helion.pl
KSIĘGARNIA INTERNETOWA · WYDAWNICTWO

IDŹ DO
PRZYKŁADOWY ROZDZIAŁ
SPIS TREŚCI

KATALOG KSIĄŻEK
KATALOG ONLINE
ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK
DODAJ DO KOSZYKA

CENNIK I INFORMACJE
ZAMÓW INFORMACJE O NOWOŚCIACH
ZAMÓW CENNIK

CZYTELNIA
FRAGMENTY KSIĄŻEK ONLINE

Black Ice. Niewidzialna groźba cyberterroryzmu

Autor: Dan Verton
Tłumaczenie: Krzysztof Masłowski
ISBN: 83-7361-364-1
Tytuł oryginału: Black Ice.
The Invisible Threat of Cyber-Terrorism
Format: B5, stron: 336

Jest oczywiste, że cyberterroryzm jest nową twarzą terroryzmu. Minęły już dni, gdy jedynymi ofiarami zamachów byli znajdujący się w zasięgu eksplozji. Dzisiejsi terroryści nauczyli się, że bezpieczeństwo każdego państwa zależy od infrastruktury – komputerów i sieci komputerowych. Strategiczny atak na te systemy miałby niewątpliwie straszne i niszczące konsekwencje dla narodu i gospodarki.

„Black Ice. Niewidzialna groźba cyberterroryzmu" to książka napisana przez Dana Vertona, byłego oficera wywiadu amerykańskiego. Autor śledzi i przedstawia różne postacie cyberterroryzmu, jego globalne i finansowe implikacje, przekraczającego granice naszej prywatności oraz sposoby przygotowania się na cyberataki. Książka jest pełna odkrywczych wywiadów i komentarzy amerykańskich autorytetów ds. bezpieczeństwa narodowego (w tym Toma Ridge'a, Jamesa Gilmore'a, Richarda Clarke'a), przedstawicieli wywiadów CIA i NSA, a nawet zwolenników al-Kaidy wspierających działania jej siatki terrorystycznej.

Książka wnosi wiele do debaty na temat bezpieczeństwa wewnętrznego. Verton przekonywująco argumentuje, że wymiana i udostępnianie informacji wywiadowczych w czasie rzeczywistym jest warunkiem powodzenia działań służb bezpieczeństwa. Tylko w ten sposób można nie dopuścić, by korzystający z najnowszych technologii terroryzm nie stał się pasmem czarnego lodu (black ice) rozciągniętym w poprzek autostrady, o istnieniu którego dowiadujemy się dopiero po utracie panowania nad pojazdem.

O autorze:

Dan Verton jest byłym oficerem wywiadu U.S. Marine Corps i dziennikarzem wyróżnionym wieloma nagrodami. Kilkakrotnie występował w audycjach telewizyjnych agencji informacyjnych, np. CNN, przemawiał w Bibliotece Kongresu i w ONZ jako uznany ekspert w dziedzinie bezpieczeństwa sieci komputerowych, obrony i wywiadu. Jest autorem „Pamiętników hakerów" i starszym członkiem redakcji „Computerworld".

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

8

Wywiad: aby nie było następnego ataku

Ludzie powinni zrozumieć, że nie mamy żadnej czarodziejskiej skrzynki, której istnienie ukrywamy[1].

—William F. Dawson
Zastępca rzecznika Wspólnoty Wywiadowczej USA[2]

UBL [Usama bin Laden] dobrał się do technologii i użył jej szybciej niż my[3].

—Larry Castro
Dyrektor ds. bezpieczeństwa wewnętrznego
w Agencji Bezpieczeństwa Narodowego[4]

---

[1] Wywiad przeprowadzony przez Autora na konferencji Information Sharing and Homeland Security (Udostępnianie informacji i bezpieczeństwo narodowe) w Filadelfii w stanie Pensylwania. Konferencja odbyła się w sierpniu 2002 i była sponsorowana przez Departament Obrony i Wspólnotę Wywiadowczą (Intelligence Community).

[2] Intelligence Community (IC) jest federacją amerykańskich agencji i organizacji zajmujących się wywiadem. Należą do nie np. CIA, wywiad powietrzny, wywiad morski, a także Departament Obrony i wiele innych. Dokładne informacje można znaleźć pod adresem *http://www.intelligence.gov — przyp. tłum.*

[3] Uwagi robione na konferencji Information Sharing and Homeland Security — patrz 1. przypis w tym rozdziale.

[4] National Security Agency (NSA) — *przyp. tłum.*

W południe 11 września nadajnik CNN intensywnie pracował na szczycie dachu kościoła naprzeciw Kapitolu. Tego dnia jednym z wielu gości stacji był kongresman Curt Weldon, starszy członek House Armed Services Committee (HASC), nadzorujący roczny budżet wynoszący 38 miliardów dolarów i przeznaczony na badania oraz rozwój najnowszych technologii wojskowych. Zapytany, jak — jego zdaniem — mogło dojść do tak straszliwych, morderczych ataków, stwierdził, że „był to błąd naszego systemu wywiadowczego. Błąd spowodowany brakiem zasobów oraz samozadowoleniem, które było naszym udziałem w ciągu ostatnich dziesięciu lat. Wynikało ono z przekonania, że po upadku Związku Sowieckiego nic już nam nie zagraża".

Weldon obwiniał wywiad za wydarzenia 11 września, za niezdolność do zapewnienia narodowego bezpieczeństwa oraz za niepoinformowanie społeczeństwa o planowaniu ataku, którego cel leżał na terytorium Stanów Zjednoczonych. Odpowiedzialnością za to obarczał administrację prezydenta Clintona. Podczas swej kadencji Bill Clinton dał do zrozumienia, że ciężka praca wywiadu jest mu równie potrzebna, jak zeszłoroczny śnieg. I rzeczywiście, pracownicy wywiadu często narzekali, że administracja w ogóle się nie interesuje tym, co CIA ma do powiedzenia, zaś Clinton jest skłonny rozwiązywać każdy kryzys i zagrożenie narodowego bezpieczeństwa przez wysyłanie pocisków cruise[5]. Próżno dowodzili, że wojna z partyzantką wymaga działania z bliska i osobistego zaangażowania.

Ale Weldon rzeczywiście wierzył, że Ameryka dysponowała środkami technicznymi, które umożliwiały analitykom wywiadu wyśledzenie planów ataków z 11 września i zapobieżenie im. Problemem było to, że spośród 32 agencji federalnych zarządzających systemami komputerowymi przechowującymi tajne dane wywiadowcze jedynie

[5] Pociski manewrujące o średnim zasięgu działania, przenoszące głowice jądrowe lub konwencjonalne, napędzane silnikiem odrzutowym lub odrzutowym strumieniowym. Obecnie są wyposażane w komputerowe systemy sterowania. Mogą być odpalane z powietrza, lądu, morza. W porównaniu z pociskami balistycznymi mogą przenosić cięższe ładunki w stosunku do swoich rozmiarów i są trudniejsze do wykrycia ze względu na mniejszy rozmiar i lot na niższej wysokości, chociaż ich ponaddźwiękowa prędkość może je zdradzać. Były używane między innymi w czasie operacji Pustynna Burza (1991) w wojnie o Kuwejt z Irakiem — *przyp. tłum.* na podstawie encyklopedii internetowej *http://wiem.onet.pl/*

kilka jest skłonnych dzielić się posiadanymi informacjami. Weldon podał doskonały przykład, nie tylko kompromitujący CIA, lecz także służący jako oskarżenie ogólnego trybu postępowania, który utrwalił się w amerykańskiej wspólnocie wywiadowczej, a świadczył o nawyku działania „stąd-dotąd", ściśle według instrukcji.

-.-. -.-- -... . .-. - . .-. .-. --- .-.

Bombardowanie rozpoczęło się 23 marca 1999 roku. Administracja Clintona była przekonana, że skończy się ono stosunkowo szybko, a jugosłowiańscy Serbowie, którzy w Kosowie prowadzili ludobójczą wojnę przeciw muzułmanom, ulegną potędze Stanów Zjednoczonych i NATO. Ostatecznie bombardowania trwały przez 78 dni. Ale w ciągu początkowych dwóch tygodni Weldon zaczął otrzymywać e-maile i telefony od swoich partnerów z rosyjskiej Dumy.

W jednym z e-maili przeczytał: „Macie prawdziwy problem. Wasza polityka bombardowania Miloševicia i niewinnych Serbów powoduje w Rosji utratę zaufania ludzi do czystości waszych intencji, co odciąga Rosję coraz dalej od USA". W rzeczywistości ten e-mail oznaczał, że Półwysep Bałkański leży w tradycyjnej strefie wpływów rosyjskich i Stany Zjednoczone mądrzej zrobiłyby, traktując Rosję jako pełnoprawnego partnera w swych wysiłkach przywrócenia pokoju w tym regionie.

„Co chcecie, abym zrobił?" — odpisał.

„Chcemy, aby pan przekonał waszego prezydenta, że Rosja może odegrać istotną rolę w doprowadzeniu do zakończenia wojny i wyrzuceniu Miloševicia z urzędu" — odpowiedział rosyjski kontakt Weldona. Ponadto e-mail zawierał informację, że Rosja uważałaby za rzecz wskazaną, by Weldon udał się do Belgradu na czele delegacji Kongresu, której Rosjanie umożliwiliby spotkanie z Miloševiciem.

Z początku Weldon uznał, że taki wyjazd jest niemożliwy, gdyż Stany Zjednoczone znajdują się w środku wojny. Ponadto zastępca Sekretarza Stanu Strobe Talbot był takiej wyprawie przeciwny, twierdząc, że USA nie może zagwarantować bezpieczeństwa jej uczestników i nie ma żadnej gwarancji, że Milošević zastosuje się do zaleceń rosyjskich.

Ponadto Milošević właśnie wziął jako zakładników trzech żołnierzy amerykańskich, którzy podczas rutynowego patrolu nieświadomie przekroczyli granicę macedońsko-jugosławiańską. Należeli do

oddziału stacjonującego w Macedonii i mającego za zadanie zapobiegać rozprzestrzenianiu się działań wojennych. Niestety, armia nie wyposażyła ich w urządzenia radiowego globalnego systemu określania pozycji — zwanego Soldier 911. Produkcję tych urządzeń rozpoczęto przed czterema laty, a miały one nie tylko przestrzegać żołnierzy przed chodzeniem w miejsca, gdzie nie powinni się znaleźć, lecz także służyć do alarmowania jednostek o aktualnym miejscu ich pobytu. Aparaty radiowe miały wbudowany komercyjny chip odbiornika GPS, który pozwalał na dokładne określenie pozycji na powierzchni ziemi, a także komputer, modem i niewielki ekran. Wyprodukowano ich tysiące, ale gdy spytano, czy schwytani żołnierze byli w nie wyposażeni, armia nie potrafiła odpowiedzieć, czy w ogóle były stosowane w Macedonii[6].

Rosja wkrótce poszła o krok dalej i na oficjalnym papierze Dumy Państwowej zaprosiła Weldona i delegację Kongresu USA na spotkanie, którego wzniosłym celem miało być przeprowadzenie negocjacji poświęconych zakończeniu wojny w Kosowie i zmuszeniu Miloševicia do oddania władzy. Z powodu niepewnej sytuacji w Belgradzie Weldon i jego koledzy (pięciu demokratów i pięciu republikanów) przystali na spotkanie z Rosjanami i przedstawicielami Miloševicia w Wiedniu. Weldonowi nakazano, by negocjował bezpośrednio z Miloševiciem za pośrednictwem jednego z jego najbardziej oddanych zwolenników Dragomira Karica. Ani Weldon, ani nikt inny z delegacji nigdy nic nie słyszał o kimś takim.

Aby przygotować się do negocjacji, Weldon poprosił dyrektora CIA George'a Teneta o opis Karica. „Nie wiem, kim jest ten facet, ale Rosjanie są przekonani, że może nam udzielić informacji, które pomogą skłonić Miloševicia do przyjęcia naszych warunków" — powiedział Weldon. — „Czy może mi pan coś o nim powiedzieć?"

Tenet zadzwonił następnego dnia i w kilku zdaniach nakreślił charakterystykę osoby. Dodał, że z danych CIA wynika, iż „maczał on palce w rosyjskich aferach korupcyjnych, ale niewiele więcej można na jego temat powiedzieć" — wspomina Weldon.

Pamięta swoją podróż z roku 1997 do pewnego garnizonu w zapadłej dziurze gdzieś niedaleko Fort Belvoir w północnej Wirginii.

---

[6] Patrz: Dan Verton i Bob Brewin *Captive Soldiers Lacked Critical GPS Radios* Federal Computer, 5 kwietnia 1999.

Armia miała mu zademonstrować możliwości czegoś, co nazywano Information Dominance Center[7] lub Land Information Warfare Activity (LIWA)[8]. Polegając na doświadczeniu byłego analityka CIA, armia zaprzęgła do pracy komercyjne technologie przekopywania się przez zwały ogólnie dostępnych danych w Internecie, w różnego rodzaju wiadomościach agencyjnych oraz pracach naukowych krajowych i zagranicznych. Następnie tak uzyskane informacje były porównywane z tajnymi danymi wywiadowczymi spływającymi z całego świata. Weldon zdecydował, że nie mając nic do stracenia, poprosi o przygotowanie rysu biograficznego Karica. Zlecił to analitykom LIWA.

Za pomocą komercyjnych programów przeczesujących przygotowano ośmiostronicowy zestaw informacji o Karicu, z którego Weldon mógł się dowiedzieć, że ma on czterech braci, którzy są właścicielami największego systemu bankowego w byłej Jugosławii. Zatrudniali ponad 60 tys. ludzi, a ich bank był bezpośrednio zamieszany w próbę sfinansowania zakupu rosyjskich pocisków SA-10. Banku tego dotyczyła też afera wyłudzenia obligacji niemieckich wartych 4 miliardy dolarów. Jednakże powiązania braci Kariców z Miloševiciem sięgały daleko poza sprawy biznesowe. Jeden z braci osobiście finansował kampanię wyborczą Miloševicia. Co więcej, dom, w którym Miloševic mieszkał z żoną, był własnością rodziny Kariców. Żony Karica i Miloševicia były najlepszymi przyjaciółkami. Był to obraz bliskiego powiernika, z którym warto było prowadzić negocjacje z prawdziwego zdarzenia.

Ocena podróży delegacji Weldona do Wiednia nie jest jednoznaczna. Negocjacje nie przyniosły natychmiastowego ugaszenia ognia nienawiści, ale uzgodnienia dokonane przez Weldona, Rosjan i Karica stały się w końcu podstawą prowadzących do zakończenia wojny postanowień grupy G-8.

---

[7] Information dominance czyli dominacja informacyjna jest rozumiana w armii jako dysponowanie przeważającymi możliwościami generowania informacji, manipulowania nią i używania jej do uzyskania przewagi militarnej. Zatem Information Dominance Center oznacza ośrodek, który taką dominację informacyjną zapewnia — *przyp. tłum.*

[8] W wolnym tłumaczeniu jest to „system informacji przestrzennej (terenowej) służący działaniom wojennym" — *przyp. tłum.*

Po powrocie Weldona do kraju CIA i FBI usiłowały wydobyć od Weldona informacje o Karicu, gdyż na żądanie Departamentu Stanu miały przygotować zestawy informacji o tym nowym graczu na scenie politycznej, który rzeczywiście był w stanie rozmawiać z Miloševiciem. Weldon powiedział im wszystko, co wiedział o Karicu, a gdy zapytali o źródło informacji, poinformował ich o danych zebranych przez wojskowe Information Dominance Center. Jak twierdzi, zmieszani pytali, „co to takiego to Information Dominance Center".

-.-. -.-- -... . .-. - . .-. .-. --- .-.

Choć CIA i FBI nigdy nie słyszały o Information Dominance Center, ani o jego olbrzymich możliwościach przeczesywania danych, to słyszało o nim U.S. Special Operations Command (USSOCOM)[9], które było zainteresowane wykorzystaniem jego możliwości dla własnych działań wywiadowczych.

Jesienią 2000 roku USSOCOM zbudowało własny system mini-LIWA, mający za zadanie wyszukiwanie informacji i przygotowywanie opracowań tematycznych. Miały one pomagać w planowaniu działań antyterrorystycznych i w zwalczaniu ruchów partyzanckich. Jednakże ważniejszą przyczyną stworzenia systemu mini-LIWA była konieczność zbierania danych w celu nakreślenia profilu al-Kaidy — łącznie z jej powiązaniami z innymi organizacjami terrorystycznymi z całego świata. W nieutajnionej wersji tego dokumentu widzimy ogólny schemat organizacji i sieci jej powiązań zewnętrznych.

Po zebraniu tych informacji USSOCOM przygotował ich przegląd dla przewodniczącego Połączonego Komitetu Szefów Sztabów Hugha Sheltona. Sugerował w nim usunięcie pięciu specjalnych komórek al-Kaidy, co miało znacznie zmniejszyć, jeżeli nie zlikwidować, jej zdolność do przeprowadzania operacji terrorystycznych. Jednakże zanim przegląd zaprezentowano Sheltonowi, został skrócony z trzech godzin do jednej, a co najważniejsze, zapisane w nim zalecenie zniszczenia pięciu komórek al-Kaidy nigdy nie doczekało się realizacji.

„Na rok przed 11 września potencjał naszych Sił Specjalnych był wystarczający do rozpracowania sieci al-Kaidy" — mówił Weldon na posiedzeniu Izby Reprezentantów w osiem miesięcy po atakach

[9] Dowództwo Operacji Specjalnych USA — *przyp. tłum.*

11 września. „Udało im się pójść o wiele dalej i przekazać nam wskazówki, gdzie powinniśmy uderzyć i jakie komórki wyeliminować, aby ich obezwładnić. Gdyby te działania podjęto, być może nie byłoby tragedii 11 września".

„Przepytywałem w tej sprawie naszego Dyrektora ds. Bezpieczeństwa Wewnętrznego[10] Toma Ridge'a. Zgodził się z moją opinią, lecz cóż z tego, skoro nadal nie udaje mu się stworzyć centrum współpracy międzyagencyjnej, a jest to oskarżenie pod adresem rządu, które może wywoływać słuszny gniew Amerykanów".

Rzeczywiście, Amerykanie byli oburzeni atakami 11 września. Wpadliby w prawdziwą furię, gdyby wiedzieli, jak dalece uchybienia i nieumiejętność wzajemnego dzielenia się informacjami przez poszczególne agencje wywiadowcze umożliwiły zamachowcom osiągnięcie sukcesu. Ale Amerykanie znają tylko część prawdy o błędach wywiadu dotyczących posługiwania się najnowocześniejszą techniką.

-.-. -.-- -... . .-. - . .-. .-. --- .-.

1 października 1999 roku grupa 19 menedżerów średniego stopnia z Agencji Bezpieczeństwa Narodowego[11], zajmującej się wywiadowczym śledzeniem przesyłanych sygnałów i informacji, przekazała swemu dyrektorowi, generałowi porucznikowi lotnictwa Michaelowi Haydenowi, oskarżenie dotyczące, jak to nazwano, kryzysu przywództwa oraz niemożności dotrzymania kroku nieokiełznanemu rozwojowi technologii komercyjnych.

Grupa menedżerów (11 mężczyzn i 8 kobiet), która przyjęła nazwę New Enterprise Team[12] lub NETeam, uznała, że „agencja jako całość dojrzała do rozwiązania". Członkowie grupy twierdzili, że „NSA straciła wiarygodność u swych mocodawców i klientów oraz

[10] Homeland Security Director — *przyp. tłum.*

[11] National Security Agency (NSA) — główne zadania tej supertajnej agencji wywiadowczej to strzeżenie amerykańskich rządowych środków łączności oraz podsłuchiwanie/przejmowanie informacji przesyłanych przez obce rządy, służby specjalne i organizacje przestępcze. Specjalizuje się przede wszystkim w wywiadzie technicznym, kryptologii, łamaniu szyfrów itp. — patrz np. *http://www.republika.pl/garton/org/usa/nsa.html* lub *http://www.totse.com/en/politics/national_security_agency/* — *przyp. tłum.*

[12] W wolnym tłumaczeniu „zespół mający się zająć nowym przedsięwzięciem/przedsiębiorstwem" — *przyp. tłum.*

że nie podejmuje żadnych prób reorganizacyjnych, koniecznych do skutecznego działania w wieku informacji". W rezultacie „wyjątkowe dziedzictwo służby NSA jest w wielkim niebezpieczeństwie".

W rzeczywistości oznaczało to, że agencja nie tylko straciła zaufanie swych klientów — członków rządu oraz różnego rodzaju osób i instytucji z amerykańskiej wspólnoty wywiadowczej — lecz że nie potrafi także dostosować się do realiów wieku Internetu. Terroryści walczący z Ameryką posiedli już umiejętność „operowania siecią i skutecznego wykorzystywania jej do realizacji własnych celów". Zaś główna krajowa agencja wywiadowcza, mająca za zadanie śledzenie sygnałów, komunikatów i przesyłanych wiadomości, tonie pod wielkimi zwałami informacji, których nie potrafi przeanalizować. NETeam ostrzegała Haydena, że NSA, choć dysponuje największą liczbą superkomputerów, z powodu kryzysu przywództwa nie dotrzymuje kroku rozwojowi technologii szyfrowania oraz przestaje ogarniać miliony mil nowo instalowanych linii światłowodowych przenoszących komunikaty terrorystów zagrażających Stanom Zjednoczonym. Twierdziła, że NSA dotychczas tkwi jedną nogą w bagnie zimnej wojny. W rezultacie „krytyczne dane potrzebne tym, którzy podejmują decyzje, (...) są często nieosiągalne lub trudne do wydobycia. W rezultacie decyzje finansowe, dotyczące zasobów ludzkich lub zaangażowania klientów w różne przedsięwzięcia są podejmowane późno lub są błędne". Twierdziła, że żadne prowizoryczne działania nie odwrócą tych trendów i nie uzdrowią agencji.

„Zakres proponowanych przez nas zmian przypomina remont samolotu podczas lotu z kompletem pasażerów" — napisała grupa 19 menedżerów.

Na raport Hayden zareagował natychmiast, rozpoczynając tzw. okres „100 dni zmian", podczas którego obiecał zreorganizować sztywny i przestarzały sposób zarządzania agencją oraz skończyć z jej przekraczającym granice rozsądku utajnieniem i izolacją. Podjęto natychmiastowe kroki w celu przygotowania strategicznego planu wdrożenia nowego sposobu zarządzania oraz zastosowania nowych technologii. Przystąpiono także do odnowienia siedziby agencji, skupiając się przede wszystkim na remoncie głównego budynku operacyjnego (129 tys. stóp kwadratowych powierzchni) w kwaterze głównej w Fort Meade w stanie Maryland. Projekt obejmował unowocześnienie połączeń ponad 1000 pracowników agencji oraz

zapewnienie dodatkowych łączy internetowych dla 10% stacji roboczych. Przewidziano także stworzenie Centrum Śledzenia Operacji, które miało przez 24 godziny na dobę zbierać i analizować dane wywiadowcze.

NSA rozpoczęło także stopniowe prace nad przygotowaniem olbrzymiego kontraktu, przewidzianego na 10 lat i 5 miliardów dolarów. Jego celem miało być zlecanie firmom z sektora prywatnego zarządzania informacjami nieobjętymi klauzulą tajności. „Musimy natychmiast zacząć inwestować w rozwój naszej struktury informatycznej, aby zapewnić sobie sprawność działania i zdolność adaptacji w wieku informacji" — napisał Hayden w publicznym oświadczeniu, w którym ujawnił plany realizacji kontraktu zwanego „Project Groundbreaker[13]". Hayden wierzył, że najlepszym sposobem, by agencja odzyskała utraconą wiodącą rolę i giętkość operacyjną, jest pozbycie się znacznej części codziennych pracochłonnych zadań przez przekazanie ich do wykonania firmie prywatnej. To samo wynikało z raportu NETeamu.

Podjęcie przez Haydena wysiłków zreformowania agencji i jego dążność do zaakceptowania i zrealizowania postulatów przedstawionych przez 19 członków NETeamu, nazywanych przez niego „lojalnymi anarchistami", nie uszła uwagi Waszyngtonu. Wkrótce po zakończeniu „100 dni zmian" Senacka Komisja Specjalna ds. Wywiadu[14] umieściła rekonstrukcję NSA na szczycie listy priorytetowych zadań ustawy zatwierdzającej budżet wywiadu na rok 2001[15]. „NSA systematycznie poświęcała modernizację infrastruktury na rzecz wykonywania bieżących zadań wywiadowczych" — stwierdziła komisja. — „W wyniku tego rozpoczęła wiek XXI bez odpowiedniej infrastruktury technologicznej i bez zasobów ludzkich pozwalających na podjęcie stojących przed nią wyzwań".

Jednak choć Hayden był reformatorem, który rozumiał konieczność dopływu świeżej krwi, jego wybór zastępcy przeczył temu. Wkrótce po przyjęciu bankowego specjalisty od spraw inwestycyjnych

---

[13] Groundbreaker to ktoś oryginalny i innowacyjny, nazwa ma więc oznaczać projekt będący przełomem, wejściem na nowe tory — *przyp. tłum.*

[14] Senate Select Committee on Intelligence — *przyp. tłum.*

[15] 2001 Intelligence Authorization Bill — *przyp. tłum.*

na stanowisko głównego księgowego udał się do Dulles w Wirginii niedaleko Waszyngtonu w poszukiwaniu swej prawej ręki w dziedzinie technologii i pomocnika w taktycznych działaniach wewnętrznej rewolucji w NSA. Jedynym problemem było to, że wybrany przez niego na zastępcę William Black był 38-letnim weteranem NSA, który zaledwie w roku 1997 odszedł z agencji. Minione trzy lata spędził, pracując w sektorze prywatnym. Wybranie Blacka nie było więc takim przełomem, jakiego się spodziewano. Zatrudnienie byłego pracownika zostało przez niektórych uznane za dowód niemożności wychowania własnej nowej generacji liderów awansowanych spośród obecnych pracowników wywiadu.

Aby być sprawiedliwym, należy uznać, że jeżeli nawet Black był powiązany z firmami prywatnymi — jak niektórzy twierdzili — dobrze rozumiał wyzwania stojące przed NSA. Jednym z nich było i nadal jest udostępnianie i upowszechnianie technologii szyfrowania. Technologie, które niegdyś pozwalały na skuteczne szyfrowanie komunikatów, teraz stawały się dostępne dla terrorystów. Rzeczywiście, odczytanie zaszyfrowanych plików znalezionych na dyskach laptopów agentów al-Kaidy, ujętych w roku 1993 w związku z zamachem bombowym na World Trade Center, zajęło NSA kilka miesięcy.

Eksperci ds. bezpieczeństwa narodowego, łącznie z poprzednikiem Blacka w NSA, od lat przestrzegali przed eksportowaniem za granicę produkowanych przez amerykańskie firmy programistyczne narzędzi do szyfrowania bez zachowania w depozycie klucza. Spowodowałoby to zwiększenie prawnego nacisku na użytkowników oraz zapewnienie sobie możliwości odczytania zaszyfrowanych komunikatów w przypadku wykorzystywania ich do działań kryminalnych lub godzących w bezpieczeństwo narodowe. Bardzo szybko okazało się, że dżin już został wypuszczony z butelki. Narzędzia do programowego szyfrowania przesyłanych informacji stały się wkrótce powszechnie dostępne na całym świecie. Coraz częściej były produkowane przez zagraniczne firmy kupowane lub zakładane przez amerykańskich inwestorów jedynie po to, aby wytwarzać rodzime technologie i sprzedawać je za granicą.

W końcu społeczność stróżów bezpieczeństwa narodowego przegrała batalię o narzucenie ograniczeń dotyczących handlu programami szyfrującymi. Globalny pęd do rozpowszechnienia handlu

elektronicznego był zbyt silny, aby mógł się mu oprzeć jakikolwiek rząd. W rezultacie potężne narzędzia szyfrujące „wyfrunęły" w świat, stały się dostępne na całym globie i są stosowane zarówno przez praworządnych obywateli, jak i przez terrorystów. NSA została pozostawiona sama sobie w trudnej walce o ponowne zapanowanie nad licznymi strumieniami informacji wysyłanymi przez wrogów Ameryki. Na razie jej możliwości kontroli są znacznie ograniczone.

Siedem miesięcy przed atakami terrorystycznymi 11 września Hayden zrobił coś niezwykłego jak na dyrektora supertajnej agencji wywiadowczej — tak tajnej, że niegdyś akronim NSA żartobliwie odczytywano jako No Such Agency[16] — pokazał się w telewizji i mówił o niezdolności NSA do efektywnego działania w dobie Internetu.

13 lutego 2001 roku udzielił wywiadu ogólnonarodowej telewizji CBS i w audycji „60 minut" powiedział, że NSA pozostaje w tyle za resztą świata i nie może dotrzymać kroku gwałtownemu rozwojowi technologii[17]. „Jesteśmy poza szlakiem, którym kroczy globalna rewolucja telekomunikacyjna" — stwierdził. Jeżeli gdziekolwiek na świecie powstanie nowe rozwiązanie telekomunikacyjne, NSA musi znaleźć sposób na podsłuchanie i rozszyfrowanie przekazu. Co najważniejsze, musi szybko znaleźć sposób na wyławianie połączeń międzynarodowych organizacji terrorystycznych i obcych służb specjalnych z wielkiego, bezprecedensowego zalewu rozmów prowadzonych przez telefony komórkowe i przekazów internetowych pochodzących z urządzeń przenośnych.

Przyznanie przez Haydena, że NSA pozostaje „poza szlakiem rozwoju najnowszych technologii", bardziej niż późniejszy elaborat NETeamu i okres „100 dni zmian" przekonały kilku ekspertów ds. bezpieczeństwa, że nadszedł czas, aby NSA poszło w ślady CIA i znalazło prywatną firmę gotową zainwestować znaczne kapitały w badania i rozwój, co pomogłoby agencji dotrzymać kroku czołowym technologiom. CIA zrobiło więcej — nie tylko dopuściło do swych prac firmy prywatne, lecz samo również weszło na rynek.

---

[16] Nie ma takiej agencji — *przyp. tłum.*

[17] Patrz: Dan Verton *NSA Struggles to Keep Up with Pace of Technology* „Computerworld", 5 marca 2001.

-.-. -.-- -... . .-. - . .-. .-. --- .-.

W kwaterze głównej CIA w Langley w Wirginii George Tenet przeważającą część roku 1999 spędził na „przygotowywaniu się na przyszłość". Wiele wysiłku poświęcił na szukanie nowych sposobów wymiany informacji wewnątrz całej wspólnoty wywiadowczej, składającej się z 14 różnych agencji, z których większość podlega Departamentowi Obrony.

Jednym z pierwszych projektów przygotowanych przez CIA w tym roku był system Intelligence Community Metropolitan Area Communications (IC MAC)[18]. Został on zaprojektowany w celu poprawienia łączności i wymiany informacji między rządowymi agencjami wywiadowczymi i Departamentem Obrony. Agencje wywiadowcze podjęły ponadto wspólny wysiłek stworzenia nowych narzędzi pozwalających na wykorzystanie możliwości komunikacyjnych Internetu. Na przykład bezpieczna aplikacja sieciowa XLINK powstała w celu poprawienia współpracy „zbieraczy" informacji z analitykami. Poza tym CIA utworzyło tajne laboratorium badawcze nazwane kryptonimem Platinum Rail, którego zadaniem było zbadanie sposobów wsparcia pracy wywiadu przez wykorzystanie oprogramowania komercyjnego.

Tenet pilnował także tworzenia PolicyNet Program Office[19], który miał nadzorować sieć bezpiecznych połączeń internetowych zapewniających dostęp do bazy danych CIA. Korzystać z niego mieli U.S. Senate Appropriations Committee[20] i inne osoby oraz instytucje tworzące prawo. Agencja rozpoczęła także badania nad oprogramowaniem służącym do eksploatowania sieci z zastosowaniem programów tłumaczących teksty z innych języków oraz programów służących do wizualizacji danych. Na przykład połączono dwa systemy, by stworzyć oprogramowanie pozwalające analitykom na śledzenie w wersji angielskiej dokumentów pisanych po japońsku i po koreańsku oraz tworzenie angielskich streszczeń możliwych do odczytywania za pomocą standardowej przeglądarki internetowej.

[18] W wolnym przekładzie „miejska sieć łączności wspólnoty wywiadowczej" — *przyp. tłum.*

[19] Biuro programu polityki sieciowej — *przyp. tłum.*

[20] Komisja senatu do badania wydatków rządowych — *przyp. tłum.*

Przedstawiono także wersję demonstracyjną programu tłumaczącego z farsi[21] na angielski. Zrobiono to w roku 1999 w samej agencji.

A poza agencją w roku 1999 udało się skorzystać z fali sukcesów wielu dotcomów[22] i dzięki funduszom uzyskanym od CIA uzyskać ich pomoc w rozwiązaniu problemów z zarządzaniem informacjami i ich analizowaniem. Był to też rok powołania do życia In-Q-Tel, Inc. firmy badawczo-rozwojowej, której inwestorem było CIA.

W lutym 1999 CIA zainwestowało w In-Q-Tel 28 milionów dolarów. Nazwa firmy była kombinacją skrótów: In-…-tel (od ang. *intelligence* — wywiad) oraz Q — imienia genialnego twórcy gadżetów szpiegowskich w filmach o Jamesie Bondzie. Nową firmę utworzono w celu wykorzystania doświadczeń technologicznych firm prywatnych i szybkiego wsparcia ich osiągnięciami wysiłków CIA. W ostatnich latach agencja ugrzęzła w bagnie biurokracji i strachu przed dokonywaniem jakichkolwiek zmian. Część pracowników CIA uważała, że agencja cierpiała na syndrom obawy przed wszystkim, „co nie u nas wmyślono", a to paraliżowało jej możliwości dotrzymywania kroku rozwojowi technologii.

Ale zgodnie z wewnętrznym raportem napisanym w roku 2001 przez L. Britta Sidera, inspektora generalnego CIA, problemy agencji sięgały o wiele głębiej. Według niego, niezdolność agencji do korzystania z osiągnięć technologicznej rewolucji, trwającej w prywatnym sektorze gospodarki, groziła podstawom jej bytu. „Zastanawiam się, czy agencja jest świadoma ciągłego zmniejszania się jej przydatności" — pisał Snider w swym piśmie pożegnalnym do władz CIA przed odejściem na emeryturę. — „Myślę, że agencja będzie w stanie zwiększać swą wartość i użyteczność jedynie wtedy, gdy uda się jej do realizacji swych zadań wykorzystać nowe technologie rozwijane w prywatnym sektorze gospodarki. A tego się nie uda zrobić bez dopuszczenia do naszych działań kompetentnych ludzi z zewnątrz.

---

[21] Odmiana perskiego — *przyp. tłum.*

[22] Dotkom; dotcom; dot-com — tak określa się firmy, które w latach 90. oparły swą działalność rynkową na Internecie. Słowo pochodzi od nazw tych firm, których większość zawierała *.com* (ang. *dot* — kropka). Przykładem jest znana księgarnia internetowa Amazon.com — *przyp. tłum.*

Gdy przed laty byłem dyrektorem ds. personalnych Aspin/Brown Commission[23], uświadomiłem sobie, że świat technologii informacyjnych niezbyt dobrze pasuje do świata wywiadu. Podstawą osiągnięć tego pierwszego środowiska jest otwartość i czytelność. Wcale tam nie tęsknią za kontraktami rządowymi i pieczęciami tajnych kancelarii. Dla nas zaś najważniejsza jest tajemnica. Zatem należy znaleźć sposób, aby zaprząc ich technologie do wykonywania naszych zadań, bez zbędnego narzucania im tego, co dla nich niewygodne. Dlatego uważam, że firma In-Q-Tel jest skazana na sukces. Menadżerowie agencji i jej nadzorcy muszą dać jej możliwość działania"[24].

Snider celnie zaatakował panującą w CIA niechęć do choćby niewielkiego zwiększenia przejrzystości działania, wskazując, że to właśnie hamuje szybkie pozyskanie dostępu o nowych technologii. CIA miało ten sam problem, co NSA: jak zreformować własne zasady działania, aby umożliwić większą elastyczność? Przypominam sobie swoją rozmowę na ten temat z George'em Tenetem w roku 1998 na bankiecie sponsorowanym przez Marine Corps Intelligence Association[25], gdzie później zostałem prezesem oddziału. Półżartem powiedziałem mu wówczas, że jako dziennikarz musiałem się sporo napracować, by przebić się przez wszystkie warstwy tajności i byłoby świetnie, gdyby mógł mi opowiedzieć kilka nowych historii. Spytał, z kim się kontaktowałem w agencji. Gdy wymieniłem nazwisko mojej pierwszej rozmówczyni, uśmiechnął się i powiedział, że jutro zaraz po przyjściu do pracy awansuje ją.

W sierpniu 2001, na miesiąc przed atakami terrorystycznymi, pojawiły się pierwsze oznaki, że In-Q-Tel zaczyna spełniać pokładane w nim nadzieje. W raporcie przygotowanym na żądanie Kongresu i włączonym do rocznego sprawozdania budżetowego wywiadu za rok 2000, 30 członków Independent Panel on the Central Intelligence

---

[23]Komisja powołana w roku 1994 przez prezydenta i Kongres USA w celu zbadania działań i możliwości wywiadu amerykańskiego — *przyp. tłum.*

[24]L. Britt Snider *A Letter from the Inspector General, Central Intelligence Agency*, wewnętrzne memorandum CIA, 19 stycznia 2001.

[25]Stowarzyszenie wywiadu Marine Corps (patrz notka o Autorze i przypis na początku książki) — *przyp. tłum.*

Agency In-Q-Tel Venture[26] orzekło, że ten sposób prowadzenia firmy „ma sens". Jednakże wstrzymali się przed zarekomendowaniem tego pomysłu innym agencjom, takim jak NSA. Najważniejsze było to, że technologia zbierania i analizowania informacji, użyteczna w pracy wywiadowczej, zaczęła wreszcie torować sobie drogę do CIA.

Jednym z narzędzi takiej technologii był Presidential Information Dessemination System (PIDS)[27], elektroniczne narzędzie do przygotowywania przeglądowych zestawień informacji dla prezydenta elekta podczas przejściowego okresu zmiany administracji. Dodatkowo PIDS był podstawą, na której opierało się działanie programu iWeb, portalu sieciowego przygotowanego przez CIA jako narzędzie dla analityków.

Ponadto In-Q-Tel zleciło SafeWeb z Oakland w Kalifornii, firmie wiodącej w dziedzinie technologii ochrony poufności danych, stworzenie narzędzia zapewniającego poufność i bezpieczeństwo informacji agencyjnych przesyłanych Internetem. Za pośrednictwem In-Q-Tela CIA zleciło także firmie Intelliseek, Inc. z Cincinnati stworzenie technologii, którą będzie można zastosować w programach-agentach mających w przyszłości służyć analitykom do sprawniejszego pozyskiwania danych wywiadowczych na podstawie informacji ogólnie dostępnych w sieci WWW. Firma przystąpiła do zbierania osiągnięć prywatnego sektora w dziedzinie R&D[28] i w chwili pisania tej książki kontynuuje tę pracę.

Szkoda, że dopiero śmierć 3000 Amerykanów 11 września 2001 roku zmusiła wspólnotę wywiadowczą, łącznie z jej najwyższymi władzami, do skupienia uwagi na rozwoju technologii budowy sieci. Dzięki temu wkrótce możliwe będzie dzielenie się informacjami, by w przyszłości ustrzec się ataków terrorystycznych i śmierci niewinnych ludzi. Projektowi przekazywania krytycznych informacji — który od dawna rozłaził się w szwach i którego realizacja postępowała w żółwim tempie — poświęcono wreszcie uwagę, na jaką zasługiwał.

Jednym z najważniejszych spośród wdrażanych obecnie programów jest Intelligence Community System for Information Sharing

---

[26] Niezależny komitet ds. inwestycji CIA w firmę In-Q-Tel — *przyp. tłum.*

[27] Prezydencki system rozpowszechniania informacji — *przyp. tłum.*

[28] Research & Development — badania i rozwój — *przyp. tłum.*

(ICIS)[29]. Korzysta on z technologii WWW i zawiera w sobie dwa inne systemy: Top Secret Joint Worldwide Intelligence Communications System (JWICS, wymawiane jako Jay-Wicks)[30] oraz Secret Internet Protocol Routing Network (SIPRNET, wymawiane jako Sipper-Net)[31] — oba od lat używane przez wywiad do współużytkowania i przekazywania informacji. Różnica polega na tym, że teraz grupa menedżerów zarządzających CIA i innymi agencjami dąży do zbudowania opartego na przeglądarce sieciowej programu dostępowego, który nie będzie kierował użytkowników do źródeł, lecz raczej do zarządzanej zgodnie z ustalonymi zasadami wspólnej wirtualnej przestrzeni informacyjnej. ICIS będzie pozwalał na korzystanie z kontrolowanych interfejsów, które po raz pierwszy pozwolą pracownikom wywiadu na dokonywanie automatycznego procesu oddzielania i nieujawniania najtajniejszych źródeł informacji i sposobów ich pozyskiwania. Zostanie także zautomatyzowany sposób udostępniania informacji analitykom z najwyższymi i niższymi uprawnieniami dostępu.

Architekci systemu przewidują stworzenie na wszystkich poziomach uprawnień oddzielnych punktów wejścia dla grup zainteresowanych różnymi zagadnieniami. Jedna z takich bramek będzie prowadziła do Open Source Information System[32], wirtualnej przestrzeni informacyjnej wspólnej dla wszystkich współpracujących. Będzie ona zawierała istotne ale nieutajnione dokumenty dla pracowników wywiadu oraz skróty wiadomości agencyjnych z całego świata. Krytycy twierdzą, że pracownicy wywiadu i tak zlekceważą wszystkie możliwości systemu. Najczęściej cytowanym na to dowodem jest wywiad z roku 2000, udzielony przez członka al-Kaidy jednemu z dzienników włoskich, w którym przepytywany wyraźnie oświadczył, że bojownicy al-Kaidy przechodzą szkolenie pilotów mające na celu przygotowanie ich do wykonania ataków kamikadze.

---

[29] System wspólnego korzystania z informacji przez wspólnotę wywiadowczą — *przyp. tłum.*

[30] Tajny ogólnoświatowy system łączności wywiadu — *przyp. tłum.*

[31] Sieć routowana tajnym protokołem internetowym, co można nazwać po prostu tajnym Internetem — *przyp. tłum.*

[32] System operacyjny otwartych źródeł, czyli zawierający dokumenty jawne — *przyp. tłum.*

Opanowanie techniki usuwania najbardziej tajnych informacji jest istotne dla stworzenia systemu informacji wywiadowczej, dostępnego dla tysięcy federalnych, stanowych i lokalnych przedstawicieli władzy znajdujących się na pierwszej linii obrony naszego bezpieczeństwa, którzy jednak nie są (i nie powinni być) uprawnieni do czytania informacji szczególnie tajnych oraz kluczowych danych wywiadu. Kiedy służyłem w wywiadzie wojskowym na początku lat 90., to właśnie często stanowiło przedmiot sporu i było przyczyną opóźnień w dostarczaniu informacji ludziom, którzy na nią czekali.

W pierwszej fazie tworzenia ICIS (która ciągle trwa podczas pisania tej książki) następuje włączanie do projektu takich rozwiązań rozszerzających możliwości systemu jak stosowanie technologii publicznego klucza szyfrowania oraz tworzenie kartotek analityków wywiadu, którzy mogą porozumiewać się za pomocą tajnej, zaszyfrowanej poczty elektronicznej. Przygotowywane są również zestawy programów mających ułatwiać współpracę; chronione interfejsy umożliwiające dostęp do repozytoriów danych na różnym poziomie tajności; system metaznaczników danych ułatwiający proces ich wyszukiwania przez członków wspólnoty wywiadowczej. To ostatnie zagadnienie jest nader ważne, gdyż pozwala na znaczne oszczędzanie czasu. W miarę powstawania narzędzi analitycznych i wyszukiwawczych wywiadu należy je upowszechniać wśród pracowników wszystkich agencji mających uprawnienia do korzystania z danych na różnych poziomach tajności.

Jednakże z tym wewnątrz wspólnoty wywiadowczej nie jest najlepiej. Nowe rozwiązania nie są popularne, a ich upowszechnianie nie jest zadaniem łatwym. Byłem pracownikiem wywiadu w czasie, gdy uruchomiono Intelink, pierwsze repozytorium danych wywiadu, działające w wewnętrznej sieci intranetowej i dające dostęp do tajnych danych i produktów. Jeden z przedstawicieli wywiadu scharakteryzował to następująco: „Weźcie AOL[33], Yahoo[34] i MSN[35], dołączcie to do zbioru tajnych danych i macie swój Intelink".

---

[33] America on Line — wielki amerykański dostawca usług internetowych, patrz *http://www.aol.com/ — przyp. tłum.*

[34] Wielki amerykański serwis internetowy: wyszukiwarka WWW, grupy dyskusyjne i wiele innych usług, patrz: *http://www.yahoo.com/ — przyp. tłum.*

[35] Microsoft Service Network — internetowy serwis usługowo-informacyjny Microsoftu, patrz: Microsoft Service Network — *przyp. tłum.*

Uruchomienie Intelinku było spełnieniem marzeń dla tych spośród nas, którzy działali na „czubku dzidy" — jak nazywano pracę w środowisku oddziałów bojowych. Pamiętam, że podczas największego nasilenia działań wojennych w Bośni mogłem przeglądać dane wywiadu na stronach WWW CIA, DIA[36], europejskiego dowództwa wojsk USA w Sztuttgarcie, a także Joint Analysis Center (JAC)[37] w Molesworth w Anglii. Intelink udostępniał informacje wywiadowcze (mapy, obrazy, analizy, rozkład sił wojskowych, itd.), normalnie niedostępne dla moich analityków w Second Marine Expeditionary Force, którzy przygotowywali Operation Plan 40104, czyli plan operacyjny niebezpiecznej misji wydobycia z Bośni (niektórzy mówią: uratowania) oddziałów United Nations Protection Force (UNPROFOR)[38].

Ale nie wszyscy patrzyli na Intelink w ten sam sposób. Wiele odizolowanych grup w różnych agencjach wywiadowczych, kultywując dotychczasowe metody działania, nie przekonało się do ujawniania informacji za pomocą technologii internetowych. Na przykład CIA nie było zadowolone, widząc swe analizy udostępnione innym agencjom (na przykład dowództwu wojskowemu, dla którego pracowałem) bez uzyskania odpowiednich zezwoleń. Dowództwa nadrzędne denerwowała łatwość pozyskiwania informacji przez dowództwa podrzędne, które mogły bez problemu ściągać produkty agencji wywiadowczych bez uzyskiwania zgody i przechodzenia przez cały łańcuszek hierarchicznych zależności. Internet podważył zasadność istnienia niektórych organizacji. Dzięki Intelinkowi w ciągu niewielu minut otrzymywałem informacje, których uzyskanie drogą urzędową trwałoby tygodniami. Ponadto zamiast zadowalać się fotografiami sprzed pięciu lat, mogłem ściągać najbardziej aktualne zdjęcia lotnicze robione w Bośni przez samoloty U-2. Ale to właśnie było zagrożeniem

[36] Defense Intelligence Agency — Wywiadowcza Agencja Obrony, utworzona przez Departament Obrony, działa od 1 października 1961, zajmuje się wywiadem zagranicznym, patrz: *http://www.dia.mil/ — przyp. tłum.*

[37] Połączone centrum analityczne wywiadu dowództwa wojsk amerykańskich w Europie. Od sierpnia roku 1975 działało w Sztuttgarcie w Niemczech, w październiku 1991 zostało przeniesione do bazy RAF-u w Molesworth w Anglii — *przyp. tłum.*

[38] Siły Ochronne Organizacji Narodów Zjednoczonych — *przyp. tłum.*

dla głęboko okopanych, sztywnych i niereformowalnych struktur zarządzania. Przejrzystość i dostępność informacji wewnątrz wspólnoty wywiadowczej stanowiła dla niej wielki problem.

W ciągu siedmiu lat, które upłynęły od czasu, gdy przestałem być pracownikiem wywiadu, zasób informacji udostępnianych przez Intelink rozszerzył się gwałtownie, a to stanowi nowe wyzwanie dla obecnych oficerów wywiadu. W pierwszą rocznicę ataków terrorystycznych 11 września 2001 istniało już 2,4 miliona stron udostępnianych przez supertajne połączenia Intelinku. Analitycy mają tam dostęp do tak wielu informacji, że jeden z wyższych przedstawicielu wywiadu stwierdził, że „szukanie czegoś w Intelinku przypomina grę w craps[39 i 40]". Obecnie przygotowuje się hierarchizację tej bazy danych zawierającej mnóstwo informacji rozsianych na wielu serwerach agencji wywiadowczych. Stworzono działające przez 24 godziny na dobę centrum operacyjne, którego jedynym zadaniem jest pomaganie użytkownikom Intelinku w znajdowaniu potrzebnych im informacji.

Ale udostępnianie informacji dotyczących bezpieczeństwa narodowego stanowi wyzwanie, które pojmuje jedynie niewiele osób spoza kręgów pracowników wywiadu — twierdzi William Dawson, zastępca rzecznika wspólnoty wywiadowczej[41]. Na przykład po raz pierwszy poproszono agencje wywiadowcze o udostępnianie takim urzędom jak Environmental Protection Agency (EPA)[42] i Departament Rolnictwa tajnych informacji pochodzących z supertajnych źródeł. „Naprawdę nie potrzeba, aby przedstawiciele EPA przeglądali informacje o rozmieszczeniu sił wojskowych" — twierdzi Dawson, odnosząc się do żądań umożliwienia pełnego dostępu do danych tego rodzaju instytucjom. — „Mogę im wysłać depeszę z potrzebnymi informacjami, pytając, czego chcą, czego potrzebują i co chcą z tymi informacjami zrobić".

---

[39] Patrz: Dan Verton *Searching Intelink Is Like Shooting Craps* „Computerworld", 9 września 2002.

[40] Popularna w USA gra w kostki — *przyp. tłum.*

[41] Wywiad Autora. Information Sharing and Homeland Security Conference, Filadelfia, Pensylwania, 19 – 20 sierpnia 2002.

[42] Agencja Ochrony Środowiska — *przyp. tłum.*

Nieprzerwany postęp technologiczny wymusił rozpoczęcie procesu „zmiękczania" skostniałych struktur społeczności wywiadowczej, zwłaszcza CIA, które dotąd tkwi w epoce zimnej wojny i musi rozwiązać problem, w jaki sposób zmusić własne struktury i kadry kierownicze do zaakceptowania postępu. Czy tradycyjne umiejętności i sposoby działania CIA przystają do wymagań wieku informacji? Czy organizacja CIA odpowiada wymaganiom współczesności? Te pytania zadawali sobie i na te tematy dyskutowali najwyżsi i najbardziej zasłużeni pracownicy agencji i dotychczas nie udało im się zakończyć tej debaty. Nic lepiej nie ilustruje tych sporów intelektualnych jak dwie różne opinie byłych dyrektorów CIA.

Na cztery miesiące przed atakami terrorystycznymi 11 września, podczas konferencji na temat przyszłości CIA sponsorowanej przez Radę Stosunków Zagranicznych[43] byli szefowie CIA — admirał Stansfield Turner, Wiliam H. Webster, James Woolsley i John Deutch — zgodzili się, że pomimo nowych zagrożeń i wyzwań, jakie niesie rewolucja technologiczna, zdobywanie obcych tajemnic pozostaje podstawowym zadaniem agencji.

„Zasadniczym zadaniem CIA jest zdobywanie tajnych informacji" — mówił Woolsey, który stał na czele agencji w latach 1993 – 95. — „To zadanie nie zmieni się z upływem czasu".

Turner, który kierował agencją za czasów administracji Cartera, nie zgodził się, że nowe technologie wywróciły agencję do góry nogami. „Myślę, że przesadzamy, twierdząc, że funkcja wywiadu zmieniła się od czasu zakończenia zimnej wojny" — powiedział. Twierdził też, że zasadniczym zadaniem jest określenie roli dyrektora agencji i zapewnienie mu uprawnień i środków pozwalających na kierowanie jej działaniami. Miał rację. Przez lata dyrektorzy CIA narzekali na brak środków na bieżącą działalność i zbyt skąpy przydział funduszy inwestycyjnych wśród 14 niezależnych agencji rządowych. Biurokracja rządowa oraz wojny o wpływy spowodowały, że uznawanie dyrektora agencji za osobę odpowiedzialną za działania wywiadowcze stało się nieporozumieniem.

Jednakże Deutch, któremu CIA podlegała w czasach administracji Clintona i który znalazł się pod obstrzałem zwolenników udostępnienia przez Internet tajnych danych i umożliwienia opracowywania

[43] Council of Foreign Relations — *przyp. tłum.*

tajnych dokumentów wywiadu na domowych PC-tach, przypomniał, że pojawienie się nowych zagrożeń wynikających z działań cyberwojny zatarło granicę między tworzeniem prawa a zagadnieniami bezpieczeństwa kraju. „Stare rozgraniczenia straciły sens, a okoliczności zmieniły się tak bardzo, że trzeba całą sprawę przemyśleć od nowa" — stwierdził.

-.-. -.-- -... . .-. - . .-. .-. --- .-.

Agencją, którą wydarzenia z 11 września i związane z nimi błędy skłoniły do przemyślenia polityki wywiadowczej od podstaw, jest Departament Stanu. Choć tradycyjnie niepowiązany z wywiadowczą działalnością zbierania i analizowania informacji, posiada zasoby użyteczne dla osób i instytucji, które w przyszłości mają strzec bezpieczeństwa kraju i nie dopuścić do kolejnych ataków terrorystycznych. Ale może to przynieść efekty jedynie w przypadku stworzenia odmiennej kultury działania oraz zbudowania nowej infrastruktury informacyjnej korzystającej z nowych technologii. I to właśnie planują niektórzy przedstawiciele urzędu.

Departament Stanu ma swoje placówki dyplomatyczne w 180 krajach na całym świecie. „Żadna inna agencja federalna nie ma takiej reprezentacji" — twierdzi przedstawiciel Office of Intelligence Resourcing and Planning[44]. „W ciągu najbliższych trzech lat zamierzamy zdobyć największe wpływy w tajnym świecie wywiadu" — dodaje[45].

Ale Departament Stanu nie jest w stanie tego osiągnąć bez pomocy CIA i Intelinku, a to dlatego, że zamierza połączyć wszystkie swoje przedstawicielstwa na świecie z centrum analiz wywiadowczych w Waszyngtonie, do czego potrzebne jest skorzystanie z tajnych łączy intranetowych wywiadu, czyli z Intelinku. Zadanie ma być wykonane do końca roku 2003, a na razie intelinkowe stacje robocze zostały zainstalowane w 125 przedstawicielstwach w różnych krajach na całym świecie. Tego rodzaju łączność pozwoli analitykom wywiadu na śledzenie informacji zbieranych dotąd przez służby

[44]Należące do Departamentu Stanu Biuro zasobów wywiadu i planowania — *przyp. tłum.*

[45]Patrz: Dan Verton *State Department Aims for Bigger Role in Hmeland Ssecurity* „Computerworld", 9 września 2002.

dyplomatyczne jedynie lokalnie w poszczególnych krajach. Na razie, tzn. podczas pisania tej książki, w programie szkolenia pracowników placówek dyplomatycznych nie ma obowiązkowego wstępnego kursu obsługi Intelinku, ale to się musi zmienić w najbliższej przyszłości.

Rok po atakach 11 września w Filadelfii na zorganizowanej przez Departament Obrony publicznej konferencji poświęconej sprawie bezpieczeństwa narodowego przedstawiciel służby zagranicznej Departamentu Stanu Gerald Galluci przyznał, że brak biegłości w posługiwaniu się komputerami stoi na przeszkodzie rozwinięcia współpracy służby zagranicznej ze wspólnotą wywiadowczą. „Jeszcze rok temu wielu nie miało pojęcia, że może korzystać z tajnych informacji za pomocą SIPRNET-u" — mówił Galluci. — „Teraz nadal informacje z kontynentu na kontynent przesyłamy głównie w postaci depesz"[46].

Zatem choć Departament Stanu poszukuje narzędzi, które umożliwią pracownikom służby dyplomatycznej publikowanie informacji na stronach WWW i utrzymywanie własnych stron dostępnych dla innych, przełom nie nastąpi z dnia na dzień. „Wszystko to wymaga przede wszystkim zmiany nawyków i sposobu myślenia" — przyznaje Galluci. Według jednego ze starszych menedżerów ds. technologii, „nie zawsze starsi pracownicy służby zagranicznej czują się w środowisku nowych technologii jak ryba w wodzie"[47].

Ale czasami możliwości, jakie daje technologia, po prostu brakuje. Na przykład jeden z przedstawicieli Departamentu Stanu odwiedził ostatnio Biuro Konsularne i spytał, w jaki sposób informacje o osobach starających się o wizę są udostępniane innym służbom rządowym. Odpowiedziano mu, że przez gońców dostarczających z urzędu do urzędu wydrukowane dokumenty.

Jednakże jeżeli Departament Stanu zamierza zostać liczącym się graczem w światowej rozgrywce antyterrorystycznej, będzie musiał zrobić daleko więcej niż tylko przemóc swą wrodzoną awersję do technologii, ma bowiem w swej historii wiele włamań do systemów spowodowanych nieumiejętnością korzystania z urządzeń nowej technologii i nieprzestrzegania procedur bezpieczeństwa.

---

[46]Ibidem.

[47]Ibidem.

Jedno ze szczególnie rzucających się w oczy potknięć miało miejsce kilka miesięcy po atakach terrorystycznych 11 września i polegało na wystawieniu wiz 105 osobom znajdującym się na prowadzonych przez FBI i CIA listach podejrzanych o działalność terrorystyczną. Przeoczenie było spowodowane działaniem specjalnego systemu wprowadzonego przez Departament Stanu w listopadzie 2001 i nazwanego „Visas Condor". Opracowano go specjalnie dla usprawnienia procesu wydawania wiz, przesyłania aplikacji przez ocean i sprawdzania, czy nazwiska chętnych nie znajdują się na prowadzonych przez FBI i CIA listach osób podejrzanych o terroryzm. Jednakże audyt wykonany przez General Accounting Office, śledcze ramię Kongresu, wykazał, że do kwietnia 2002 roku FBI miała zaległości i około 8 tys. nazwisk przesłanych z Departamentu Stanu przez Visas Condor czekało jeszcze na sprawdzenie. Spośród 38 tys. aplikacji załatwianych przez system w sierpniu 2002 około 280 nazwisk okazało się odnotowanych na listach antyterrorystycznych. Departament Stanu wydał mylnie owe 105 wiz osobom podejrzanym o terroryzm z powodu błędów literowych lub powtarzania się nazwisk.

W styczniu 2000 roku Sekretarz Stanu Madeleine Albright zwolniła zastępcę dyrektora Bureau of Intelligence and Research (INR)[48] i oficjalnie ukarała sześciu innych wyższych urzędników z powodu utraty laptopa, który zawierał tysiące stron supertajnych informacji zaklasyfikowanych jako „codeword", co w świecie wywiadu amerykańskiego oznacza najwyższy stopień utajnienia. Zwykle w ten sposób są klasyfikowane dokumenty dotyczące rozmieszczenia broni na świecie. Laptop zniknął z sali konferencyjnej w kwaterze głównej Departamentu Stanu w Waszyngtonie.

Ale nie tylko ten incydent mógł zaprzepaścić program bezpieczeństwa Departamentu Stanu. W grudniu 1999 odkryto wyrafinowane urządzenie podsłuchowe w poręczy fotela w sali konferencyjnej na siódmym piętrze głównego budynku Departamentu Stanu w Waszyngtonie. Umieścił je tam Stanisław Gusiew, rosyjski agent pracujący w ambasadzie rosyjskiej w Waszyngtonie, który następnie usiłował monitorować je z ukrycia z samochodu ustawionego przed

[48]Biuro wywiadu i badań, należy do Departamentu Stanu, patrz *http://www.state.gov/s/inr/ — przyp. tłum.*

budynkiem Departamentu Stanu. Nieco wcześniej, w lutym 1998, zdarzyło się, że jakiś mężczyzna wszedł do gabinetu sekretarza stanu i wyniósł stamtąd supertajne dokumenty. Nie było to wcale zaskakujące, wziąwszy pod uwagę, że wynajętym pracownikom technicznym pozwalano swobodnie poruszać się po budynku — również w strefach, gdzie nie mieli prawa przebywać bez eskorty[49].

-.-. -.-- -... . .-. - . .-. .-. --- .-.

Rewolucja technologiczna w informatyce wprowadziła zamieszanie także w operacjach wywiadowczych i kontrwywiadowczych FBI, co doprowadziło do serii żenujących, a czasem bardzo niebezpiecznych incydentów.

Dyrektor FBI Robert Mueller, który dzierżył ster głównej narodowej agencji zwalczającej zbrodnie i terroryzm, zaledwie na kilka tygodni przed atakami 11 września wielokrotnie przyznawał publicznie, że FBI nie będzie w stanie zapewnić w kraju bezpieczeństwa na oczekiwanym poziomie, jeżeli „nie zacznie stosować technologii wspierającej działania śledcze". Według Muellera, obecnie stosowane technologie informatyczne nie pozwalają na dokonywanie analiz wspierających pracę agentów w terenie. Mueller w czerwcu 2002 wielokrotnie powtarzał te komentarze w Kongresie podczas kolejnych przesłuchań dotyczących proponowanego przez niego planu gruntownej reorganizacji biura.

Najbardziej palącym problemem FBI był brak narzędzi do przeszukiwania i analizowania finansowych danych i komunikatów — takich, jakich używały CIA i NSA. Służyłyby one agentom do przeprowadzania kwerend oraz identyfikowania wzorców i zależności między danymi, ukrytymi w górach informacji zapisanych w różnych formatach. Jeden z agentów FBI określił to jako potrzebę zainstalowania wielkiego komputera mainframe, zdolnego do „rozgryzienia" tak wielkiej ilości danych i dodał, że FBI pod względem technologii pozostaje wiele lat w tyle za innymi agencjami[50]. Inni wieloletni agenci twierdzili, że stosowana w FBI filozofia inwestowania w nowe

[49]Patrz: Dan Verton *State Department to Punish Six over Missing Laptop* „Computerworld", 11 grudnia 2000.

[50]Patrz: Dan Verton *FBI Must Fix Outdated IT Infrastructure* „Computerwold", 17 czerwca 2002.

technologie przypomina założenia budowy wielkiego muru chińskiego. Było pewne, że nikt nieuprawniony nie mógł wejść do środka. Niestety, komunikowanie się ze światem zewnętrznym było również niemożliwe. Ponadto zainstalowany system zarządzający informacjami o zdarzeniach był tak skomplikowany, że część agentów wolała go po prostu nie używać[51].

Mueller przyznał także, że FBI nie utrzymuje kontaktów z innymi agencjami federalnymi, które obecnie stanowią część ogólnonarodowej infrastruktury służącej bezpieczeństwu i działaniom antyterrorystycznym. Ponad sześć miesięcy po atakach terrorystycznych 11 września biuro nadal nie może się doprosić bezpiecznego intranetu, który ułatwiłby wymianę tajnych informacji z własnymi agentami oraz z przedstawicielami innych federalnych, stanowych i lokalnych agencji.

Jednakże ten brak łączności z innymi agencjami, zwłaszcza ze stanowymi i lokalnymi strukturami policyjnymi, wynika nie tylko z braków finansowych, lecz w równej mierze z dotychczasowych przyzwyczajeń i zahamowań. Choć w liście protestacyjnym do wydawcy „Computerworldu" zostałem oskarżony o naginanie luźnych wypowiedzi do potrzeb własnej polityki, nie mogę pominąć faktu, że oficer śledczy z Departamentu Policji w Houston podczas rządowego sympozjum na temat udostępniania informacji i zagadnień bezpieczeństwa narodowego[52], które odbyło się w Filadelfii w sierpniu 2002, ostro skrytykował niechęć FBI do udzielania informacji.

„FBI jest głównym repozytorium informacji wywiadu antyterrorystycznego i jednocześnie najbardziej archaiczną bazą danych" — stwierdził oficer przed audytorium złożonym z setek oficjalnych przedstawicieli rządu i sektora prywatnego. — „Niestety, bardzo uważa, by posiadanymi informacjami z nikim się nie dzielić".

Uważają, że jeżeli ktoś ma problem, powinien przyjść z nim do nich i opowiedzieć, w czym rzecz. FBI nie rozpowszechnia analiz ani raportów przewidujących nadchodzące wydarzenia. Taki poziom i taka metoda informowania nie mogą być nadal akceptowane.

---

[51] Ibidem.

[52] Government Symposium on Information Sharing and Homeland Security — *przyp. tłum.*

Biuro nie korzysta z Internetu. Mają tylko własny intranet, dla innych niedostępny"[53].

Houston nie było jedynym miastem, w którym policja miała trudności z udziałem w kierowanych przez FBI Joint Terrorism Task Force[54]. Gdy zbliżała się pierwsza rocznica ataków terrorystycznych, pojechałem na Manhattan porozmawiać z jednym z oficerów policji, który zgodził się spotkać się ze mną pod warunkiem, że nie ujawnię jego tożsamości. Powiedział mi, że tysiącom funkcjonariuszy strzegących mostów i tuneli nakazano wypatrywanie znanych terrorystów oraz podejrzanych o terroryzm osób, które mogą jeszcze przebywać na Manhattanie. Nie dano im przy tym żadnego technologicznego wsparcia ułatwiającego sprawdzanie danych i porównywanie ich z zapisami na listach antyterrorystycznych.

„No dobrze, więc jeżeli na przykład zatrzymacie w samochodzie kogoś, kto przypomina poszukiwanego terrorystę, do kogo macie się udać, aby sprawdzić jego tożsamość?" — spytałem.

„Nazwiska i opisy podejrzanych nadajemy przez radio do kwatery głównej, a oficer dyżurny sprawdza, czy podane nazwisko figuruje na jednej z wydrukowanych list podejrzanych, które spięte razem tworzą roboczy biuletyn. Poszukiwany facet może mieć komplet fałszywych nazwisk i pseudonimów, więc to wszystko kpina" — dodaje[55].

„A co z dokumentami?" — spytałem. — „Czy ci ludzie nie muszą mieć jakichś dokumentów potwierdzających tożsamość?"

„To jeszcze większa kpina. Prosimy takiego o prawo jazdy i dowód rejestracyjny, a on nam pokazuje międzynarodowe prawo jazdy. To jest świstek papieru, który mój syn może wyprodukować na swoim komputerze" — odpowiedział.

---

[53] Patrz: Dan Verton *Cops Watching for Terrorists Say IT Support Lacking*, „Computerworld", 5 września 2002. W wysłanym później liście do wydawcy opisany oficer policji stwierdził, że ten artykuł, napisany na podstawie luźnych komentarzy jego i jego kolegów z Nowego Jorku, „jest niezgodny z duchem współpracy i wzajemnego udzielania sobie pomocy, który podkreślałem w swoim wystąpieniu. Choć FBI rzeczywiście nie dysponuje współczesnymi środkami informatycznymi potrzebnymi do walki z terroryzmem, nie jest w tym osamotnione". Z całego listu wynika, że „policja w Houston pozostaje w jak najlepszych stosunkach z FBI". Patrz „Computerworld", *http://www.computerworld.com/letters*, 23 września 2002.

[54] Połączone oddziały specjalne do walki z terroryzmem — *przyp. tłum.*

[55] Wywiad Autora.

Zgodnie z prawem stanowym obywatele obcych krajów, którzy przekroczyli granicę z międzynarodowym prawem jazdy, powinni w ciągu 30 dni wystąpić o wydanie nowojorskiego stanowego prawa jazdy. Jednakże międzynarodowe prawa jazdy to tylko kawałki papieru nie mające potwierdzenia nigdzie, więc łatwo je sfałszować.

„Jeżeli więc cudzoziemiec zostanie zatrzymany na przykład za przekroczenie prędkości i pokaże międzynarodowe prawo jazdy, policjant nie ma żadnej możliwości sprawdzenia danych w Wydziale Komunikacji[56]. Zwykle wypisujemy im wezwanie do sądu za jazdę bez prawa jazdy i życzymy miłego dnia. Potem taki jegomość za pomocą komputera zmienia nazwisko na międzynarodowym prawie jazdy, wynajmuje inny samochód i zabawa zaczyna się od nowa. Jestem pewny, że zatrzymujemy takich, którzy są na listach podejrzanych i puszczamy ich wolno"[57].

-.-. -.-- -... . .-. - . .-. .-. --- .-.

Uczciwie trzeba przyznać, że na poziomie federalnym daje się zauważyć pewien postęp, zwłaszcza jeśli chodzi o aplikacje z dziedziny najnowszych technologii przeznaczonych do udostępniania informacji i analiz wywiadowczych.

Na przykład w ciągu roku od zamachów terrorystycznych analitycy i działający w terenie agenci CIA oraz NSA usprawnili działania antyterrorystyczne dzięki zastosowaniu nowych technologii ułatwiających wyszukiwanie tekstowe i głosowe oraz dokonywanie analiz. Zakup nowych technologii był bezpośrednią odpowiedzią na nieudolność zademonstrowaną przez służby bezpieczeństwa, które nie potrafiły zapobiec atakom 11 września. Nie umiano wyśledzić, zanalizować i rozpowszechnić na czas informacji dotyczących komunikowania się terrorystów za pomocą telefonów komórkowych i używanych przez nich słów służących do przekazywania zaszyfrowanych informacji, które wskazywały, że atak ma wkrótce nastąpić.

Analitycy CIA obecnie korzystają z tzw. Name Reference Library[58] stworzonej przez Language Analysis Systems Inc. (LAS) z Herndon w Wirginii. System analizuje pochodzenia nazw, nazwisk i imion,

[56] Department of Motor Vehicles — *przyp. tłum.*

[57] Ibidem.

[58] „Podręczna biblioteka nazw/nazwisk/imion" — *przyp. tłum.*

informuje analityków, czy liczne imiona i nazwiska są podane we właściwej kolejności (Egipcjanie i Saudyjczycy często używają nazwisk związanych z wieloma pokoleniami przodków) oraz podaje informacje o sposobie ich wymawiania oraz o płci osób, które je noszą. CIA jest także zainteresowane produktem, który dopiero powstaje i który ma pozwolić na interpretację zapisów w językach narodowych. Wówczas, jeżeli któryś z analityków trafi na imię Mohamed zapisane po arabsku, będzie mógł sprawdzić, czy zapis i wymowa są właściwe, bowiem to imię wymawia się tylko w jeden sposób.

Analitycy z NSA odpowiedzialni za podsłuchiwanie, magazynowanie i analizowanie komunikatów głosowych, danych i nagrań z wideokonferencji także korzystają z osiągnięć najnowszych technologii informatycznych. Nowe oprogramowanie zakupione przez agencję pozwala na rozbijanie mowy na najmniejsze składniki zwane fonemami. Fonemy można potem indeksować i wyszukiwać według słów kluczowych. Oprogramowanie jest w stanie wychwycić z zapisu dźwiękowego dany wyraz, nazwę lub frazę niezależnie od dialektu osoby wypowiadającej słowa z 98-procentową dokładnością i do 72 tys. razy szybciej niż w czasie rzeczywistym. Dzięki temu 20-godzinny zapis dźwiękowy analitycy NSA mogą przeszukać w ciągu 1 sekundy. Dzięki laptopom mogą też korzystać z tych możliwości podczas pracy w terenie.

Po wprowadzeniu technologii usprawniających działanie poszczególnych agencji wiele osób niesłusznie sądziło, że powołanie nowego Departamentu Bezpieczeństwa Wewnętrznego[59] będzie oznaczało natychmiastową, zauważalną poprawę w udostępnianiu informacji wśród agencji i departamentów rządowych. Nic dalszego od prawdy.

Stworzenie nowego departamentu integrującego 22 poprzednio niezależne agencje i 170 tys. zatrudnionych tam ludzi być może dopiero po latach doprowadzi do wytworzenia wspólnej kultury działania i polityki bezpieczeństwa. Na razie jest to dopiero początek mozolnej drogi i większość ekspertów sądzi, że osiągnięcie wyznaczonego przez prezydenta poziomu zdolności operacyjnej nie nastąpi wcześniej niż za pięć lat. A ponieważ pełna integracja różnego rodzaju stanowych

[59] Department of Homeland Security — *przyp. tłum.*

i lokalnych jednostek wspierających przestrzeganie porządku prawnego, służb specjalnych i ratowniczych, pogotowia ratunkowego i innych jest w sposób istotny uzależnione od uruchomienia ogólnokrajowego systemu udostępniania informacji, cały proces może się przedłużyć do lat dziesięciu.

W marcu 2002 roku Biały Dom powierzył Steve'owi Cooperowi zadanie ujednolicenia tych wszystkich agencji, tak aby działały jak jedna organizacja. Cooper to były główny rzecznik Corning, Inc. Podczas pisania tej książki skupił uwagę swego personelu na budowaniu — jak to lubi nazywać — „pathfinders"[60] — elementów konstrukcyjnych, które mają pokazywać przedstawicielom władz drogę do stworzenia w pełni zintegrowanego Departamentu Bezpieczeństwa Wewnętrznego. Pierwsze Pathfinder Projects dotyczą konsolidacji różnych list osób i instytucji podejrzanych o terroryzm, aby wszystkie agencje rządowe i siły pilnujące przestrzegania prawa, mając ten sam cel taktyczny, mogły korzystać z tego samego źródła informacji i miały przed oczami ten sam obraz sytuacji. Następnym projektem jest stworzenie sieciowego portalu informacyjnego zawierającego przede wszystkim dane dotyczące ochrony krytycznie ważnych infrastruktur, co ma zapewnić dostarczanie zawsze aktualnych informacji agencjom ponoszącym odpowiedzialność za bezpieczeństwo w tej dziedzinie. Trzeci Pathfinder Project jest budowaniem koalicji zainteresowanych agencji i instytucji w celu wspierania wspólnych wysiłków upowszechnienia wymiany informacji drogą elektroniczną. Już dziesięć instytucji stanowych, z Florida Department of Law Enforcement[61] na czele, zgodziło się na współpracę w tworzeniu narzędzi mających służyć do przeszukiwania olbrzymich zasobów informacji i rozpowszechniania ich wśród zainteresowanych instytucji.

Jednakże Cooper rozumie skalę stojących przed nim zadań. „Jeszcze nie widziałem agencji federalnej, której charakter odpowiadałby potrzebom współpracy z innymi instytucjami" — powiedział w sierpniu 2002 w Filadelfii podczas Government Information

[60] Pathfinder to ktoś wytyczający, dosłownie lub w przenośni, nowe szlaki w nieznanym terenie. Czasem określa się tak również pionierskie urządzenia i rozwiązania techniczne — *przyp. tłum.*

[61] Departament sprawiedliwości Florydy — *przyp. tłum.*

Sharing and Homeland Security Conference[62]. Wypowiedział te słowa wkrótce po odmowie Kongresu przyznania żądanych przez rząd funduszy na stworzenie centralnego biura integracyjnego w nowym Departamencie Bezpieczeństwa Wewnętrznego. „Jak wynika z naszych informacji, oni po prostu nie wierzą, że to może być wykonane" — powiedział Cooper.

-.-. -.-- -... . .-. - . .-. .-. --- .-.

Z powodu biurokratycznych, zwyczajowych, kulturowych i prawnych przeszkód stojących na przeszkodzie rzetelnemu i dokonywanemu na czas udostępnianiu informacji, walka z terroryzmem będzie w najbliższym czasie spoczywać niemal wyłącznie na barkach stanowej i lokalnej policji i sił ratowniczych. Cieszy informacja, że niektóre z wielkich metropolii amerykańskich rozpoczęły na własną rękę przygotowania do obrony przed atakiem.

Na przykład w Bostonie latem 2000 zainicjowano pilotażowy projekt o nazwie Boston Prepardness Pilot[63], którego celem jest uzyskanie dostępu do zasobów National Imaginery and Mapping Agency (NIMA)[64] oraz do materiałów wywiadowczych Departamentu Obrony. Projekt bostoński wyrasta z większego ogólnonarodowego programu znanego jako 120 Cities Project[65], który ma upowszechnić wśród stanowych i lokalnych służb ratunkowych informacje uważane przez NIMA za „minimalny poziom geoprzestrzennej gotowości".

Przedstawiciele bostońskiej policji otrzymali od NIMA 100 plików map cyfrowych, z których jedna przedstawia miasto z dokładnością do sześciu cali. Są na niej zaznaczone wszystkie lokalne szkoły, sklepy spożywcze, szpitale, posterunki policji, budynki rządowe, urządzenia przemysłowe, ważne znaki orientacyjne, mosty, autostrady, parkingi i systemy wodne. Ale dane otrzymane od NIMA nie są jedynie płaskimi plikami. Są to tak zwane „pliki inteligentne", co oznacza, że kliknięcie jakiejś instalacji zaznaczonej na mapie

---

[62]Patrz: Dan Verton *Congressman Says Data Mining Could Have Prevented 9-11* „Computerworld", 26 sierpnia 2002.

[63]W wolnym tłumaczeniu „projekt pilotażowy bostońskiej gotowości" — *przyp. tłum.*

[64]Narodowa Agencja Obrazowania i Kartografii — *przyp. tłum.*

[65]Projekt 120 miast — *przyp. tłum.*

powoduje wyświetlenie wartościowych danych dotyczących tego obiektu. Pozwala to służbom ratunkowym na szybkie sprawdzenie, ile łóżek jest dostępnych w danym szpitalu albo ilu pracowników może się danego dnia znajdować w jakimś biurze. Policjanci mają też dostęp o krytycznych danych dotyczących konstrukcji mostów, stadionów sportowych i innych wielkich konstrukcji użyteczności publicznej, które mogą się stać pierwszymi celami ataków terrorystycznych, gdyż spowodowałyby masowe ofiary. Boston i inne miasta korzystają także z innego pakietu oprogramowania, znanego jako Consequence Application Toolset[66], stworzonego przez Defense Thread Reducton Agency[67] oraz Science Applications International Corporation (SAIC)[68] z San Diego. Jest to oprogramowanie pozwalające planistom szybko ocenić skalę ataku chemicznego, biologicznego lub nuklearnego i ocenić w sekundach czas przenoszenia się skażeń w danym rejonie geograficznym wraz z obliczeniem liczby zagrożonych budynków i ludzi. Wyniki są otrzymywane przez aktualizację w czasie rzeczywistym danych o pogodzie, co pozwala na określenie szybkości i zasięgu rozchodzenia się toksycznego obłoku.

Stoi przed nami wyzwanie stworzenia ogólnonarodowego systemu informacyjnego udostępniającego dane ogólne i wywiadowcze, które lokalne władze i służby ratunkowe będą mogły otrzymać wystarczająco szybko, by na ich podstawie stworzyć plany ewakuacyjne, a to może oznaczać uratowanie dziesiątków tysięcy istnień ludzkich. Broń jądrową, biologiczną i chemiczną musimy tu traktować jednakowo.

---

[66]W wolnym tłumaczeniu „zestaw narzędzi do oceny konsekwencji" — *przyp. tłum.*

[67]W wolnym tłumaczeniu „agencja bezpieczeństwa ds. zmniejszani zagrożeń" — *przyp. tłum.*

[68]Międzynarodowa korporacja zastosowań naukowych — niezależna firma konsultingowa i ośrodek przeprowadzający oceny zastosowania badań naukowych w technikach informacyjnych, a także integrację systemów informatycznych; patrz *http://www.saic.com/* — *przyp. tłum.*