STREFA STUDENTA

Michał Pochopień - SPECJALISTYCZNY SYSTEM ZABEZPIECZEŃ WOJSKOWYCH „ECHELON”[113]

Abstract

Echelon started probably in the nineteen-seventies, although very few people knew of its existence, just as is the case with the existence of the NSA. Echelon intercepted all signals coming overheard via telecom links. However, a significant increase in the amount of information transmitted via the Internet prompted the NSA in the early nineties to expand the arsenal of methods specifically aimed at the Internet in order to observe the network.

Key word: Echelon, NSA, Internet, overheard

Abstrakt

Artykuł przedstawia zagadnienie globalnej sieci wywiadowczej Echelon. System powstał przy udziale Stanów Zjednoczonych, Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii w ramach porozumienia AUSCANNZUKUS i jest zarządzany przez amerykańską służbę wywiadu NSA. Echelon posiada w całym świecie urządzenia techniczne do przechwytywania (podsłuch) wiadomości w kanałach telekomunikacji.

Key words: Echelon, NSA, Internet, podsłuch

Priorytetem wielu amerykańskich agencji, głównie wojskowych takich jak National Security Agency, zajmujących się bezpieczeństwem państwa stało się opracowanie systemu i oprogramowania pozwalającego na wykrywanie informacji dotyczących bezpieczeństwa państwa. W National Security Agency powstał Projekt Trailblazer, którego celem było stworzenie systemu łamiącego wszelkiego rodzaju zabezpieczenia. Najważniejszym „dzieckiem” NSA jest jednak oczywiście Echelon.

NSA powstała w 1952 roku i zajmuje się przede wszystkim wywiadem technicznym, kryptologią i łamaniem szyfrów. Przez lata o jej istnieniu wiedzieli tylko nieliczni. Nadal należy zresztą do najbardziej strzeżonych tajemnic amerykańskich służb specjalnych, a naczelnym hasłem agencji jest: *serving in silence* („służyć w milczeniu”).

NSA koordynuje i kieruje operacjami w celach obrony systemów teleinformacyjnych Stanów Zjednoczonych. Zatrudnia najlepszych specjalistów od ochrony i łamania zabezpieczeń. Stąd wynikają dwa główne zadania agencji: dbanie o zachowanie integralność systemu informacyjnego Stanów Zjednoczonych oraz szukanie dziur w systemach innych państw. NSA czuwa, aby do rządowych systemów informacyjnych nie miały dostępu osoby do tego nieupoważnione. Ochrona ta rozciąga się od najwyższych szczebli rządowych do pojedynczych jednostek wojskowych.

[113]Praca jest fragmentem pracy licencjackiej Pana Michała Pochopienia - studenta WSBPiI „Apeiron” w Krakowie: *Administrowanie bezpieczeństwem systemów i sieci teleinformatycznych w jednostce organizacyjnej sił zbrojnych* napisanej pod kierunkiem dra Jerzego Depo.

Domeną NSA jest tzw. wywiad sygnałowy (signal *intelligence,* SIGNIT) co stanowi specyficzną formę wywiadu informacyjnego i obejmuje: wywiad komunikacyjny (COMINT), wywiad elektroniczny (ELINT) oraz wywiad telemetryczny (TELINT). W 1966 roku agencja w ramach projektu Signals Intelligence, rozpoczęła budowę największej obecnie na świecie stacji nasłuchowej Menwith Hill w brytyjskiej miejscowości North Yorth Moors. Kilkanaście lat wcześniej w 1947 roku doszło bowiem do zawarcia porozumienia nazywanego UKUSA między Stanami Zjednoczonymi a Wielką Brytanią do którego później przyłączyły się Australia, Kanada i Nowa Zelandia. Państwa te porozumiały się w kwestii budowy sieci stacji nasłuchowych przez które przechodzą wszystkie rozmowy tele- i radiofoniczne oraz faksy. Tak powstał Echelon, który z czasem został wykorzystany do monitorowania ruchu w Internecie.

Każda stacja odpowiada za inną część świata, a co za tym idzie — na grupę satelitów telekomunikacyjnych. Minuta po minucie, dwadzieścia cztery godziny na dobę miliony wiadomości trafiają do takich stacji. W obiektach Menwith Hill, nazwanych kryptonimem F83, zajmuje się nimi skonstruowany przez koncern Lockheed potężny system komputerowy „Silkworth*"*. Jedną z jego części jest Magistrand - podsystem odpowiedzialny za przeszukiwanie mowy i tekstu. Najpierw jednak wiadomości mówione zamieniane są na postać tekstową. Narzędzie firmy Memex nazywane „Pathfinder", na podstawie skomplikowanych algorytmów wyszukuje słowa, daty, liczby lub ich kombinacje, które wcześniej zostały zdefiniowane przez wywiadowców w systemie nazwanym „Dictionary*"*. System potrafi także przeszukiwać wiadomości pod kątem występowania w nich głosu wybranej osoby. Jeżeli tylko dana sekwencja pojawia się w przekazywanej wiadomości zostaje oznaczona i poddana szczegółowej analizie. Następnie dane mogą być przesłane do centrali.

Echelon ruszył prawdopodobnie w latach siedemdziesiątych, chociaż o jego istnieniu podobnie jak o istnieniu samej NSA wiedziało bardzo niewiele osób. Pierwsza wzmianka o tym projekcie trafiła do opinii publicznej w sierpniu 1988 roku, kiedy to Duncan Campbell opublikował w „New Statesman" raport na temat bazy Menwith Hill. Nie spotkał się on jednak z dużym odzewem. Dopiero książka Nowozelandczyka Nicky'a Hagera „Secret Power: New Zealand's Role in the International Spy Network*"* wzbudziła ogromne zainteresowanie. Do dziś uważana jest za jedno z podstawowych źródeł informacji dotyczących Echelona.

Do 1990 roku Internet nie był właściwie obiektem szczególnego zainteresowania programu Echelon. Ruch internetowy przechwytywano niejako „przy okazji" ogółu sygnałów płynących podsłuchiwanymi łączami telekomunikacyjnymi. Jednak znaczny wzrost ilości informacji przesyłanych za pośrednictwem Internetu skłonił NSA, na początku lat dziewięćdziesiątych do rozbudowy arsenału stosowanych metod podsłuchu o metody specyficznie internetowe jak sniffing sieci. Znany jest fakt zainstalowania przez NSA w 1995 roku oprogramowania typu sniffer, przechwytującego wszystkie przesyłane pakiety danych w dziewięciu głównych węzłach szkieletu amerykańskiego Internetu, przez które w owym czasie przechodziła znaczna część ruchu internetowego przebiegającego do/z lub poprzez USA.[114]

Obecnie większość amerykańskich operatorów Internetu rozbudowała strukturę połączeń alternatywnych. Wcale to jednak nie oznacza, że internetowy ruch nie jest monitorowany.

Państwa nie mają nic przeciwko temu aby przechwytywać informacje pochodzące od terrorystów, obawiają się jednak, iż system wykorzystywany jest także do kontroli politycznych, biznesowych i prywatnych aspektów życia zwykłych obywateli. Znane są przypadki, że europejskie koncerny (m.in. Airbus, Volkswagen) nagle były wypierane przez amerykańskich konkurentów - Boeinga i GM. Możliwe więc, że Echelon został użyty przez USA dla celów wywiadu gospodarczego. Sprawa ta trafiła na forum Unii Europejskiej. Podczas pierwszej debaty na ten temat w Parlamencie Europejskim w 1998 roku stwierdzono: „Jeżeli system ten rzeczywiście istnieje, byłby to nie akceptowalny atak na wolności obywatelskie, konkurencję i bezpieczeństwo państw".

[114]J. Rafa, *Złowrogi Echelon* ,http://ultra.wss.krakow.pl/papers/echelon.html z dnia 23.08.2007.

W lutym 2000 roku D. Campbell przygotował, na zlecenie UE, raport - „Interception Capabilities 2000". Brytyjski dziennikarz wprost stwierdzał, że europejskie łącza są podsłuchiwane, i że uzyskane w ten sposób informacje są wykorzystywane przez amerykańskie koncerny do nieuczciwej konkurencji.[115] Pod wpływem raportu Parlament Europejski powołał w czerwcu 2000 roku specjalną komisję, mającą zbadać sprawę Echelona. W maju 2001 roku członkowie komisji złożyli wizytę w Stanach Zjednoczonych. Jednak w ostatniej chwili swoje spotkania z nimi odwołali zarówno przedstawiciele CIA, jak i NSA.

W przygotowanym raporcie jednoznacznie stwierdzono, że globalny system podsłuchiwania cywilnych połączeń telekomunikacyjnych istnieje i jest utrzymywany przez państwa związane porozumieniem UK-USA.[116] Parlament Europejski przyjął raport, jednak dalsze śledztwo jest utrudnione z przyczyn obiektywnych. Wielka Brytania jest bowiem sygnatariuszem porozumienia dotyczącego Echelona, zaś Francja posiada własny system - Frenchelon w Domme i Nowej Kaledonii. W dodatku brytyjska organizacja Statewatch twierdzi, że w Unii Europejskiej od 1991 roku trwają prace nad stworzeniem podobnego do Echelona systemu inwigilacji.

Można powiedzieć, że państwa są nie tyle zaniepokojone samym zjawiskiem podsłuchiwania i kontroli wiadomości ile ich skalą. Przede wszystkim dlatego Echelon traktowany jest przez wiele osób za system niezwykle niebezpieczny.

Kolejnym sposobem na walkę z „miękkim" cyberterroryzmem jest Carnivore („Mięsożerca", oficjalna nazwa - DCS 1000), program komputerowy powstały w latach dziewięćdziesiątych, umożliwiający automatyczne kontrolowanie korespondencji elektronicznej. Opracowali go specjaliści FBI z Marcusem Thomasem na czele.

Federalne Biuro Śledcze szybko zdało sobie sprawę, że Internet stwarza ogromne możliwości komunikowania się niemożliwe do inwigilacji tradycyjnymi metodami wywiadowczymi. Dzięki globalnej sieci policja federalna stała się nagle niemal zupełnie „ślepa". Dlatego też zdecydowano o stworzeniu Carnivore choć jego działalność budzi wiele kontrowersji wśród obrońców praw człowieka.

W czerwcu 2001 roku „Mięsożerca" zademonstrowany został na spotkaniu Stowarzyszenia Przemysłu Telekomunikacyjnego (Telecommunications Industry Association), nie wzbudziło to jednak zainteresowania prasy. Rozgłos zdobyła dopiero sprawa dostawcy usług internetowych Yerio. Kiedy kontrolowana w 53% przez Japończyków firma NTT Communications wystąpiła z ofertą wykupienia za 5,5 miliarda dolarów amerykańską firmę, FBI wyraziło publicznie zastrzeżenie, że oddanie firm łącznościowych pod zagraniczną kontrolę może utrudnić agentom federalnym kontynuację podsłuchu. Amerykańska Unia Swobód Obywatelskich (American Civil Liberties Union - ACLU) wystąpiła na początku lipca 2001 roku ze skargą do Podkomitetu Prawnego Izby Reprezentantów twierdząc, że poczynania FBI w Internecie „podnoszą nowe pytania natury prawnej, które krzyczą o uwagę Kongresu". Do ACLU dołączyło się Centrum Elektroniczne Informacji Prywatnej (Electronic Privacy Information *Center* - EPIC) i inne organizacje strzegące obywateli przed nadużyciami władzy państwowej. W ten sposób afera „Mięsożercy" trafiła na łamy prasowe.[117]

Reakcja Kongresu na głosy krytyki pod adresem Carnivore była stosunkowo szybka i już 24 lipca wysokiej rangi przedstawiciele FBI i Departamentu Sprawiedliwości zostali wezwani na spotkanie z grupą kongresmanów, którzy nie ukrywali swego zaniepokojenia. Problem z nowym systemem elektronicznego podsłuchu — twierdzili niektórzy z nich: wiąże się z tym, że po to aby wydobyć ze strumienia danych informacje, do których przechwycenia FBI zostało przez sąd upoważnione, Carnivore przecedzić musi masę innych informacji, których prywatność chroniona jest prawem. Specjaliści FBI twierdzą jednak, że są w stanie z „chirurgiczną" dokładnością wyselekcjonować te informacje, które

[115]W. Campbell, *Interception Capabilities 2000,* Edinburgh, 1999.
[116]http://www.europarl.eu.int/tempcom/echelon/pdf/rapport_echelon_en.pdf z dnia 23.08.2007.
[117]K. Szymborski, *Mięsożerca w Internecie*, „Wiedza i życie", styczeń 2001.

niosą zagrożenie dla państwa lub są przejawem poważnej działalności przestępczej. Analizowane są tylko te informacje, które są dopuszczone przez prawo do inwigilacji. Pozostałe pozostają „nietknięte".

Prawdziwy kłopot to fakt, że rzetelne rozstrzygnięcie kwestii, czy użycie Carnivore narusza, czy nie narusza tajemnicy korespondencji wymagałoby od FBI publicznego ujawnienia kompletnego kodu programu. A to, zdaniem Biura, oznaczałoby oddanie systemu na żer hakerów i całkowite pozbawienie go skuteczności.

Po zamachach terrorystycznych w Stanach Zjednoczonych amerykański Senat zezwolił FBI na korzystanie z tego kontrowersyjnego systemu inwigilacji. Senatorowie stwierdzili, że stosowanie Carnivore może przyczynić się do wykrycia sprawców tych ataków oraz ułatwi zapobieganie kolejnym aktom terroru. Korzystając z tego przyzwolenia FBI zapowiedziało, że pracuje nad unowocześnieniem systemu o funkcję instalowania na podejrzanych komputerach konia trojańskiego, „magiczna latarnia" *(magic lantern).* Program ten rejestruje i przesyła swym autorom informacje o naciśniętych przez użytkownika klawiszach, co ma pomóc w wykradaniu haseł i innych wiadomości z komputerów obserwowanych osób. „Magiczna latarnia" powstała w celu rozwiązania jednego z pierwszoplanowych problemów nękających agentów FBI monitorujących sieć. Okazała się nim wspomniana wcześniej wysoka skuteczność programów szyfrujących, które pozwalają wielce efektywnie zakodować wiadomości. Bez znajomości klucza nawet FBI ma kłopoty ze złamaniem szyfru.
Według opublikowanych informacji „oficjalny" trojan niepostrzeżenie instaluje się na komputerze ofiary korzystając ze znanych furtek w systemie operacyjnym, po czym przejmuje kontrolę nad maszyną.

Unowocześniony Carnivore miał być jeszcze lepszym narzędziem od Echelona do walki z cyberterroryzmem. Jednak przydatność „Mięsożercy" została podważona 24 maja 2002 roku, kiedy EPIC ujawniło wewnętrzną notatkę FBI z 5 kwietnia 2000 roku. Okazało się, że system nie działa poprawnie gdyż przechwytywał nie tylko informacje dopuszczone przez prawo ale także takie, których agenci federalni zbierać nie mieli upoważnienia. W konsekwencji tego zdarzenia trzeba byto wyrzucić wszystkie zapisy z poczty elektronicznej z marca 2000 roku. Podobnych wypadków mogło być więcej. Możliwe że wśród nieprawidłowo przechwyconej korespondencji były informacje o planach ataków terrorystycznych na Nowy Jork i Waszyngton.

Wprawdzie ujawnione informacje nie sugerują, że FBI mogło w jakikolwiek sposób zapobiec atakom, ale pokazują jak niedoskonały jest „Mięsożerca". Wynika z tego, że FBI wprowadzało w błąd Kongres i opinie publiczną twierdząc, że Carnivore jest zdolny do zbierania tylko autoryzowanych informacji.

Bibliografia

1. Adamski J., *Nowe technologie w służbie terrorystów*, Wydawnictwo TRIO, 2007.
2. Amoroso G. E., *Fundamentals of Computer Security Technology*, Upper Saddle River, (NJ) 1994
3. Campbell W., *Interception Capabilities 2000*, Edinburgh, 1999.
4. Ciborowski L., *Walka informacyjna*, Toruń 1999
5. Cohen F.B., *Protection and Security on the Information Superhighway*, New York 1995.
6. Denning D. *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.
7. Doroziński D., *Hakerzy. Technoanarhiści cyberprzestrzeni*, Gliwice 2001.
8. Howard J.D. Longstaff T.A., *A Common Language for Computer Security Incidents*, Springfield 1998.
9. Schwartau W., *Information Warfare, Cyberterrorism: Protecting your personal security in the electronic age*, Thunder's Mouth Press, 2nd ed, (1996).
10. Szymborski K., *Mięsożerca w Internecie*, „Wiedza i życie", styczeń 2001.

Strony WWW

1. http://www.hacking.pl/news.php?id=1187 z dnia 14.04.1009
2. http://www.election99.com z dnia 02.02.2010
3. http://www.ng.ru/ideas/2000-05-26/8_context.html z dnia 08.04.2009
4. Terrorism Act 2000; http://www.homeoffice.gov.uk/terrorism/ z dnia 19.02.2001
5. http://www.kongres.org.pl/on-line/1-szy_kongres/raport.html z dnia 12.12.2009
6. http://www.kongres.org.pl/on-line/2gi_kongres/raport/Raport.html z dnia 08.05.2007
7. http://www.kbn.gov.pl/cele/raporty/index.html z dnia 3.07.2009
8. Decision No1336/97/EC of the Parlament of the Council of the 17 June of 1997 on series of Guidelines for Trans-European
9. Rafa J., „Złowrogi Echelon", http://ultra.wss.krakow.pl/papers/echelon.html z dnia 23.08.2007
10. http://www.europarl.eu.int/tempcom/echelon/pdf/rapport_echelon_en.pdf