty takich działań.

Stany Zjednoczone znajdują się w internetowym impasie. Obywatele ostro reagują na próby ograniczenia wolności słowa. Powstaje wiele projektów ustaw, które proponują m.in. wprowadzenie zakazu publikowania poradników budowy bomb, bardzo rozpowszechnionych w sieci komputerowej Internet. Jednak na razie nie ma co liczyć na konkretne decyzje. Po zamachu bombowym w Oklahomie Stany Zjednoczone zaczęły tez uważniej przyglądać się prawicowym organizacjom paramilitarnym. Grupy takie działają we wszystkich 50 stanach USA. Raport wymienia ponad 800 tzw. organizacji patriotycznych, w tym 441 „milicji", czyli ugrupowań o charakterze militarnym(30). Grupy te są ze sobą związane głownie przez siec komputerowa (dzielą się wiedza o sposobach unikania płacenia podatków czy przepisami na temat konstrukcji bomb). Niestety jakiekolwiek próby wkroczenia w ich działalność są w znacznym stopniu blokowane przez zakaz wprowadzenia nawet bardzo ograniczonych form cenzury w USA.

Równie poważnym, jeśli nie groźniejszym problemem są ataki przeprowadzane przy pomocy urządzeń wykorzystujących najnowsze technologie. Terrorysci i hackerzy często posługują się systemami telefonii komórkowej i przywoławczej. W 1997 roku, na skutek włamania do sieci Białego Domu, służbowe pagery odbierały tylko wiadomości wysyłane przez hackerów˘. Internetowi przestępcy atakują obiekty wojskowe, rządowe, ale również służby cywilne, przedsiębiorstwa i banki. *„Żadne*

państwo nie może nam stawić czoła na konwencjonalnym polu walki. Ale nowe zagrożenia pojawiają się ze strony tych, którzy atakują cywilne i militarne struktury, w wielu miejscach stanowiące jedność – stwierdził Arnaud de Borchgrave, jeden z autorów raportu o cyberterroryzmie, opracowanego na zlecenie amerykańskiego Centrum Studiów Międzynarodowych i Strategicznych”(31).

Z raportu wynika, ze nagły rozwój technologii informatycznych jest w stanie zagrozić wszystkim, do których można uzyskać dostęp przez Internet. Szczególnie narażone są dziedziny takie jak:

- **zarzadzanie ruchem kolejowym i lotniczym** (chociażby fakt istnienia urządzenia oferowanego przez rosyjska firmę, które zagłusza sygnały GPS {Global Positioning System} w cenie 4000 dolarów, do zakłócenia działanie systemów nawigacyjnych w samolocie wystarczy zwykły telefon komórkowy),
- **przedsiębiorstwa i banki prowadzące działalność w sieci** (najbardziej narażone sa banki, które codziennie przelewają pieniądze w formie elektronicznej z konta na konto, większość firm nie informuje o włamaniach bojąc się utraty zaufania, według ekspertów wszystkie firmy z listy „Fortunne 500” były już obiektami elektronicznych ataków),
- **wszystkie sieci nie przygotowane na nadejście roku 2000** (programiści, którzy przystosowują komputery na zmianę z dwu- na czterocyfrowy system zapisywania roku mogą zostawić na nich własne pułapki, które później ułatwia szpiegowanie lub szantażowanie byłych pracodawców),
- **instytucje użyteczności publicznej,**
- **telekomunikacja,**
- **energetyka.**

Większość cywilnych instytucji posiada dziś systemy komputerowe. Z reguły są one słabo zabezpieczone i podatne na manipulacje z zewnątrz. Dla przeciętnego hackera włamanie do

nich nie jest specjalnym problemem. Atak może być przeprowadzony z bardzo odległego kraju i wykorzystany do zdobycia pieniędzy, ale również do bardzo niebezpiecznych akcji terrorystycznych. Sytuacje pogarsza fakt, ze powstające dziś oprogramowanie „nowej generacji" do szukania luk w systemach zabezpieczeń może być z powodzeniem wykorzystywane nie tylko do naprawiania takich luk, ale również do dostarczania informacji nieodpowiednim ludziom na temat słabych punktów, przez które można podłączyć się do systemu. Narzędzia takie wymagają od potencjalnego włamywacza coraz mniej wiedzy z dziedziny informatyki, czasami wystarczy po prostu wpisać adres i nacisnąć ente.

Administratorzy systemów komputerowych próbują samodzielnie bronić się przed włamywaczami, używając programów monitorujących dostęp do sieci wewnątrz przedsiębiorstwa czy instytucji. W takiej sytuacji każda próba włamania np. przez podanie niewłaściwego hasła, czy wykonanie operacji, do której wykonania nie ma się uprawnień jest natychmiast zapisywana. W każdym momencie można sprawdzić, kto i z jakiego miejsca w świecie próbował się włamać. Dlatego tez poszukiwani są profesjonaliści, którzy potrafią nie tylko włamać się do zamkniętych prywatnych sieci intranetu, ale spowodować w niej określone zakłócenia. Zdaniem amerykańskich ekspertów wojskowych, takie państwa jak Irak, Iran i Libia zatrudniają cyberterrorystów. Ich zadaniem jest penetrowanie i niszczenie sieci komputerowych należących do wojska i służb cywilnych. Istnieją segmenty rynku, które również sponsorują komputerowe włamania i robią to rutynowo. Najczęściej praktyki takie stosowane są przez firmy piszące oprogramowanie i koncerny farmaceutyczne. Spowodowane jest to zazwyczaj olbrzymimi korzyściami płynącymi z wykradania tajemnic handlowych i własności intelektualnej.

Wydawałoby się, ze dostęp do danych wysokiej klasy jest z odpowiednio zabezpieczony. Jednak przeprowadzony w 1997 roku pozorowany atak, przeprowadzony przez agentów Narodowej

Agencji Bezpieczeństwa udowodnił nieskuteczność wszelkich rządowych blokad. Świetnie wyszkoleni agenci NSA (Nasiona Security Agenci) zaatakowali instalacje komputerowa Departamentu Obrony. Nie skorzystali z specjalnie do tego celu spreparowanych, wojskowych programów, posłużyli się oprogramowaniem znalezionym wyłącznie w sieci, dostępnym dla wszystkich internautów. Pięćdziesięciu zatrudnionych do tej pracy agentów włamało się do komputerów Pentagonu w całym kraju, udowadniając, ze komputery Departamentu Obrony są dla prawdziwych hackerów łatwym celem. Agenci dostali się m. in. do dowództwa US Pacific Komand na Hawajach. Dowództwo to zarządza ponad 100 tys. żołnierzami w rejonie Azji. Az strach pomyśleć, co by się stało, gdyby nie był to atak pozorowany.

Tymczasem hackerzy właśnie najchętniej włamują się do pilnie strzeżonych instalacji wojskowych i rządowych. Ataki te przeprowadzają różnorodni ludzie – od młodych chłopców powodowanych pragnieniem zwyklej satysfakcji do cyberterrorystów, dla których jest to dobry sposób na walkę lub realizowanie poleceń swoich wojskowych przełożonych(32). Dane samego Pentagonu wykazują 250 tysięcy prób włamania się do ich komputerów. Nie podają jednak, ile z nich zakończyło się powodzeniem. Wiadomo jednak, ze już wykradziono i zniszczono wiele istotnych danych i oprogramowania. Sposób był prosty – hackerzy zainstalowali tzw. „tylne drzwi” w systemach komputerowych, przez które niezauważalnie podłączali się do ważnych systemów obronnych. Jednocześnie zniszczyli cały system, uniemożliwiając prace wszystkim jego użytkownikom.

Stany Zjednoczone poważnie traktują problem wzmacniania zabezpieczeń zakładanych na sieci o wysokim znaczeniu dla państwa. Można sadzić, ze amerykańska administracja zaczyna dostrzegać niebezpieczeństwo, jakie wynika z uzależnienia sprawnego funkcjonowania państwa od słabo chronionych i narażonych na ataki sieci komputerowych. Tegoroczny budżet Stanów Zjednoczonych przewiduje 10 mld dolarów na walkę z terroryzmem. Z tego niemal 1, 5 miliarda dolarów

przeznaczonych jest na obronne przed atakami hackerów i cyberterrorystów. Suma ta jest o 40% większa niż dwa lata temu, jednak w dalszym ciągu zbyt mała, aby rzeczywiście wykorzystanie jej przyniosło zauważalne efekty. Istnieje zagrożenie, ze terroryści Beda próbować używać komputerów do przerwania linii zasilania, bankowości, komunikacji i transportu, policji, straży pożarnej i ochrony zdrowia, a także instalacji obronnych. Systemy te są już dziś oparte na sieciach komputerowych, a jednocześnie niedofinansowane, wiec szczególnie narażone na ataki cyberterrorystów.

W epoce informacyjnej nikt już nie korzysta z papierowych pieniędzy przy manipulowaniu dużymi sumami. Dzięki internetowi, modemowi i faksowi pieniądze (również nielegalnie zdobyte) mogą przemieszczać się z duża szybkością z jednego konta na drugie. Najczęściej dzieje się to pod przykrywka spółek „off skore", czyli spółek, których jedynym celem jest oszukanie urzędu skarbowego. Firmy off skore, czyli „spółki poza wodami terytorialnymi" znajdują się daleko od kraju macierzystego, gdzie zainteresować mogłyby się nimi organy śledcze i są najczęściej kontrolowane przez „czcigodnych, honorowo powołanych powierników". Oszuści są dzisiaj prawie całkowicie bezkarni.

Również konkretne ugrupowania terrorystyczne często z dużym powodzeniem poszukują funduszy przez Internet. Ogłoszenia tego typu podane wprost lub w zafoliowanej formie trafiają do potentatów finansowych, którzy życzą sobie nieoficjalnie wspierać nielegalne działania.

Jednak nie zawsze ostrze Internetu wymierzone jest w stróży prawa. Internetowa strona Departamentu Stanu www.heores.com obiecuje wszystkim, którzy chcieliby złożyć donos pomagający w ujęciu terrorystów: *„Możemy dać ci 4 miliony powodów, by powstrzymać terroryzm*". Rzeczone 4 miliony to oczywiście suma, jaka można otrzymać za informacje, które doprowadzają do ujęcia poszukiwanego. W wielu przypadkach jest to jednak kwota o wiele wyższa. Strona zawiera szczegółowe informacje o

nagrodach wyznaczanych przez rząd amerykański za pomoc w zdobyciu informacji o przestępcach, fałszerstwach dokumentów i pieniędzy oraz zamachach terrorystycznych. Jest ona dostępna w dziesięciu jeżykach (angielskim, niemieckim, francuskim, włoskim, hiszpańskim, portugalskim, greckim, tureckim, japońskim, arabskim i farsy). Znajdują się na niej również opisy zamachów terrorystycznych, poszukiwanych osób, przede wszystkim daty, nazwiska i fakty. Strona ta i program HEROES, który propaguje, cieszy się dużym zainteresowaniem, dlatego, ze oprócz pieniędzy oferuje również program identyczny z programem ochrony świadków (nowa tożsamość). Jest on skutecznym narzędziem w walce z terroryzmem.

Można przypuszczać, ze w przyszłości wiele grup nacisku będzie podejmować próby włamywania się do sieci w celu zniekształcenia wyników wyborów w niej się odbywających. Może to skutkować zmniejszeniem zaufania obywateli do narzędzi społeczeństwa informacyjnego. W rezultacie mogłoby doprowadzić do obniżenia aktywności społecznej, która jest podstawowym wykładnikiem skuteczności demokracji uczestniczącej. Grupy przestępcze przy pomocy sfałszowanych glosowań mogłyby umieszczać własnych kandydatów politycznych w strategicznych miejscach, sztucznie wspierać poparcie społeczne dla prywatnie finansowanych inwestycji, atakować serwery przeciwnych partii. Sytuacja ta podważyłaby zaufanie do sieci informacyjnej i hamowała rozwój „informacyjnej demokracji uczestniczącej". Należy zastanawiać się nad zdecydowanym wzmacnianiem bezpieczeństwa w sieci. Konieczne jest wprowadzenie podziału na:

- dostępne powszechnie informacje,
- informacje dostępne użytkownikom uprawnionym (po autoryzacji).

Należy wiec wprowadzić autoryzacje użytkowników (osób fizycznych lub prawnych) a nie terminali włączających się do systemów teleinformacyjnych. Jednocześnie szczególne opieka już dziś należy otoczyć:

- kontrole przekazów kodowanych,
- informacje personalne użytkowników sieci,
- ochronne „elektronicznego pieniądza”,
- ochronne tajemnicy medycznej,

Ochronne obywateli przed „cyberprzestępcami” utrudnia brak jakiejkolwiek kontroli, które pozwoliłyby na kontrole przesyłania informacji w sieci, które wyeliminowałyby możliwość jej wykorzystania przez organizacje terrorystyczne. Wolność słowa musi zostać w Internecie ograniczona z uwagi na szeroko pojęte dobro społeczne, tak, aby można było jawnie występować przeciw propagowaniu wartości fundamentalistycznych lub faszystowskich.

Reasumując chcemy podkreślić, ze przed społeczeństwem ziemskim pojawia się szansa na zrealizowanie pewnego rodzaju utopi – jest to możliwe dzięki szerokim możliwościom proponowanym przez techniki teleinformacyjne.

Tak naprawdę, nikt nie wie, do czego tak wielki potencjał tkwiący w ludzkiej twórczości może doprowadzić. Sygnał emitowany przez ziemie dociera dużo dalej niż jesteśmy w stanie to sobie wyobrazić. Dookoła ziemi krążą satelity wspomagające komunikacje. A od wynalezienia telefonu minęły zaledwie 123 lata, od skonstruowania pierwszego komputera 53 lata. Trudno zrozumieć, co działo się wcześniej. Jak to możliwe, ze przez setki lat nauka sennie pełzła powoli nie przejmując się losem ludzkim, aby nagle niecałe 150 lat temu wystrzelić do przodu niosąc ze sobą tak ogromne możliwości i tak wiele zagrożeń.

Mocarstwa współczesnego świata – Stany Zjednoczone, państwa Unii Europejskiej i Chiny – jednomyślnie proklamują nadejście ery informacji. Zróżnicowanie ideowe pojawia się dopiero w sposobie podejścia do tej kwestii. „Ameryka” i „Europa” chcą realizować idee społeczeństwa informacyjnego przez stworzenie struktur demokracji bezpośredniej i samorządności. Władze Chin pragną wyodrębnić z współczesnych zmian tylko jeden element –

rewolucje techniczna, cala resztę natomiast – jako niebezpieczna ideowo – zastąpić poprawa sytuacji ekonomicznej społeczeństwa. W moim przekonaniu jednak, nadejście społeczeństwa informacyjnego jest w dużej mierze procesem oddolnym i naturalnym, a również koniecznym następstwem rewolucji telekomunikacyjnej. Tak wiec wszelkie próby blokowania zmian skazane są na niepowodzenie.

Czy era, której nadejście postuluje tylu wielkich tego świata nadejdzie. Przyszłość pozostaje nieznana dopóki się nie zdarzy i zawsze jest szansa na cos zaskakującego, cos czego my się nie spodziewali. Jednak sama myśl, co stworzymy w następnym tysiącleciu, skoro ostatnie 150 lat przyniosło nam tak wiele, pozwala wierzyć w Człowieka i być optymista.

---

(28) Koscielniak P., Nienawiść na WWW, „Rzeczpospolita" z dnia 17.11.97.

(29) ibidem.

(30) Walczak S., Strach przed żółta ciężarówka, „Rzeczpospolita" z dnia 20.04.96.

(31) Koscielniak P., Klawiatury zamiast bomb, „Rzeczpospolita" z dnia 04.02.99.

(32) Najsłynniejsi to król hackerów Kevin Mitnick i nieco mniej znany Julio Cesar Ardita., który włamał się m.in. do systemów Departamentu Obrony, Zarządu Morskiego, Lotniczego i Kosmicznego, Dowództwa Sil Morskich, ośrodka NASA w Pasadena i laboratorium w Los Alamos.

Internet w sytuacji kryzysowej – wojna w Kosowie

świetna praca magisterska o społeczeństwie informacyjnym

Internet, w odróżnieniu od radia i telewizji nie poddaje się zbyt łatwo kontroli jednej opcji politycznej. Dopóki istnieje w kraju sprawna łączność (która dziś mogą zapewnić satelity) nic nie może powstrzymać funkcjonowania sieci komputerowej. Jest najszybsza w przekazywaniu relacji naocznych świadków i raportów, daje również możliwość leczenia tekstów, filmów, map i zdjęć w jedna multimedialna całość. W sieci mogą znaleźć się informacje o przyczynach i przebiegu wojny. Dlatego tez Internet stal się w Kosowie jedynym źródłem niezależnej informacji, pomimo cenzury, wydalenia niemal wszystkich zagranicznych dziennikarzy i monitorowania informacji – dzięki niemu z terenów ogarniętych wojna nie przestały przez cały czas trwania konfliktu napływać informacje.

Siec internetowa sprawdziła się w warunkach kryzysowych. Podczas konfliktu w Kosowie stalla się najsprawniej funkcjonującym medium przekazującym informacje z objętych działaniami wojennymi obszarów. Informacje pojawiały się na stronach World Widea Web, zamieszczane tam również były opisy i zdjęcia, informatorzy korzystali z list dyskusyjnych i poczty e-mail. W Internecie działały rozgłośnie radiowe, z których cześć prezentowała repertuar wyłącznie albański. Internet stal się w Kosowie „częścią pola bitwy”.

O działaniach Serbów dowiedzieć się można było zarówno z

oficjalnych stronach rządowych i ze stron WWW prowadzonych przez Albańczyków. Serbskie Ministerstwo Informacji posiadało własna stronę internetowa serbia-info.com , aktualizowana kilka razy w ciągu dnia. Również Ministerstwo Spraw Zagranicznych www.smip.sv.gov.yu prowadziło serwis informacyjny, przedstawiając zniszczenia na obszarach zajmowanych przez Serbów. Strony o kryzysie w Kosowie znajdowały się również na serwerze NATO. Fakty były przedstawiane w obu przypadkach odmiennie. *„Obserwujemy prawdziwa walkę propagandowa prowadzona na różnych stronach World Widea Web.”* – powiedział agencji Reuters Richard Din Nick – *„Strony należące do NATO były nawet atakowane przez hackerów, wysłano na nie ok. 2 tys. listów e-mail, z których cześć zawierała wirusy. Po wytropieniu nadawców, okazało się, ze listy te pochodziły z Belgradu”*(26).

Informacje wysyłane przez Internet zyskały szczególne znaczeniu, gdy władze Jugosławii uniemożliwiły prace reporterów i dziennikarzy państw zachodnioeuropejskich, a w szczególności członków NATO. Wtedy to, Albańczycy i Serbowie komunikujący się ze światem przez siec, stali się jednym z ważniejszych źródeł informacji. Najwięcej było pisemnych raportów i relacji świadków. Mimo wstrzymania wydawania ostatnich albańskich gazet w Kosowie: „Kosowa Sto” i „Koha Ditore”, w sieci znajdowała się treść ostatniego wydania jednej z nich z dnia 13 marca, w którym redakcja zgłasza protest przeciwko *„nieuczciwym metodom wykorzystywanym przez serbski rząd”*(27).

W Internecie działało radio i telewizja, można było codziennie oglądać i słuchać raporty z Kosowa, tworzone przez stacje radiowo-telewizyjna z Prisztiny RTPSAT. W sieci funkcjonowały również: kosowskie Radio 21 pod adresem www.radio21.com , oraz niezależna stacja B92 www.b92.net/b92/live/live.html . Kończyła ona swoja audycje radiowa słowami, które głęboko zapadają w pamięć: *„Prosimy wszystkich, aby o ile to możliwe wykorzystywali Internet w utrzymywaniu stałego kontaktu z*

nasza stacja, przesyłania bieżących informacji z różnych stron Jugosławii na temat aktualnej sytuacji, zniszczeniach, ofiarach, rannych. Jeżeli jesteście w stanie, to podawajcie ich nazwiska…”. Radio B92 wykorzystywało technologie Real Audio, nadawało w jeżyku angielskim i serbskim. Program B92 był retransmitowany przez mirrory na całym świecie oraz stacje w Amsterdamie i stacje austriacka. Dziennikarze Radia B92 publikowali również serwis informacyjny w jeżykach serbskim i angielskim, wzbogacony często o krótkie sekwencje wideo prezentujące codzienne zżycie mieszkańców Belgradu oraz sceny z nocnych bombardowań miasta. W sieci działało również internetowego forum WWW Stevena Cliffa będące kolejnym, niezależnym źródłem informacji o sytuacji w Kosowie. Steven Cliff jest Amerykaninem, aktywista ruchu liberalnego z Minnesoty. Na jego adres pisali wszyscy, kosowscy Albańczycy, Serbowie, oraz internauci z całego świata.

Ojciec Sawa Janic „Cyceron”, z klasztoru w kosowskiej wiosce Visowi Decami informował przez Internet o aktualnej sytuacji w Kosowie i reszcie kraju. Nawiązywał on kontakt z reszta świata przez e-mail, irc oraz własna listę dyskusyjna. Jego doniesienia przytaczało wiele agencji prasowych i gazet. Często pochodziły one wyłącznie od niego. Ojciec Sava pragnął przede wszystkim pomagać ludziom. Każdego dnia otrzymywał dziesiątki listów od rodzin i ludzi, których bliscy pozostali w Kosowie. Media podawały tylko liczby, internauci poszukiwali konkretnych ludzi. Własna lista dyskusyjna ojca Savy, która spełniała role forum dla dialogu miedzy obiema stronami konfliktu, publikowała wiadomości z mediów albańskich i kosowskich. Na stronach WWW / ojciec Sava prowadził serwis informacyjny „Kosowo Daily News”, na którym znajdowały się doniesienia światowych agencji prasowych, relacje z kraju oraz wiele adresów innych stron o podobnej tematyce. Strony te nie zawierały za to nacjonalizmu i propagandy wojennej, tak często spotykanych na wszystkich innych stronach internetowych.

Raporty wysyłały w świat również Kosowa Press

www.kosovapress.com , oraz jugosłowiańska agencja Tanjug. Raporty Kosowa Press dotyczyły dokładnych miejsc operacji serbskich wojsk. Strona Kosowa Info www.kosovainfo.com zawierała relacje naocznych świadków ataków NATO i Serbów, kolorowe zdjęcia i wiadomości z innych stron WWW. Na stronie Tanjug inet.co.yu/kamera można było zobaczyć jedna z ulic Belgradu zbombardowana przez NATO. Informacje o historii i kulturze Kosowa są dostępne na jugosłowiańskiej stronie rządowej gov.yu.

Paradoksalnie największym zagrożeniem zespołów informacyjnych działających w Internecie nie był rząd Miloszevicia, lecz bombardowanie NATO. Rządowi za bardzo zależało na sieci, z którego korzystał w celach propagandowych. Serbskie władze mogły jedynie ograniczyć wolność słowa przez ograniczanie publicznego dostępu do Internetu np. na uczelniach czy w cyberkawiarniach, nie były jednak w stanie kontrolować indywidualnych użytkowników domowych komputerów. Jednocześnie serbskie oddziały dywersyjne cały czas z dobrym skutkiem atakowały strony i serwery amerykańskie i natowskie. Udało im się na cały weekend zablokować oficjalna stronę główna Białego Domu. Hackerzy atakowali również inne strony w Stanach umieszczając na wszystkich niewybredne teksty. Z dużym skutkiem uderzyli na główny natowski serwer www.nato.int . Serbscy hackerzy wysłali pod adresem serwera tak duża liczbę informacji ze ten nie był w stanie ich przetworzyć i przestał działać na cały dzien. Strona NATO była niedostępna cały dzien. Dywersanci umieszczali również wirusy na wrogich stronach. Jednocześnie częste ataki odpierała również strona radia B92, której audycje często próbowano zawiesić.

Konflikt w Kosowie był wielkim sprawdzianem dla Internetu. Udowodnił, ze siec to nie tylko ułatwienie zżycia, ale również śluzy obronie wolności, walce z agresja wyniszczająca ludzi. Dzięki internetowi świat mogli poznać informacje o „z pola walki”, padały nazwiska, nazwy spacyfikowanych wiosek kosowskich, pojawiały się bezpośrednie relacje mieszkańców

jugosłowiańskich miast bombardowanych przez natowskie samoloty. E-mail wysłany z kawiarni internetowej w Prisztinie ostrzegł światowe media, ze Serbowie polują na kosowskich współpracowników misji OBWE i rozstrzeliwują ich. Specjalnie dla wszystkich, którzy chcieli skorzystać z Internetu aby podać informacje z obszaru ogarniętego wojna powstały specjalne serwisy anonimowej poczty e-mail, umożliwiające anonimowe przeslanie informacji, np. specjalna strona-bramka Kosowo Pracy Project anonymizer. com/Kosowo. W formularzu nadawca wpisuje adres odbiorcy oraz treść wiadomości, która jest następnie przesyłana za pośrednictwem bezpiecznego protokołu HTTPS. Władze są w stanie ustalić jedynie, ze wiadomość została wysłana za pośrednictwem serwisu anonimowej poczty – zarówno jego treść, jak i nadawca zostaną nieznani.

---

(26) Koscielniak P., Propagandowa wojna w sieci, „Rzeczpospolita” z dnia 13 kwietnia 1999.

(27) ibidem.