

# ZAGROŻENIA W CYBERPRZESTRZENI A PRZESTĘPSTWA EKONOMICZNE

Jerzy Wojciech WÓJCIK<sup>1</sup>

*Powstające systematycznie nowe technologie to czynnik, który powoduje, że od momentu powstania cyberprzestrzeni, trwa największa cicha wojna. Żołnierze to wyspecjalizowani eksperci informatyki, analitycy informacji, specjaliści wywiadu i kontrwywiadu gospodarczego. W cyberwojnę angażowane są duże pieniądze, a więc bierze w niej udział zarówno światowa finansjera, media, politycy, jak i przestępcy.*

*W referacie zwrócono uwagę na kryminologiczne i kryminalistyczne aspekty manipulowania informacjami zawartymi w cyberprzestrzeni. Wszelkie dane uzyskane zarówno w sposób legalny, jak i nielegalny mogą być wykorzystane w sposób sprzeczny z prawem. Skutkować to może różnorodnymi przestępstwami o charakterze ekonomicznym, a szczególnie wyrafinowanymi oszustwami finansowymi.*

*W związku z tym najbardziej zagrożone są instytucje finansowe, a szczególnie banki. Na nich spoczywa obowiązek zapewnienia bezpiecznego funkcjonowania oraz poczucia bezpieczeństwa klientów, a zatem konieczność wypracowywania skutecznych zabezpieczeń.*

## 1. WPROWADZENIE

Funkcjonowanie współczesnego życia społecznego i gospodarczego, a szczególnie informowanie i komunikowanie opiera się na przede wszystkim na osiągnięciach najbardziej energicznie rozwijającej się technologii informacyjnej. Z osiągnięć tej dziedziny korzystają wszyscy, najczęściej w sposób zgodny z prawem. Jednakże jak zwykle niektórzy ludzie dążą do osiągnięcia swoistych celów, nie zawsze zgodnych z zasadami życia społecznego, normami etycznymi i prawnymi tym bardziej, że nieprecyzyjne prawo ułatwia działalność przestępcom. Przykładowo, rozwijający się na całym świecie cyberbiznes wykorzystywany jest również przez zawodowych oszustów. Wbrew ustalonym zakazom rośnie liczba usług w zakresie handlu farmaceutykami, alkoholem, e-hazardu. Oprócz innych skutków państwo ponosi duże szkody z powodu braku wpływów podatkowych. Można nawet dostrzec bez specjalnych analiz, że w rękach nieuczciwych użytkowników Internetu e-mail stał się wymarzoną narzędziem dla fałszerzy i oszustów.

Współczesne wydarzenia, które miały miejsce w wielu regionach świata, kiedy to przez specjalistyczne działania doprowadzono do kradzieży cennych danych, czy do zablokowania internetowych stron wielu instytucji strategicznych, a szczególnie rządowych, bankowych i wielu mediów, to dowód, że cyberterrorizm jest realnym zagrożeniem dla bezpieczeństwa państwa.

Manipulowanie informacjami uzyskanymi zarówno w sposób legalny, jak i nielegalny skutkować może różnorodnymi przestępstwami, z których najbardziej groźnymi mogą okazać się również czyny o charakterze ekonomicznym<sup>2</sup>.

Powszechnie znana jest przede wszystkim komunikacyjna i informacyjna, a także edukacyjna, integracyjna, handlowa, biznesowa, a nawet randkowa rola Internetu. Jednakże równocześnie dokładniej rozpoznawane są również ciemne strony tego komunikatora. Spośród rozpoznawanych wciąż nowych zagrożeń o charakterze kryminalnym szczególna rola przypada cyberterrorizmowi, uznanemu współcześnie jako nowe zagrożenia nie tylko dla światowych mediów. To właśnie cyberprzestrzeń stworzyła klimat na powstanie nowych form i metod działania wyspecjalizowanych przestępców, których zainteresowania kierowane są na niezmiernie bogate i interesujące obszary zawierające wiele dóbr, jak np. towar w postaci informacji. Jeżeli informacja jest towarem to ochrona informacji jest kwestią strategiczną.

Nowe technologie, a także powstanie cyberprzestrzeni to czynnik, który powoduje, że od momentu jej powstania trwa największa cicha wojna. Żołnierze to wyspecjalizowani eksperci informatyki, analitycy informacji, specjaliści wywiadu i kontrwywiadu gospodarczego, a także wielu innych dziedzin. W cyberwojnę angażowane są duże pieniądze, a więc światowa finansjera, media, politycy i zorganizowani przestępcy.

<sup>1</sup> Prof. dr hab. Jerzy Wojciech Wójcik Wyższa Szkoła Informatyki Zarządzania i Administracji w Warszawie

<sup>2</sup> Niniejsze opracowanie jest kontynuacją wcześniejszych rozważań dotyczących wielopłaszczyznowych aspektów zorganizowanej przestępczości gospodarczej, a zagrożeń w cyberprzestrzeni w szczególności oraz zagadnienia kryminalistycznego śladu transakcyjnego mającego istotne znaczenie dla celów dowodowych. Szerzej: J.W. Wójcik, *Oszustwa finansowe. Zagadnienia kryminologiczne i kryminalistyczne*, Wydawnictwo JWW, Warszawa 2008, s. 336-385, więcej informacji o książce na stronie [www.jww.waw.pl](http://www.jww.waw.pl)

## 2. POJĘCIE I ZAKRES CYBERPRZESTRZENI, CYBERPRZESTĘPCZOŚCI I CYBERTERRORYZMU

*Cyberprzestępczość, cyberterroryzm, cyberfraud, cyberszpieg, cyberbanking, cyberlaundering*, a także *cyberprzemoc, cyberstalking*, czyli cybermolestowanie, to tylko niektóre nowe terminy, z którymi warto się zapoznać, gdyż ich pojawienie się może świadczyć o nasilaniu się negatywnych zjawisk społecznych w tej wciąż bardziej atrakcyjnej przestrzeni.

Zagadnienie definicji wzbudza wiele kontrowersji. Należy jednak stwierdzić, iż cyberterroryzm to określenie dotyczące posługiwania się zdobyciami technologii informacyjnej w celu wyrządzenia szkody z pobudek politycznych lub ideologicznych, zwłaszcza w odniesieniu do infrastruktury o istotnym znaczeniu dla gospodarki lub obronności atakowanego kraju. Pojęcie cyberterroryzmu jest obiektem publicznego zainteresowania, a spekulacje dotyczące tego zagadnienia znacznie nasiliły się po zamachach 11 września 2001 w USA. Jako typowe cele ataków przywoływane są systemy kontroli lotów, infrastruktura bankowa, elektrownie, czy systemy dostarczania wody. Mimo tych spekulacji, nie odnotowano dotychczas udanych ataków cyberterrorystycznych, które prowadziłyby do poważnych strat dla atakowanych organizacji, a katastroficzne wizje przedstawiane przez niektórych publicystów często odrzucane są przez informatyków jako oparte na nierealnych założeniach<sup>3</sup>.

W Polsce zaczęto poważnie traktować zjawisko cyberterroryzmu dopiero z początkiem XXI wieku. Dały temu wyraz niektóre uczelnie<sup>4</sup>.

Warto przy tym podkreślić, że jeżeli znanych jest ponad 200 definicji samego terroryzmu, należy się również liczyć z systematycznymi próbami wielu autorów dążących do dokładnego zdefiniowania zjawiska cyberterroryzmu.

Aktualnie społeczeństwa posługują się informacją, która jest również towarem, traktowanym jako szczególne dobro niematerialne, równoważne lub cenniejsze nawet od dóbr materialnych. Przewiduje się wciąż szybki rozwój usług związanych z przechowywaniem, przesyłaniem i przetwarzaniem informacji.

Cyberprzestrzeń, cyberprzestępczość i cyberterroryzm to terminy ściśle ze sobą powiązane. Natomiast cyberterroryzm to pojęcie używane już w latach 80. XX wieku przez amerykańskich specjalistów w dziedzinie wywiadu wojskowego. Jednakże niektórzy autorzy uważają, że pojęcie cyberprzestrzeni, a wraz z nią nowy typ zagrożenia, czyli cyberprzestępczość, narodziła się w momencie powstania politycznej koncepcji „autostrad informacyjnych”, w czasie kampanii prezydenckiej Billa Clintona, w 1992 roku. Koncepcja ta zakładała, że wszelkiego typu informacje zawierające tekst, dźwięk i obraz będą mogły być przekazywane na duże odległości szybko i bez przeszkód. Świat globalnej sieci coraz bardziej się rozrastał i stawał się coraz bardziej podobny do świata rzeczywistego, a zatem zarówno przestępczość, jak i terroryzm znalazły swoje miejsce w przestrzeni wirtualnej. Natomiast zmasowane ataki na komputery zanotowano pod koniec lat 90. ubiegłego wieku.

Przekazywanie różnorodnych wiadomości, zapisywanie ich do dziennika informacji o wiadomościach i połączeniach, zdalne podsłuchiwanie i potajemne zestawianie połączeń, a także usługi lokalizacyjne, oto niektóre tylko elementy mogące stanowić niezwykle istotną bazę danych dla zorganizowanych przestępców, a cyberterrorystów w szczególności. Metody działania są zróżnicowane, od prostych aż do zainstalowanej w pełni funkcjonalnej aplikacji szpiegowskiej, co całkowicie pozbawia prywatności podczas rozmów, gdyż osoba kontrolująca oprogramowanie ma dostęp do wszystkich informacji.

Narzędzia tego typu mogą posłużyć do szpiegostwa przemysłowego, kradzieży tożsamości i danych, podszywania się pod inne osoby, aż do oszustw finansowych na szkodę instytucji finansowych i ich klientów.

Przykłady podobnych działań można oczywiście mnożyć. Jednak większość ekspertów nazywa je nie cyberterroryzmem, a po prostu cyberprzestępczością, a dokładnie hackingiem, hackingiem politycznym, wojną informacyjną, cyberwojną, hakytywizmem czy po prostu zwykłym wandalizmem. Jaka jest różnica pomiędzy tymi zjawiskami? W jaki sposób można je zdefiniować?

Brak definicji w międzynarodowych aktach prawnych i bałagan terminologiczny w polskim ustawodawstwie skłania do różnorodnych spekulacji i nie zawsze do słusznych wniosków. Przykładowo, cyberterroryzm (zwany czasem *soft terrorism*) – to działania blokujące, niszczące lub zniekształcające informację przetwarzaną, przechowywaną i przekazywaną w systemach teleinformatycznych oraz niszczące

<sup>3</sup> <http://pl.wikipedia.org/wiki/Cyberterroryzm>

<sup>4</sup> Por. np.: J.W. Wójcik, *Zagrożenia systemu bankowego*. Referat wygłoszony 9 maja 2001 roku w Szkole Głównej Handlowej na konferencji *Bezpieczeństwo w Sieci. Cyberterroryzm 2001*, która została zorganizowana przez Studenckie Koło Naukowe Badań nad Przestępczością Gospodarczą i Bezpieczeństwem w Biznesie. Szerzej: <http://www.sgh.waw.pl/instytuty/ism/materialy/CYBERTERRORYZM%202007.pdf>

(obezwładniające) te systemy. W pojęciu tym mieści się także wykorzystywanie systemów teleinformatycznych do dezinformacji, walki psychologicznej itp. Celem ataku jest najczęściej informacja przetwarzana, a nie system jako taki.

Dorothee Denning, profesor uniwersytetu w Georgetown, amerykańska specjalistka od cyberterrorizmu trafnie określa, że są to bezprawne zamachy lub ich groźby na sieci i systemy komputerowe oraz informacyjne. Ale tylko wtedy, gdy są to zamachy w celu zastraszenia czy zmuszenia władz do spełniania określonych żądań politycznych lub społecznych. Takie działania muszą mieć skutki o cechach przemocy wobec osób i mienia, powodować istotne szkody, by wzbudzać strach, prowadzić do śmierci, uszczerbku na zdrowiu, eksplozji, a także dużych szkód majątkowych<sup>5</sup>.

Zdaniem tej autorki sieć komputerowa jest wprost wymarzoną polem działania dla terrorystów, a możliwe akcje cyberterrorystyczne to takie działania, które polegają przykładowo na:

- rozmieszczeniu kilku skomputeryzowanych bomb w mieście, wszystkie transmitują określony kod, który dociera do każdej z nich. Jeśli transmisja zostanie przerwana, bomby zostaną symultanicznie zdetonowane;
- dokonaniu włamania do systemu finansowego państwa pod groźbą jego całkowitego sparaliżowania i wysuwania kolejnych żądań;
- zaatakowaniu systemu kontroli powietrznej i doprowadzeniu do zderzenia dwóch samolotów pasażerskich, grożąc następnymi;
- dokonaniu zmian w komputerowych recepturach na podstawie których produkowane będą lekarstwa;
- wprowadzeniu zmiany zasadniczego ciśnienia w gazociągach, co niewątpliwie grozi spowodowaniem eksplozji<sup>6</sup>.

Według innej specjalistki w dziedzinie cyberprzestępczości – Solange Ghernaoui – Helie, profesora Ecole des Hautes Etudes Commerciales w Lozannie, cyberprzestępczość przyjmuje coraz częściej wymiar cyberterrorizmu, gdyż zasoby informatyczne związane z krytyczną infrastrukturą niezbędną do życia dla jakiegoś kraju są dostępne przez Internet, a właśnie przejęcie kontroli nad owymi krytycznymi infrastrukturami, czyli energią, wodą, transportem, telekomunikacją, bankowością i finansami, służbami medycznymi, instytucjami rządowymi, jest celem cyberterrorystów. Jednak cyberprzestępczość jest faktem, a cyberterrorizm wciąż jeszcze pozostaje fikcją. Wydaje się bowiem, że „człowiek-bomba” to skuteczniejsza metoda na przeprowadzenie ataku, niż opanowanie bardzo dobrze strzeżonych systemów informatycznych instytucji mających strategiczne znaczenie dla infrastruktury krytycznej. Stwierdzenie powyższe może potwierdzić fakt, że przed 11. września Bin Laden straszył świat planowanymi atakami cyberterrorystycznymi, mówił, że Al-Kaida jest gotowa użyć komputerów jako broni w walce o swoje ideały, kiedy jednak przyszło mu działać, posłużył się klasycznymi metodami terrorystycznymi<sup>7</sup>.

Zatem cyberprzestępczość może równać się cyberterrorizmowi, czyli przejęciem kontroli nad krytycznymi infrastrukturami: energią, wodą, transportem, telekomunikacją, bankowością i finansami, służbami medycznymi, instytucjami rządowymi.

Mark Pollit, specjalista FBI, podaje bardzo szeroką definicję cyberterrorizmu. Podkreśla, że słowo to jest kombinacją dwóch innych: *cyberprzestrzeni* i *terrorizmu*: „jest to celowy, motywowany politycznie atak przeciw informacji, systemom komputerowym, programom komputerowym i danym, który skierowany jest przeciw niewalczącym celom przez grupy subnarodowe lub przez podziemnych agentów”. Pollit zwraca jednocześnie uwagę, iż należy go odróżniać od innych nielegalnych aktów, takich jak przestępczość komputerowa, szpiegostwo gospodarcze czy też wojna informacyjna<sup>8</sup>. Do tej ostatniej zaliczyć można zjawisko określane jako hakytywizm, czyli „manifestacje o charakterze propagandowopolitycznym”.

Internet jest też wykorzystywany przez terrorystów do celów propagandowych w tym wzniesienia niepokoju, szerzenia nienawiści, a ogólnie do prowadzenia wojny psychologicznej. Znane są powszechnie ich groźby, a nawet pokazywane akty egzekucji dziennikarzy i innych osób, w tym członków akcji humanitarnych.

---

<sup>5</sup> D. E. Denning, *Activism, haktivism and cyberterrorism: The Internet as a tool for influencing foreign Policy*, w: J. Arquilla, D. Ronfeldt, *Networks and Netwars*, Santa Monica 2001, s. 239-262.

<sup>6</sup> Tamże, autorka wyróżnia również hakytywistów (*hacktivists*), którzy mogą mieć poczucie siły, bowiem potrafią kontrolować komputery rządowe i zyskiwać rozgłos w mediach, chociaż to nie znaczy, że mogą zmieniać politykę.

<sup>7</sup> <http://www.sgh.waw.pl/instytut/ism/materialy/CYBERTERRORYZM%202007.pdf>

<sup>8</sup> M. Pollit, *Cyberterrorism – fact or fancy?*,

[http://cyberpolice.free.fr/cybercriminalite/cyberterrorisme\\_factorfantasy.html](http://cyberpolice.free.fr/cybercriminalite/cyberterrorisme_factorfantasy.html);

Nie można pominąć również wykorzystywania Internetu przez organizacje terrorystyczne do zdobywania środków finansowych: tą drogą uzyskują one ogromne sumy. Według informacji FBI już w latach dziewięćdziesiątych dokonywano kradzieży komputerowych na sumę 3-7,5 mld dolarów, a ponadto organizacje te czerpią olbrzymie środki ze skradzionych kart kredytowych, sfingowanych przelewów elektronicznych czy wymuszeń na bankach, do których banki te nawet się nie przyznają.<sup>9</sup>

Wychodząc z tezą określającą terroryzm jako ideologię i pieniądze należy podkreślić istotne znaczenie zagadnienia finansowania terroryzmu<sup>10</sup>, nie tylko w ramach legalnej działalności gospodarczej, lecz przede wszystkim zdobywania środków w ramach cyberterroryzmu. Podstawowym warunkiem działalności, a także jak wykazuje praktyka śledcza, warunkiem powodzenia w realizacji planów terrorystów jest niejednokrotnie niezbędne zdobycie dużych funduszy. Wówczas to dochodzi dopiero do realizacji poszczególnych etapów aktu terrorystycznego, a w szczególności poprzez:

- 1) nawoływanie do aktu terrorystycznego,
- 2) rozpoznanie środowiskowe,
- 3) werbowanie kandydatów na członków grupy,
- 4) uzyskanie funduszy,
- 5) pozyskanie zaplecza logistycznego, przygotowanie fałszywych dokumentów stwierdzających tożsamość itp.,
- 6) szkolenie i sprawdzenie nabytych umiejętności,
- 7) rozpoznanie miejsca przestępstwa i wykonanie czynności przygotowawczych,
- 8) podłożenie ładunku wybuchowego i odpalenie lub
- 9) podłożenie ładunku wybuchowego i samozniszczenie.

### 3. INTERNET A WOJNA IDEOLOGICZNA

Publicyści od kilku lat twierdzą, że w cyberprzestrzeni toczy się wojna na śmierć i życie między al-Kaidą a antyterrorystami.<sup>11</sup> Przykładowo, Mohamed Omar Bakri, radykalny imam z Londynu, już kilka lat temu groził, że al-Kaida wykorzysta sieć komputerową do zadania ciosu Zachodowi. Należy zatem przewidywać najgorsze scenariusze w tej kwestii, gdyż przepowiadany kilka lat temu informatyczny dżihad stał się faktem. Te ciosy są zadawane giełdom papierów wartościowych, bankom, elektrowniom atomowym i innym instytucjom o charakterze strategicznym, jak ataki na komputery wieże kontroli lotów i inne systemy komunikacyjne. Tak twierdzi Yonah Alexander, dyrektor Międzynarodowego Centrum ds. Terroryzmu przy amerykańskim uniwersytecie Potomac, który jest współautorem opracowania będącego rezultatem prac nad terroryzmem, na podstawie materiałów pochodzących z ostatnich kilku lat, dostępnych na międzynarodowych seminariach i konferencjach, a także licznych informacjach przedstawianych w mediach, sprawozdań z rozpraw sądowych oraz przedsięwzięć badawczych podejmowanych na Bliskim Wschodzie, Azji i Europie.<sup>12</sup>

Groźby al-Kaidy początkowo uznano za czcze przechwałki, jednakże obecnie potwierdza się, że Internet stał się niebezpieczną bronią w rękach radykałów, gdyż wszystkie liczące się skrajne organizacje mają swoje strony, na których szerzą ideologię, zbierają fundusze i rekrutują nowych członków. Potencjalni zamachowcy, zamiast jechać do obozów szkoleniowych dla terrorystów, mogą przejść kurs przy komputerze. Internet stał się również nieocenionym narzędziem w wojnie propagandowej. Zamieszczane tam zdjęcia z egzekucji zakładników wielokrotnie szokowały zachodnią opinię publiczną.

Ekstremiści w ciągu paru lat do perfekcji opanowali sztukę wykorzystywania Internetu do walki ideologicznej. Teraz szukają sposobów, by dezorganizować życie zachodnich społeczeństw i powodować straty w gospodarce. Dowody i skutki zaistniałych zamachów w sieci systematycznie dostarczane są przez media.

### 4. TERRORYŚCI Z CYBERPRZESTRZENI

Kiedy Timothy Lloyd, 30-letni informatyk, w 1998 r. został zwolniony po 11 latach pracy z firmy Omega w Wilmington w stanie Delaware, wykonującej zamówienia rządu USA w postaci wyspecjalizowanych urządzeń elektronicznych dla marynarki wojennej, stało się coś, czego nikt jeszcze wówczas nie przewidywał. Pewnego dnia pracownicy Omegi nie mogli rozpocząć rutynowych działań, gdyż ich komputery świeciły pustkami, a komputer centralny utracił 80% danych. Wyniki śledztwa przeprowadzonego przez FBI i kontrwywiad były szokujące. Okazało się, że bomba logiczna, którą skonstruował zwolniony informatyk,

<sup>9</sup> B. Hołyst, *Terroryzm*, LexisNexis, Warszawa 2009, t. 1, s. 763, 764.

<sup>10</sup> Szerzej: J.W. Wójcik, *Przeciwdziałanie finansowaniu terroryzmu*, Wolters Kluwer business, Kraków 2007.

<sup>11</sup> N. Labi, *Dżihad w sieci*, Rzeczpospolita z dnia 22-23 lipca 2005 r.

<sup>12</sup> Y. Alexander, M. S. Swetnam, *Siewcy śmierci. Osama Bin Laden i inni szefowie Al.-Quaidy*, Bellona 2001 oraz [www.jgm.gov.ar/Paginas/MemoriaDetallada04/Anexos2004MinRelaciExteriores.pdf](http://www.jgm.gov.ar/Paginas/MemoriaDetallada04/Anexos2004MinRelaciExteriores.pdf)

spowodowała straty w wysokości 10 mln USD nie tylko w postaci straconych zamówień, lecz również w kosztach odbudowy informacji w bazach danych.

Niezwykłe efekty działania kolejnego uzdolnionego hakera stały się już kanwą przynajmniej kilku sensacyjnych filmów fabularnych. A co najmniej jeden z nich dotyczył możliwości wywołania światowego konfliktu atomowego. Jeszcze przed kilkunastu laty produkcja hollywoodzkich filmów science fiction zawierała niewyczerpane wprost pomysły. Jeden z nich polegał na włamaniu się do komputerowego systemu kontroli lotów i udzielaniu złych wskazówek pilotowi samolotu podchodzącego do lądowania z kompletem bezbronnych pasażerów. Rzeczywistość wielokrotnie przerosła jednak świat fantazji poprzez terrorystyczne zamachy pilotów–samobójców.

Czy cyberterrorysty zdecydują się na ataki, aby siać grozę, czy też osiągnąć swoje cele polityczne? Takie pytania zadają sobie nie tylko specjaliści od spraw terroryzmu komputerowego. Czy kandydaci na terrorystów mogą wykorzystywać podobne pomysły? Eksperci badający najnowsze formy terroryzmu nie mają w tym zakresie wątpliwości. Twierdzą nawet, że cyberterrorysty mogą być groźniejsi od terrorystów działających z karabinami i bombami. Uzasadnieniem tej tezy może być stwierdzenie: jeżeli haker włamie się do systemu komputerowego kierującego ruchem metra i doprowadzi do zderzenia dwóch pociągów, to w takiej katastrofie zginie więcej osób niż w trakcie indywidualnej strzelaniny czy podłożeniu ładunku wybuchowego.

Czy zatem haker żądny krwi to terrorysta, który być może zechce panować nad miastem, a nawet krajem? Wciąż dość trudnym i niezwykle istotnym problemem jest ustalenie miejsca, z którego działa taki specjalista. Trudno jest określić, czy siedzi on przed komputerem umieszczonym w sąsiednim domu, czy też w innym kraju lub na innym kontynencie po drugiej stronie globu. Śledzenie włamywaczy komputerowych jest już możliwe, lecz wymaga wyjątkowych umiejętności, urządzeń i programów, ponadto jest bardzo kosztowne. Nawet przeciętni hakerzy potrafią doskonale zacierać ślady swojej bytności w cudzym komputerze i w odległych krańcach Internetu. Mimo to jednak można ich zidentyfikować, ale czy w określonym zdarzeniu nie będzie już za późno?

Zarówno CIA, jak i FBI, a także New Scotland Yard i inne służby specjalne, jak również polska policja posiadają wyspecjalizowane jednostki prowadzące inwigilację komputerową poczynań hakerów, pedofilów itd. Pomagają im najnowsze osiągnięcia techniki. Wciąż niezbędna jest jednak fantazja albo raczej z pomocą przyjść może fikcja literacka autorstwa Stanisława Lema czy Toma Clancy'ego. Ich czytelnicy doskonale pamiętają o pomysłach i rozwiązaniach, które z pewnością były inspirujące dla wielu naukowców i wynalazców. Chociażby stosowane obecnie różnorodne technologie satelitarnego podsłuchu czy podglądu w ich dziełach nie były niczym niezwykłym, czyli wówczas gdy nikt jeszcze nie potrafił tego dokonać. Podobnie było z elektronicznymi systemami rozpoznawania śladów biologicznych, czyli biometrycznych<sup>13</sup>, jak np.: kodów wizerunku, głosu, śladów linii papilarnych, tęczy oka itp.

Już w latach osiemdziesiątych i dziewięćdziesiątych ubiegłego wieku zanotowano wiele włamań do pilnie strzeżonych systemów komputerowych w wielu krajach. W związku z tym już wówczas rozpoczęto działania profilaktyczne poprzez edukację wybitnych specjalistów od bezpieczeństwa teleinformatycznego, manipulacji hakerów, a także możliwości działania terrorystów komputerowych. Wspomniana tematyka była przedmiotem wykładów w tajnej, elitarnej szkole Sił Specjalnych USA.

Na temat zdolnych hakerów i informatyków istnieje już dość obszerna literatura. Spośród nich wyróżnia się Ehud Tenenbaum, pseudonim Analityk, 18-letni Izraelczyk, to najbardziej tajemnicza postać świata hakerów — niezwykle uzdolniony w pokonywaniu zabezpieczeń systemów teleinformatycznych i chlubiący się dostępem do 120 tys. kont klientów bankowych. Swoje zdolności i możliwości udowodnił w przesłanych do FBI hasłach dostępu do kilku rządowych sieci. Wszystkie były autentyczne. Ze swoich zdolności nie uczynił użytku i nie spowodował strat. Stał się jednak przedmiotem badań ekspertów do spraw terroryzmu komputerowego. Zastanawiali się oni nad możliwymi skutkami „wpadki” Analityka czy innych utalentowanych hakerów nie w ręce policji, lecz w sidła terrorystów, np. Al-Kaidy, Hezbollahu czy innej organizacji, która niekoniecznie chciałaby zapłacić za dane będące w zakresie możliwości działania włamywacza komputerowego, lecz zmusiłaby go do udostępnienia takich danych na rzecz organizacji. Na razie

---

<sup>13</sup> Biometria to termin wywodzący się z greckich słów *bio* (życie, żywy, procesy życiowe) i *metrics* (mierzyć), określa się jako zespół metod służących do sprawdzania tożsamości osób (autoryzację) poprzez analizę ich cech fizycznych czy behawioralnych. To współcześnie technika dokonywania pomiarów istot żywych, a także ukierunkowane metody automatycznego rozpoznawania ludzi na podstawie ich cech dla celów bezpieczeństwa. Przykłady biometrycznych cech anatomicznych to: zapach, linie papilarne, geometria dłoni, geometria i rysy twarzy, rozkład temperatury twarzy, geometria ucha, geometria ust, cechy charakterystyczne tęczy oka i siatkówki oka, układ żył nadgarstka, identyfikacja DNA.

do tego nie doszło, a także do przewidywanych w tym przypadku tragedii. Tymczasem jednak aresztowanie Analityzera stało się przyczyną wzięcia odwetu na amerykańskich sieciach komputerowych przez innych włamywaczy<sup>14</sup>.

Należy zwrócić szczególną uwagę na fakt, że terrorystami XXI w. określono tych informatyków, którzy działają lub będą działać, posługując się metodami Timothy'ego Lloyda. Od terrorystów w tradycyjnym tego słowa znaczeniu dzielą ich zasadnicze różnice. Obce im są brutalne metody fizyczne, a przede wszystkim ćwiczenia na rozpalonych piaskach pustynnych. Nie stosują agresywnych i skutecznych w zabijaniu walk Wschodu, nie zabijają, a także nie podkładają ładunków wybuchowych.

Ten rodzaj terrorystów to absolwenci renomowanych uczelni, pasjonujący się naukami sprzyjającymi rozwojowi wiedzy i intelektu. Ich hobby to np.: elektronika, matematyka, statystyka, informatyka czy budowa tranzystorów. Nie wzbudzają większego zainteresowania. Pracują w zaciszu swoich pracowni komputerowych. Jednakże skutki ich działalności mogą być nieobliczalne, trudne do przewidzenia, katastroficzne...

Przewidywane scenariusze zagrożeń powodowanych przez terrorystów– informatyków opracowywane są w Centrum Studiów Strategicznych i Międzynarodowych w Waszyngtonie. Tam też powstał scenariusz dotyczący możliwości manipulacji w systemie komputerowym pogotowia ratunkowego w dużym mieście. Terrorysta może na przykład wysłać wszystkie karetki pogotowia w jedno miejsce, w którym uzbrojeni napastnicy zorganizowali zasadzkę. To samo mogą uczynić ze strażą pożarną. W taki właśnie sposób w przeciągu kilkudziesięciu minut zorganizowana grupa terrorystyczna może sparaliżować życie dużego miasta, gdyż odpowiednie służby zostaną wyłączone z możliwości interwencji w niewralgicznych punktach, tj. w miejscach rzeczywistych zagrożeń.

Już 10 lat temu prognozy dotyczące informatycznych ataków terrorystycznych na duże organizacje państwowe, obiekty strategiczne i instytucje finansowe wydawały się bardzo realne. Nikt jednak nie rozwiązał problemu: kiedy one nastąpią i jak im skutecznie przeciwdziałać? Czy walka z tego rodzaju terrorystami wymaga dużych nakładów finansowych? Z pewnością w obecnych warunkach zagrożeń wymaga nowej strategii przeciwdziałania.

Odnosząc się do czarnych wizji komputeryzacji, można częściowo przyznać rację Wiliamowi Gibsonowi<sup>15</sup>. Zdarzają się bowiem sytuacje, z których jasno wynika, że informatyk może być groźny dla swojego środowiska. Dochodzić może nawet do swoistych ataków terroru nakierowanych nie tylko na systemy instytucji finansowych czy naukowych, ale także na instytucje związane z bezpieczeństwem i porządkiem publicznym, jak wcześniej wspomniane np.: pogotowie ratunkowe, szpitale, straż pożarna, policja czy służby specjalne.

Kolejne niebezpieczeństwo, równie groźne, stanowią terroryści z cyberprzestrzeni. Świadczy o tym następujący przykład. Przed sądem w Sarajewie 20 lipca 2006 r. stało trzech członków pierwszej na świecie wirtualnej komórki terrorystycznej. Rok temu byli o krok od przeprowadzenia zamachu. Jej członek, Mirsad Bektasević, rozpoczął działalność jako 17-letni muzułmanin z Bośni, znany w sieci jako Maximus. Pierwszymi, z którymi nawiązał kontakt, byli muzułmanie z Danii. Najmłodszy miał 14 lat. Wymieniali się linkami do stron terrorystycznych i podsyłali podręczniki Al-Kaidy o tym, jak szkolić terrorystów, nie dać się złapać i zrobić prostą bombę. Świat prawdziwego dżihadu stanął przed nimi otworem w dniu, w którym na jednym z czatów natknęli się na internautę o pseudonimie „irhabi007”, czyli terrorysta. Pojawił się w sieci w lutym 2004 r., zaczynał od wrzucania na różne strony internetowe informacji o zamachach. Już w lipcu dokonał spektakularnego wyczynu — włamał się do serwera departamentu dróg i transportu stanu Arkansas i zamieścił na jego stronie teksty o dżihadzie oraz linki do stron terrorystycznych. Od tego czasu był śledzony przez FBI. Dla grupy wirtualnych terrorystów kradł i rozprowadzał w sieci m.in. podręczniki szkoleniowe CIA i podręczniki amerykańskiej marynarki wojennej dla snajperów. Zamieszczał prezentacje wideo, jak przygotować samochód pułapkę, szkolił innych, wyjaśniał, jak zacierać za sobą ślady w sieci. Teorię postanowili wprowadzić w życie. Zatem we wrześniu 2005 r. Bektasević wyciągnął od matki pieniądze na podróż „do cioci w Sarajewie” i ruszył do ojczyzny. W tym samym czasie do Sarajewa wybrał się z Kopenhagi Cesur Abdulkadir, z którym znał się wirtualnie. Spotkali się na miejscu, wynajęli mieszkanie i

<sup>14</sup> Szerzej: J. W. Wójcik, *Przestępstwa komputerowe, cz. I - Fenomen cywilizacji*, CIM, Warszawa 1999, s. 162.

<sup>15</sup> Przejawom terroru komputerowego poświęca się uwagę w literaturze ze względu na przewidywane rozprzestrzenianie się i nasilanie tego typu zagrożeń. Szerokie zastosowanie Internetu, a także negatywne skutki w postaci opanowania świata przez bezwzględnie działające korporacje przewidział amerykański pisarz *science fiction* W. Gibson w swojej powieści *Neuromancer* wydanej w 1984 r. Jemu także przypisuje się autorstwo terminu „cyberpunk”.

zaczęli przygotowywać zamach. Jego celem miały być ambasady amerykańska, brytyjska albo baza sił pokojowych EUFOR położona około 100 m od ich mieszkania. Bomby chcieli umieścić na sobie, by zdobyć sławę męczenników za wiarę i trafić do raju. Po aresztowaniu przez bośniackie służby specjalne 19 października 2005 r. policja znalazła w ich mieszkaniu 30 kg materiałów wybuchowych, broń, pas zamachowca–samobójcy i nagrane na kasecie wideo przesłanie, które miało ukazać się po zamachu.

Dalszych zatrzymań dokonały policje w Wielkiej Brytanii, Danii, Kanadzie, USA i Bangladeszu. W Londynie wpadł „irhabi007”, którym okazał się urodzony w Wielkiej Brytanii 22–letni Yusin Tsouli. Dwóch członków grupy z USA miało planować zamach z użyciem samochodu pułapki w Waszyngtonie. Łącznie zatrzymano 17 osób, które planowały serię zamachów, m.in. na metro i wieżę telewizyjną. Prokuratura zarzuca im też, że przygotowywały szturm na parlament, gdzie chciały ściąć głowę premiera Stephena Harpera.

Internet od dawna jest wykorzystywany przez terrorystów islamskich. Od trzech lat donoszą o tym raporty holenderskiego wywiadu. Okazało się bowiem, że część członków skazanej z początku 2006 r. w Holandii grupy Hofstad zwerbowano właśnie w sieci. To może być niepomyślna wiadomość dla służb specjalnych, gdyż wirtualni dżihadysty nie chodzą do radykalnych meczetów, nie spotykają się ze znanymi fanatykami i nie jeżdżą na szkolenia do Pakistanu i Afganistanu<sup>16</sup>.

Przykład grupy Maximusa dobitnie wskazuje, jak trudnym zagadnieniem jest rozpoznanie terrorystów w liczącym już miliardy stron Internecie. Pomimo że „irhabi007” nie był zawodowym informatykiem, przez półtora roku na oczach służb specjalnych prowadził działalność, szkolił i zorganizował grupę terrorystyczną. Natomiast ci członkowie, którzy mieli być wykonawcami zamachów, pozostawali całkowicie niezauważeni.

## 5. TERRORYŚCI NUKLEARNI

Przeciwdziałaniem terroryzmowi nuklearnemu na forum ONZ zajmuje się UN Action Against Terrorism, który powołał komitet ds. zwalczania tego rodzaju zjawiska. Na temat realności zagrożeń 10 marca 2005 r. wypowiedział się sekretarz generalny ONZ Kofi A. Annan: „(...) musimy pozbawić terrorystów możliwości dokonywania zamachów. Chodzi o to, by utrudnić im podróżowanie, korzystanie z finansowego wsparcia lub nabywanie materiałów nuklearnych lub radiologicznych. Terroryzm nuklearny jest wciąż zaliczany przez wiele osób do sfery fantastyki naukowej. Chciałbym, żeby tak było. Niestety, żyjemy w świecie pełnym niebezpiecznych materiałów i możliwości technologicznych. Niektórzy terroryści otwarcie dążą do spowodowania katastrof, w których giną ludzie.

Zarówno szefowie G-8, jak i Rada Bezpieczeństwa Narodów Zjednoczonych podejmują kroki, których celem jest eliminacja niebezpiecznych materiałów, wprowadzenie skutecznej kontroli ich eksportu oraz uszczelnienie systemu zapobiegającego ich rozprzestrzenianiu. Kolejnym, ważnym krokiem jest powołana przez prezydenta Busha Inicjatywa na rzecz Bezpiecznego Rozprzestrzeniania (Proliferation Security Initiative) tych substancji. Takie działania muszą spotkać się z pełnym poparciem<sup>17</sup>.

Wypowiedź sekretarza generalnego oraz podjęte przez ONZ kroki organizacyjne świadczą o powadze zagrożeń. Potwierdzają to informatorzy Reuters'a. Agencja ta podała, że w marcu 2006 r. aresztowano siedmiu Brytyjczyków, powiązanych z Al-Kaidą, podejrzanych o planowanie zamachów terrorystycznych w Wielkiej Brytanii. Planowali oni m.in. wysadzenie jednego z największych w kraju centrów handlowych i największego klubu nocnego w Londynie. Ujawniono również, że jeden z podejrzanych planował nawet kupić bombę nuklearną od rosyjskiej mafii. Zakup miał być dokonany w Belgii, a kontakt z mafią został nawiązany przez Internet. Jednakże okazuje się, że "Stany Zjednoczone nie są gotowe na poważny atak terrorystyczny wykonany za pośrednictwem Internetu" – taki komunikat został ogłoszony w grudniu 2008 r. przez przedstawicieli amerykańskich władz oraz firm związanych z branżą IT. *"Nie istnieje żaden konkretny plan, ani nawet sposób działania. Nie ma również jednego organu, który koordynowałby wszystkie prace mające na celu zwiększenie internetowego bezpieczeństwa obywateli, firm oraz państwa."* W trakcie symulacji przykładowego ataku okazało się, że w przypadku poważnego konfliktu teoretycznie możliwe jest wykonanie zamachu na amerykańskie elektrownie czy banki<sup>18</sup>. Nieoficjalnie wiadomo, że podobnego zdania jest prezydent Barack Obama. W niedalekiej przyszłości można się więc spodziewać zwiększonych nakładów na ochronę amerykańskich systemów informatycznych, a przede wszystkim profesjonalnych przedsięwzięć organizacyjnych.

<sup>16</sup> P. Szczerkowski, *Proces terrorystów z cyberprzestrzeni*, Gazeta Wyborcza z 21 lipca 2006 r.

<sup>17</sup> Ośrodek Informacji ONZ w Warszawie, [www.unic.un.org.pl/terroryzm/organyoniz.php](http://www.unic.un.org.pl/terroryzm/organyoniz.php)

<sup>18</sup> IDG.pl/Jakub Kuchnio, *USA: "Nie jesteśmy przygotowani na cyberterroryzm"*

<http://www.securitystandard.pl/news/330567/USA.Nie.jestesmy.przygotowani.na.cyberterroryzm.html>

## 6. TERRORYŚCI EKONOMICZNI

Współczesnymi celami działania wszelkiego rodzaju terrorystów jest zniszczenie gospodarki bogatych krajów. Warto również zauważyć, że cyberterroryzm ma tę przewagę nad terroryzmem konwencjonalnym, że ani nie wymaga środków, ani nie stwarza zagrożenia dla samego przestępcy, powoduje natomiast niewyobrażalne skutki ekonomiczne. Jednakże w odróżnieniu od przestępstw gospodarczych związanych z technologią cyfrową i działalnością hakerów jest zjawiskiem bez porównania groźniejszym

Celem ataków terrorystycznych jest przede wszystkim paraliż gospodarczy. Na przykład po ataku na Bali w 2002 r. gospodarka tej części Indonezji — oparta głównie na turystyce — musiała się przez dwa lata odbudowywać. Świadczą o tym również inne cele ataków.

Terroryści coraz częściej atakują na morzu. Natomiast skutki tych ataków mogą mieć znaczenie globalne. Okazuje się, że zagadnienie skoordynowanych ataków na centra gospodarcze może mieć skutki katastrofalne w skali globalnej. Singapurski Instytut Badań Obronnych i Strategicznych przeprowadził niedawno symulację ataku terrorystycznego na międzynarodowy port morski. Okazało się, atak na infrastrukturę takiego portu, jak Singapur, przez który między Wschodem i Zachodem przechodzi co roku niemal 24 mln kontenerów (nie licząc innych ładunków), zakłóciłby cykle produkcyjne w skali całego świata, powodując straty przekraczające 200 mld USD. W takim przypadku paraliż światowej gospodarki byłby realną groźbą.

Pewną zapowiedzią takiej sytuacji są systematyczne ataki terrorystów na ropociągi w Iraku, ostatnio również w krajach afrykańskich, np. w Nigerii, po których cena ropy osiągnęła gwałtowny skok. Należy spodziewać się również innych zagrożeń w gospodarce. Ponadto ataki w krajach charakteryzujących się dużym ruchem turystycznym, jak np. Egipt czy Indonezja, mają właśnie na celu sparaliżowanie ich gospodarki. Zastosowany już w 2001 r. atak działań finansowych na giełdy papierów wartościowych również miał zachwiać gospodarką Zachodu, pozbawić społeczeństwa poczucia stabilizacji i ekonomicznego bezpieczeństwa.

Powagę zagrożeń ekonomicznych wywoływanych przez terrorystów, potwierdzają wyniki sondażu przeprowadzonego w lutym 2006 r. wśród członków amerykańskiej organizacji ekonomistów. Na zagrożenia terroryzmem w gospodarce wskazało 26% ankietowanych, natomiast 20% — na zagrożenia związane z cenami energii.

Okres kryzysu finansowego czy gospodarczego stwarza nowe okazje i szerokie możliwości zarówno dla zorganizowanych grup przestępców kryminalnych, jak i gospodarczych. Wiadomo bowiem, że pieniądze pochodzące z nielegalnych źródeł najczęściej przypominają strumień wody zawsze płynący w tym kierunku, w którym napotyka on na najmniejszy opór. Natomiast wprost niezwykle szkodliwą rolę mogą odegrać cyberprzestępcy. Związane jest to z kolejnym terminem, jakim jest cyberbank, który może działać wszędzie, nawet w najmniejszej miejscowości lub w cyberprzestrzeni.

Informatycy, a szczególnie eksperci w zakresie bezpieczeństwa ostrzegają, że w 2009 roku dojdzie do rewolucji w zakresie cyberprzestępczości<sup>19</sup>. Jednakże brak jest konkretnej prognozy kryminologicznej. Wprawdzie internetowych przestępców, a szczególnie oszustów jest w Polsce coraz więcej. W 2007 roku rozpoznano ich o połowę więcej niż rok wcześniej. Aktualni przestępcy stają się jeszcze bardziej dokuczliwi, gdyż dobierają się również do telefonów komórkowych i popularnych portali społecznościowych.

Czy można zaryzykować tezę, że wszystko zaczyna się od cyberpiractwa? Jeśli już co drugi uczeń na świecie w wieku 9-14 lat ściąga muzykę, gry, a starsza młodzież ściąga programy, filmy i inne pliki, czym narusza cudzą własność intelektualną. Zainteresowania tego typu mogą rozwijać się w różnych, nie zawsze pozytywnych kierunkach. Warto zatem prowadzić badania kryminologiczne na temat dalszych zainteresowań i ich skutków realizacji tego rodzaju zainteresowań młodych użytkowników Internetu.

Jednym z zagadnień badawczych jest zagadnienie tworzenia i rozsyłania wirusów, robaków, koni trojańskich itp. Czasami uzdolniony student - internauta bawi się tworzeniem wirusów<sup>20</sup>. Kolejny problem to kiedy i z jakich powodów dochodzi do tego, że dostęp do określonych witryn za pomocą wirusa jest niejednokrotnie sprzedawany konkurencyjnym firmom. Natomiast blokowanie serwerów może być powodem olbrzymich strat ekonomicznych. Natomiast ich odblokowanie odbywa się niejednokrotnie poprzez wymuszanie opłat.

<sup>19</sup> Kaspersky Lab, *Zagrożenia* <http://www.kaspersky.pl/cyberthreats.html>

<sup>20</sup> D. Ferbrache, *Patologia wirusów komputerowych*, Wydawnictwa Naukowo – Techniczne, Warszawa 1993, s. 37 i n.

Od kilku lat w stanie wojny elektronicznej znalazły się Stany Zjednoczone i ChRL. Przykładowo, w maju 2001r., kiedy to amerykańscy hackerzy zaatakowali masowo chińskie strony internetowe. W odpowiedzi Chińczycy włamali się na strony amerykańskiej administracji i wielkiego biznesu. Obyło się bez wielkich strat materialnych, ale efekt pozwolił zdać sobie sprawę z tego jak mogą wyglądać wojny w przyszłości. Eksperti chińscy twierdzą, że nie oni rozpoczęli tę wojnę. Z wielu napływających informacji wynika, że niewątpliwie biorą w niej aktywny udział. Z kolei eksperci amerykańscy angażują olbrzymie środki w nasłuch i analizę danych<sup>21</sup>. Natomiast przedstawiciele wywiadu USA obawiają się, że cyberszpiecy mogą przejąć kontrolę nad elektrowniami atomowymi i sieciami finansowymi. Podobno ślady prowadzą nie tylko do Chin lecz również do Rosji<sup>22</sup>.

Pod koniec października 2002 roku świat obiegła również kolejna elektryzująca wiadomość, podana przez FBI. Zaatakowanych zostało 13 podstawowych serwerów DNS, które „tłumaczą” adresy internetowe na numeryczne adresy IP, wykorzystywane przez komputery, ich całkowite zablokowanie mogłoby spowodować zupełny paraliż Internetu.

Natomiast na skutek działania haktivistów, którzy również modyfikują zawartości stron www, czy je podmieniają albo stosują środki zakłóceń elektronicznych przeciwko wrogim witrynom, czyli na ich kasowaniu, ale też na atakowaniu wirusami i zablokowaniu – doszło do poważnych strat ekonomicznych<sup>23</sup>. Inny przykład to internetowa strona arabskiej telewizji Al-Dżazira, nastawionej wyraźnie antyamerykańsko, która przestała nagle działać w marcu 2003. Zamiast strony głównej portalu pojawiała się amerykańska flaga i napis: „niech zabrzmi wolność”.

## 7. TERRORYŚCI FINANSOWI - KOLEJNE „NAJWIĘKSZE” AFERY BANKOWE I GIEŁDOWE

Realne poglądy na wady i niedociągnięcia systemu kontroli bankowej czy giełdowej wyłaniają się wówczas, gdy mamy do czynienia z kolejną aferą, określaną zazwyczaj jako „największa”<sup>24</sup>. Ich znakomita większość dotyczyła transakcji zawieranych drogą elektroniczną. To samo dotyczyło wpłat i wypłat, przelewów, analiz i prognoz finansowych, różnorodnych zleceń inwestycyjnych, czy spekulacyjnych, a przede wszystkim ofert zarówno dla zwykłych klientów, jak i potężnych inwestorów. Na przełomie XX i XXI wieku dość często dochodzi do rozpoznawania „największych” afer bankowych i giełdowych. Jednakże określenie „największa” zawsze dotyczy tej ostatniej, gdyż kolejna ujawniona okazuje się jeszcze większa.

Spośród wielu afer bankowych i giełdowych warto wymienić kilka najbardziej znanych charakteryzujących się zarówno największymi szkodami, jak i wyrafinowanymi metodami działania zarówno szefów, jak i personelu, a mianowicie:

- 1991 r. - Bank of Credit and Commerce International (BCCI) - upadek po udzieleniu serii ryzykownych i nielegalnych kredytów i przeprowadzeniu podobnych transakcji, które skutkowały stratami ok. 10 mld USD. Zdaniem prokuratora okręgowego w Nowym Jorku był jedną z najbardziej skorumpowanych i tajemniczych organizacji kryminalnych na świecie. Historia tego banku, jego powstanie, rozwój, działalność i upadek są bardzo pouczające. Zakończyła się tajna operacja policyjna pod kryptonimem "C-Chase". Aresztowano wiele osób, a w tym 9 urzędników BCCI z USA i Wielkiej Brytanii. Przykładowo, oddział w Londynie prowadził tajny oddział, który udzielał porad nt. oszustw podatkowych i prania pieniędzy. Udowodniono 28 przypadków prania pieniędzy na sumę przynajmniej 20 mld USD. Jedną z wielu sensacji był fakt zatrudniania, dla potrzeb inwestorów, przez oddział w Karachi (Pakistan) kilkunastu prostytutek, z których najstarsza miała 18 lat. Zamknięcie banku spowodowało pozostawienie "na lodzie" ponad 530 tys. wierzycieli z całego świata i długi na kwotę 12,4 mld USD<sup>25</sup>;
- 1995 r. - Barings - Nick Leeson, diler Baringsa z Singapuru, ryzykownymi operacjami na rynku azjatyckim spowodował straty w wysokości 1,3 mld USD. Osłabiony Barings został potem przejęty przez holenderski ING Bank. Leeson, który na tych transakcjach osobiście nic nie zyskał, został w

<sup>21</sup> Por. np.: M. Janik, *Mao śledzi cały świat*, oraz M. Zawadzki, *Chińska wojna w sieci*, Dziennik z 30 marca 2009 r.

<sup>22</sup> S. Gorman, *Szpiecy penetrują sieć energetyczną USA*, Dziennik – THE WALL STREET JOURNAL. POLSKA z 16 kwietnia 2009 r.

<sup>23</sup> *Cyberterrorisme: l'arme absolue sur Internet*,

[http://cyberpolice.free.fr/cybercriminalite/cyberterrorisme\\_armeabsolue.html](http://cyberpolice.free.fr/cybercriminalite/cyberterrorisme_armeabsolue.html);

<sup>24</sup> Szerzej: J.W. Wójcik, *Oszustwa finansowe. Zagadnienia kryminologiczne i kryminalistyczne*, Wydawnictwo JWW, Warszawa 2008, s. 62 i n.

<sup>25</sup> Szerzej: J.W. Wójcik, *Kryminologiczna ocena transakcji w procesie prania pieniędzy*, Twigger, Warszawa 2001, s. 210-216 oraz podana tam literatura.

Singapurze skazany za oszustwo na karę pozbawienia wolności. Po kilku latach został deportowany do W. Brytanii. Napisał książkę i scenariusz filmu opartego na własnych przeżyciach. Dzisiaj jest zamożnym obywatelem brytyjskim i prezesem klubu piłkarskiego w Irlandii;

- 1997 r. - Yamaichi Securities – na transakcjach giełdowych straciła 2,1 mld USD;
- 1998 r. - Sumitomo - Yasuo Hamanaka, makler który naraził japońską korporację na straty wysokości 2,6 mld USD na ryzykownych transakcjach giełdowych;
- 2002 r. - AIB Allfirst - John Rushnak, makler należącego do irlandzkiego banku oddziału w Baltimore, zaangażował się w ryzykowne transakcje finansowe, które przyniosły 750 mln USD strat. Przez kilka miesięcy fałszował dokumenty, aby zamaskować efekty swojej działalności. Wierzył, że zdoła je odrobić. FBI udowodniła Rushnakowi, że jeszcze na tym zarobił, bo otrzymywał najróżniejsze gratyfikacje (bilety na imprezy sportowe, pokrycie kosztów podróży, turnieje golfa) od współpracujących z nim brokerów Citibanku w Nowym Jorku;
- Luty 2004 r. - to polski akcent, którym została sprawa określana jako „100 sekund”. W dalszym ciągu prowadzone jest śledztwo w sprawie tej transakcji giełdowej. Makler Bankowego Domu Maklerskiego PKO BP złożył dwa duże zlecenia na kontrakty terminowe. W ten sposób wywołał niespodzianie gwałtowne zmiany notowań. Wszystko to przewidział tajemniczy inwestor z brytyjskich Wysp Dziewiczych. Wystarczyło mu 100 sekund, by kosztem BDM PKO BP i kilkuset nieświadomych inwestorów warszawskiej giełdy, tajemniczy inwestor zarobił 2,6 mln zł.;
- Wrzesień 2006 r. - Amaranth Advisors - stracił 6,6 mld USD w dziesięć dni. Przyczyną tej katastrofy był upadek funduszu hedgingowego<sup>26</sup> zarządzanego przez Amaranth Advisors LLC. Zaliczano to do najbardziej spektakularnych katastrof, które zdarzyły się na globalnym rynku finansowym na przełomie XX i XXI wieku, obok podobnych wypadków jakie stały się udziałem banku inwestycyjnego Barings, prowadzonego przez laureatów Nagrody Nobla w dziedzinie ekonomii R. Mertona i M. Scholesa funduszu LTCM oraz Enron Corporation. Obecnie wiemy jednak, że wszelkie rekordy w tym względzie pobił Jerome Kerviel, 31 letni makler SG. Amaranth - był klasycznym funduszem hedge, czyli prywatną firmą, w której udziały kupowali zamożni inwestorzy - zarówno indywidualni, jak i instytucje. Przez pięć wcześniejszych lat zarobił dla swoich inwestorów 162 procent, a w ciągu jednego miesiąca stracił 50 procent w wyniku "serii wyjątkowo nieprzewidzianych zdarzeń" na rynkach związanych z gazem ziemnym.<sup>27</sup> Zdarzenie to było wręcz szokujące, gdyż do ostatniej chwili inwestorzy i analitycy rynkowi nie dostrzegali sygnałów zbliżającej się katastrofy;
- Wrzesień 2007 r. - Credit Agricole S.A. - makler stracił na ryzykownych transakcjach 230 mln euro. To największa pod względem ilości klientów grupa bankowa we Francji, która powstała do obsługi finansów francuskich rolników;
- Styczeń 2008 r. - Jerome Kerviel 31-letni makler spowodował straty 4,9 mld euro (7,1 mld USD) strat na szkodę Societe Generale;
- Marzec 2009 r. – Bernard Madoff powszechnie znany 70 letni finansista z Wall Street, były szef giełdy NASDAQ przed sądem w Nowym Jorku, przyznał się do wszystkich 11 zarzutów dotyczących oszustw finansowych, prania pieniędzy, fałszerstwa dokumentów finansowych i kradzieży. Po aresztowaniu w grudniu 2008 r. został uznany za największego w historii USA oszusta finansowego. Przyznał, że od lat 80. ub. wieku prowadził oszukańcze inwestycje w formie piramidy aferzysty z lat 20. XX wieku, tj. systemu Ponziego<sup>28</sup> czym spowodował straty na ponad 50 mld USD. Grozi mu za to kara 150 lat pozbawienia wolności. Prowadził on firmę Bernard L. Madoff Investment Securites, która była „funduszem funduszy” czyli inne banki i fundusze powierzały jej pieniądze swoich klientów w zarządzanie. Były to najbardziej znane fundusze i banki, które mając nadmierne zaufanie nie kontrolowały firmy Madoffa, nie reagowały na sygnały o nieprawidłowościach, nie domagały się przejrzystego raportowania o wynikach inwestycji, które zawsze były ponad wszelką średnią zysków. Zarówno ofiary, jak i eksperci nazywają go terrorystą i finansowym seryjnym mordercą. Przez jego fundusz przepłynęło 177 mld USD, a oskarżyciel domaga się zwrotu tej sumy. Klientami Madoffa

<sup>26</sup> Fundusz hedgingowy (z ang. *Hedge fund*) - to rodzaj instytucji finansowej pobierającej opłatę za zarządzanie powierzonym kapitałem, w którym dokonuje się kupna i krótkiej sprzedaży papierów na rynku kapitałowym w celu ograniczenia ryzyka wahań cen obejmujących swoim zasięgiem cały rynek dla maksymalizacji zysków. Jego najważniejszą cechą jest osiąganie wysokiej stopy zwrotu zarówno podczas hossy jak i bessy na rynku. Fundusze hedgingowe charakteryzują się bardzo wysokim ryzykiem inwestycyjnym a ich strategia inwestycyjna jest często agresywna i spekulacyjna. Szerzej: [www.wikipedia.pl](http://www.wikipedia.pl)

<sup>27</sup> <http://www.skarbiec.biz/inwestycyjne-fundusze/wiadomosci/amaranth.htm>

<sup>28</sup> Wnikliwe omówienie systemu Ponziego patrz: J.W. Wójcik, *Oszustwa finansowe*, wyd. cyt., s. 280 i n.

były nie tylko instytucje finansowe, lecz również gwiazdy filmowe z Hollywood, fundacje i uniwersytety.

Internet w szczególności nadaje się zarówno do dużych transakcji kasynowych, giełdowych, czy piramid lub małych inwestycji łańcuskowych. Wciąż ujawniane są kolejne piramidy czy łańcuszki finansowe. Kolejna z nich ujawniona w lipcu 2007 roku tygodniami rozsyłała użytkownikom polskiej Sieci do skrzynek e-mail, na konta wiadomości serwisów społecznościowych, na fora dyskusyjne i na ekrany komunikatorów - informację zachęcającą do inwestowania swoich pieniędzy w celu szybkiego ich pomnożenia<sup>29</sup>. Użytkownicy zazwyczaj są zapraszani do lawinowego systemu inwestowania. Powszechnie wiadomo, że mechanizm piramidy pozwala inwestować każdemu, lecz wzbogacić się tylko uczestnikom pierwszych dwóch lub trzech segmentów. Pozostali – pomimo zapewniających informacji, że jest inaczej po prostu tracą na rzecz szefów i tych, którzy szybko zdecydowali się realizować zyski. Jedna z „mini kas” zachęca do uiszczenia opłaty w wysokości 5 PLN na jeden z podanych w treści rachunków bankowych i przesłania wiadomości dalej z dopisaniem swojego rachunku do listy. Użytkownik wabiony jest możliwością szybkiego wzbogacenia się o 15 tysięcy złotych. Niektóre wersje zawierają też instrukcje dotyczące zakładania rachunku bankowego za pośrednictwem Internetu. Jest to pochodna poprzedniej piramidy, przy czym istotna zmiana w stosunku do poprzedniego wariantu polega na zastosowaniu rachunków bankowych jako metody przekazywania środków między ogniwami systemu. Podobno wśród zasobów WWW funkcjonuje około tysiąca witryn poświęconych różnym formom łańcusków i piramid finansowych zachęcających do uczestnictwa i inwestycji w systemie.

## 8. WYBRANE ZAGROŻENIA

### 8.1. Kategorie cyberprzestępczości

Truizmem jest stwierdzenie, że przestępcy wykorzystują również Internet, który zapewnia różnorodne formy komunikowania i zdobywania informacji. Umożliwia nowy styl życia m.in. poprzez możliwość informowania, wymiany danych i poglądów, uczenia się, zawierania transakcji. Daje nam do dyspozycji e-maile, SMS-y, pliki i komunikatory jak np.: Skype, Gadu-Gadu i inne. Umożliwia dostęp do niezwykle obszernych i interesujących nas danych. Można zatem stwierdzić, że Internet sprzyja rozwojowi gospodarki narodowej, lecz umożliwia także kontakty i transakcje przedstawicieli środowisk patologicznych i przestępczych.

Rozpoznano już szereg tego typu przestępstw mających szczególne związki z nielegalnym biznesem w Internecie. Są to przykładowo:

- 1) usługi finansowe *on-line* jak: zakup akcji, propozycje udziału w wirtualnym hazardzie, czy zaproszenia do wirtualnych kasyn gry, oszustwa nigeryjskie, pranie pieniędzy w formie cyberprania – *cyberlaundering*,
- 2) naruszenie praw autorskich poprzez plagiaty, oferty pisania na zamówienie i sprzedaż prac dyplomowych,
- 3) pedofilia i twarda pornografia,
- 4) nieuczciwa konkurencja i szpiegostwo gospodarcze,
- 5) nielegalny handel gatunkami ginącymi lub zagrożonymi wyginięciem (trofea zrobione z takich zwierząt są wystawiane w internetowych domach aukcyjnych, tak samo jak zrobione z nich medykamenty i afrodyzjaki),
- 6) zakup leków bez recepty z zagranicy, które są zabronione w innym państwie, lub które nie przeszły całej procedury dopuszczenia do sprzedaży,
- 7) nielegalny handel antykami, dziełami sztuki itp.,
- 8) nielegalny handel bronią, materiałami wybuchowymi, amunicją, a także pomocnictwo w skonstruowaniu bomb (instruktaż),
- 9) handel żywym towarem - Internet jest wykorzystywany do przyciągnięcia potencjalnych ofiar ofertami pracy za granicą, itp.
- 10) dystrybucja utworów i materiałów o charakterze nazistowskim, rasistowskim, lub szerzących nienawiść rasową itp.<sup>30</sup>

Ten indeks nie jest zamknięty i można go uzupełnić o wiele innych czynów, jak np.: niszczenie informacji, oszustwa i fałszerstwa, haking, podsłuch, sabotaż, piractwo, phishing, nieuczciwą konkurencję, cybersquatting i inne. Zatem, nawet same oszustwa przy użyciu komputera trudno jest wszystkie określić,

<sup>29</sup> <http://www.heise-online.pl/news/Piramida-finansowa-w-polskim-Internecie--/item/483/>

<sup>30</sup> Por. np.: W. Filipkowski, *Internet – przestępcza gałąź gospodarki*, Prokurator nr 1(29) 2007 oraz J.W. Wójcik, *Oszustwa finansowe*, wyd. cyt., s. 336 i n.

gdyż powstają wciąż nowe, a aktualnie brak jest branży, która nie jest zmuszona posługiwać się technologią teleinformatyczną.

Istotnym zagadnieniem kryminologicznym, związanym z przestępczością internetową jest duża ciemna liczba tego rodzaju przestępstw. Jeżeli ujawniono brak szkody lub szkodę minimalną, z zasady nie powiadamia się organów ścigania w obawie przed utratą dobrej reputacji firmy pomimo, że przestępstwo jest ścigane z oskarżenia publicznego.

Próbę podziału zagrożeń ujęto w Komunikacie Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów KOM(2007) 267 wydany w Brukseli dnia 22 maja 2007 r. dotyczący ogólnej strategii zwalczania cyberprzestępczości<sup>31</sup> wskazuje na rangę współczesnych zagrożeń. Zwraca uwagę na fakt, że trudno jest uzyskać dokładny obraz obecnej sytuacji ze względu na ciągły rozwój przestępczości i brak wiarygodnych informacji. Można jednak zauważyć kilka ogólnych trendów, a przykładowo:

- 1) liczba przestępstw informatycznych stale wzrasta, działania przestępcze stają się też coraz bardziej wyrafinowane i wykraczają poza granice państwowe;
- 2) wyraźne przesłanki wskazują na rosnący udział w cyberprzestępczości zorganizowanych grup przestępczych;
- 3) nie wzrasta jednak liczba aktów oskarżenia na podstawie transgranicznej współpracy organów ścigania w Europie.

Wspomniane zagrożenia podzielone są w cytowanym komunikacie na dwie podstawowe grupy. Pierwsza, to tradycyjne przestępstwa w sieciach łączności elektronicznej, w których szczególnie popularnymi i częstymi formami są różnego rodzaju oszustwa i ich usiłowania. Do popełniania oszustw na masową skalę używane są takie metody jak kradzież tożsamości, *phishing*, *spam* oraz złośliwe wirusy. Rosnącym problemem staje się również nielegalny krajowy i międzynarodowy handel internetowy. Obejmuje on handel narkotykami, bronią oraz zagrożonymi gatunkami zwierząt.

Druga, to przestępstwa typowe dla sieci teleinformatycznych. W tej kwestii coraz częstsze stają się ataki na skalę masową, skierowane przeciwko systemom informatycznym, organizacjom i osobom prywatnym (często za pośrednictwem tzw. botnetów). Ostatnio zaobserwowano również przypadki systematycznych, dobrze skoordynowanych bezpośrednich masowych ataków na krytyczne infrastruktury informatyczne kilku państw. Sytuację pogarsza łączenie technologii i coraz częstsze powiązania między systemami informatycznymi, co sprawia, że są one bardziej podatne na takie ataki. Ataki te są często bardzo dobrze zorganizowane, a ich celem jest zdobycie określonych informacji lub blokada systemów. Ponadto, wyrażone jest przekonanie, o czym wspominaliśmy wcześniej, że liczba zgłoszonych ataków jest zaniżona, przede wszystkim ze względu na straty, jakie mogłoby przynieść przedsiębiorstwom upublicznienie informacji o problemach z bezpieczeństwem.

## 8.2. Wyniki analiz Internet Fraud Complaint Center – inwazja oszustw

Wyniki analiz Internet Fraud Complaint Center (Centrum Zgłaszania Oszustw Internetowych) określają rozmiary zagrożeń<sup>32</sup>. Pierwszy raport IFCC ogłosiło z wynikami badań na temat nadużyć popełnionych w cyberprzestrzeni w 2001 roku. Na szczególną uwagę zasługują skargi dotyczące:

- 1) oszustw na aukcjach internetowych. Dotyczyło to aż 42,8 procent wszystkich skarg. Okazało się, że blisko 10 tysięcy Amerykanów zostało okradzionych w Internecie na łączną sumę 178 mln USD, co daje przeciętnie 435 dolarów na jedno oszustwo;<sup>33</sup>
- 2) niedostarczenia towarów kupionych za pośrednictwem Internetu lub niezapłacenia za nie – 20,3 proc.;
- 3) listy nigeryjskie, które stanowiły 15,5 proc. spraw. Zostały one uznane za najniebezpieczniejsze spamy finansowe. Obserwuje się ich największy wzrost. Aktualnie są to najczęściej e-maile wysyłane przez oszustów podających się za wysokich przedstawicieli rządu Nigerii. Obiecują oni przelać na konto łatwowiernej ofiary wielomilionową sumę, której część zamierzają potem odebrać, a resztę pozostawić jako zapłatę za udostępnienie konta. Najpierw jednak proszą o przesłanie im pewnej sumy na opłaty transakcyjne lub inne, a gdy sumę tę otrzymają, ślad po nich ginie.
- 4) kradzieże z kart kredytowych i debetowych stanowią 9,4 proc. oszustw;

<sup>31</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:PL:HTML>

<sup>32</sup> Internet Fraud Complaint Center utworzono w 2000 roku przy współudziale FBI. Patrz: [www.ifccfbi.gov](http://www.ifccfbi.gov)

<sup>33</sup> W Polsce systematycznie wzrastają o 50 proc. rocznie zakupy przez Internet. Wzrastają również oszustwa na aukcjach internetowych. W grudniu 2007 r. grupa zorganizowanych oszustów „sprzedawała” po 550 złotych płaskie telewizory i laptopy. Nabywcy nie zwrócili uwagi, że ceny nie są adekwatne do nabywanych towarów. Zatem stracili pieniądze i nie otrzymali towaru.

- 5) najwięcej oszustw internetowych, bo aż 93,4 proc. łącznej ich liczby, zgłoszono w 2001 roku w Stanach Zjednoczonych.

Mając na względzie rangę zagrożeń cyberprzestępstwami w grudniu 2003 roku Internet Fraud Complaint Center (IFCC) został przemianowany przez FBI na Internet Crime Complaint Center (IC3). Ta nowa instytucja opracowała wyniki kolejnych badań w dokumencie zatytułowanym "IC3 2006 Internet Crime Report"<sup>34</sup>. Jest to już szósta roczna edycja informacji o skargach i przestępstwach otrzymanych i wyjaśnianych przez IC3, a także o regulacjach prawnych agencji uprawnionej do odpowiednich działań.

Warto również dodać, że *modus operandi* sprawców cyberoszustw istotnie związany jest z kontaktami teleinformatycznymi, gdyż 73,9% omawianych przestępstw popełniono przy pomocy poczty elektronicznej i 36,0% poprzez wykorzystanie strony internetowej. Natomiast poprzez tradycyjne kontakty telefoniczne popełniono o wiele mniej przestępstw, tj. 17,7%.

Z rozpoznania dokonanego przez służby FBI, nie tylko w USA, lecz również w wielu innych krajach świata, także w Polsce potwierdza się teza o narastających zagrożeniach oszustwami nigeryjskimi. W wielu środowiskach utarło się przekonanie, że oszustwa finansowe to dla Nigerii trzecia co do wielkości przychodów "gałąź przemysłu." Podobnie jest z korespondencją z tego kraju. Każdy, lub prawie każdy list z Nigerii, a także listy z Południowej Afryki, Zimbabw, Angoli, Sierra Leone czy Wybrzeża Kości Słoniowej, są podejrzewane za wstęp do wyłudzenia pieniędzy<sup>35</sup>.

W 2008 roku w transakcje internetowe Polaków powiększyły się, jak co rocznie o kolejne 50 % i osiągnęły blisko 10 miliardów złotych. Rozpoznano, że w Polsce nasilają się również wszystkie badane przestępstwa określone w cytowanych raportach IFCC oraz IFC3.

W ciągu ostatnich 3 lat znacząco zwiększyła się liczba przestępstw internetowych, na co pośrednio wpływ ma rosnąca liczba osób korzystających z sieci. Obecnie blisko 10 mln Polaków używa Internetu. Wzrasta również liczba transakcji dokonywanych *online*. Na szczególną uwagę zasługuje jednak drastycznie powiększające się terytorium działania oszustów oraz nasilająca się ich aktywność. Nie bez znaczenia jest zatem ostrzeżenie stosowane przez CSO Magazyn Zarządzających Bezpieczeństwem, że w ostatnim okresie nasila się działalność *phisherów*. Ich działalność, związana z wyłudzeniem pieniędzy z kont bankowych, obliczana jest już w milionach złotych.<sup>36</sup> Natomiast KGP podaje, że rocznie samych spraw związanych z oszustwami online zgłasza się ponad półtora tysiąca. Liczba tego typu przestępców wzrasta, nasilają się również straty klientów, a wciąż istnieją duże wątpliwości na temat skuteczności ścigania.

### 8.3. Spam – terror reklamowy?

Związła i pouczająca jest definicja spamu otrzymanywanego w formie najbardziej dokuczliwego bombardowania e-mailami. A. Adamski określa, że jest to „zasypywanie” serwera pocztowego dużą ilością korespondencji elektronicznej w celu wywołania dysfunkcji systemu<sup>37</sup>.

Z przeprowadzonych sondaży wśród niektórych znanych mi posiadaczy poczty internetowej wynika, że nasilenie różnorodnych informacji i reklamy w formie spamu wyraźnie wystąpiło w latach 2005-2006 roku. Jeśli w poprzednich latach dziennie wpływało po kilka, to w 2006 r. kilkanaście, a w 2007 roku nawet od około 20 do 50 spamów dziennie. Można zatem prognozować dalsze nasilenie się tego zjawiska.

Szkodliwość spamu już od dość dawna nie budzi wątpliwości. Skutki finansowe tego zjawiska rozpoznano na przykładzie strat finansowych zarówno w dużych, jak i małych firmach. Dotyczą nie tylko blokowania skrzynek pocztowych i konieczności ich kasowania, ale także z powodu spadku produktywności, kosztów dostępu do Internetu i łączy oraz utrudnionego dostępu do Internetu i adresów firmy. Niejednokrotnie wskazane są dodatkowe inwestycje szczególnie wówczas, gdy wystąpiły trudności w prowadzeniu działalności gospodarczej<sup>38</sup>.

Dyskusja na temat szkodliwości spamu wciąż się rozwija. Systematycznie ujawnia się nowe aspekty tego zagadnienia, którego skutki bliskie są swoistemu terrorowi reklamowemu. Jak dotychczas wymienia się szkodliwość polegającą na tym, że:

1. Powoduje zatykanie się łączy i blokuje miejsce na twardych dyskach.
2. Przetworzenie spamu zabiera czas serwerom, spowalniając ich działanie.

<sup>34</sup> *Internet Crime Report January 1, 2006 – December 31, 2006*, Prepared by the National White Collar Crime Center and the Federal Bureau of Investigation, [www.ic3.gov/media/annualreport/2006\\_ICR](http://www.ic3.gov/media/annualreport/2006_ICR)

<sup>35</sup> J.W. Wójcik, *Oszustwa finansowe*, wyd. cyt., s. 386-453.

<sup>36</sup> <http://cso.cxo.pl/artykuly/51049.html>

<sup>37</sup> A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, TNOiK, Toruń 2001, s. 33.

<sup>38</sup> J.W. Wójcik, *Oszustwa finansowe*, wyd. cyt., s. 349.

3. Powoduje również stratę czasu poszczególnych użytkowników Internetu, bo muszą oni czytać i kasować niepotrzebne wiadomości. Utrudnia czytanie „normalnej” poczty i stwarza ryzyko jej utraty (z powodu blokad antyspamowych albo przepełnienia skrzynki) lub niezauważenia (z powodu „przysypiania” przychodzącym spamem). Zwiększa w ten sposób koszty pracy osób zawodowo korzystających z poczty elektronicznej.
4. Naraża operatorów internetowych i użytkowników na dodatkowe koszty ponoszone na przeciwdziałanie pladze. Spam jest również metodą przerzucenia kosztów promocji na operatorów internetowych i odbiorców korespondencji, a zatem jest formą wyłudzenia.
5. Narusza prywatność i bezpieczeństwo odbiorców, ponieważ często zawiera treści, których nie zyczyliby sobie oglądać, jak obraźliwe, pornograficzne, nieodpowiednie dla dzieci.
6. Spam wiąże się często z różnego rodzaju wirusami i innymi złośliwymi programami.
7. Powoduje utratę zaufania do komunikacji elektronicznej jako takiej.
8. Ze względu na zagrożenie spamem, poczta elektroniczna została pozbawiona niektórych przydatnych funkcji, jak potwierdzeń dostarczenia i przeczytania wiadomości<sup>39</sup>.

Dodać należy, że aczkolwiek spamerzy są ścigani w Polsce jako sprawcy wykroczeń to jednak stają się coraz bardziej niebezpieczni, a ich działania upodabniają się do poważnych przestępstw kryminalnych. Według internautów aż 50-80% otrzymywanych przez użytkowników poczty wiadomości to spam. Wprawdzie najczęściej wysyłany spam dotyczy farmaceutyków - 22,4%, na drugim miejscu są wiadomości dotyczące kwestii finansowych - 10,4%. Natomiast viagra stanowi osobną kategorię spamu. Udział przesyłanych pocztą reklam tego specyfiku, jeszcze nie tak dawno wynosił również blisko 10% (9,62). Z danych policyjnych wielu krajów wynika, że ten środek obecnie jest produkowany, reklamowany i sprzedawany przez zorganizowane międzynarodowe grupy przestępcze.

Spamy z reklamą viagry i innych medykamentów pobiły wszelkie rekordy. Taką tezę potwierdzają wyniki badania odebranych spamów w okresie jednego miesiąca, tj. od 1 do 31 lipca 2007 r. Wspomnianą analizę przeprowadziłem na podstawie nadesłanych spamów na mój prywatny adres e-mailowy. Okazało się, że w analizowanym okresie otrzymałem 427 niechcianych informacji w języku angielskim i tylko jedną w języku polskim (łącznie 428). Całość analizowanego materiału udało się skategoryzować w 15 pozycjach, na które składają się:

- 1) oferty z propozycjami medycznymi (farmakologiczne i techniczne) wyeliminowania problemów seksualnych mężczyzn - 102, tj. 23,8% wszystkich otrzymanych spamów,
- 2) oferty dot. wyłącznie zakupu cialis – 84, tj. 19,6%,
- 3) oferty firm farmaceutycznych i aptek internetowych z propozycjami zakupu różnorodnych medykamentów, a w tym hormony wzrostu i środki dla kulturystów – 72, tj. 16,8%<sup>40</sup>,
- 4) ekskluzywne repliki Roleksa i innych zegarków proponowano w 42 spamach, tj. 9,8%,
- 5) specjalne oferty zakupu takich leków jak: viagra, cialis, valium, ambien i phentermine – 38, tj. 8,8%,
- 6) specjalne oferty zakupu viagry i cialis – 27, tj. 6,3%,
- 7) wyłącznie zakup viagry – 26, tj. 6,1 %,
- 8) reklama internetowych kasyn gry – 14, tj. 3,3%,
- 9) oferty pracy w międzynarodowej instytucji finansowej – 9, tj. 2,1%,
- 10) reklama specyfików na odchudzanie – 5, tj. 1,2%,
- 11) udziału w aukcjach eBay – 2, tj. 0,5%,
- 12) reklamy leków geriatrycznych - 2, tj. 0,5%,
- 13) propozycje zakupu akcji śmieciowych - 2, tj. 0,5%,
- 14) propozycje wynikające z serwisu randkowego – 2, tj. 0,5%,
- 15) propozycja pracy dla obywatela kraju członkowskiego UE -1, tj. 0,2%.

Podsumowując analizę tematyki nadesłanych niechcianych reklam i informacji należy zwrócić uwagę przynajmniej na kilka różnorodnych aspektów, a w szczególności:

- tematyka i czasookres nadsyłanych spamów mogą być zmienne. Zapewne są one uzależnione od otrzymanych zleceń przez spamerów i ich zdolności rozsyłania tego typu informacji;
- z podsumowania tematyki nadesłanych 428 spamów, przy założeniu, że na inne adresy wysyłano podobne lub takie same spamy, można wnioskować, iż jesteśmy wprost zalewani informacjami natury medycznej, a przede wszystkim farmakologicznej. Pomijając nawet takie reklamy jak

<sup>39</sup> <http://pl.wikipedia.org/wiki/Spam>

<sup>40</sup> W ciągu ostatnich pięciu lat ujawniono 170 leków sprzedawanych z pominięciem obowiązkowej procedury badań i rejestracji.

- na szczególną uwagę zasługują spamy o charakterze finansowym, których było wprawdzie tylko 6,9%, lecz ich rodzaj może budzić istotne podejrzenia, że mogą mieć związek z oszustwami finansowymi, a zatem mogą spowodować o wiele groźniejsze skutki niż inne reklamy.

Przedstawione wyniki badania potwierdzają wcześniejsze informacje, że systematycznie rozprzestrzeniają się spamy: randkowe z propozycjami kontaktów seksualnych, quasi-medyczne z propozycjami usprawnienia męskich narządów płciowych oraz kolejne, podobno bardziej atrakcyjne i skuteczne środki na sprawność seksualną mężczyzn i kobiet, a także skuteczne metody odchudzania. Jednakże najwięcej spamów dotyczy reklamowania różnych towarów i produktów. Wiele z nich to spamy o charakterze finansowym.

#### 8.4. Falszywe witryny bankowe

Podczas kryzysu finansowego, który zawładnął światową gospodarką, w siłę rosła międzynarodowe gangi okradające w Internecie konta bankowe. Eksperci mówią już wprost o gigantycznej lawinie wirusów i fałszywych witryn internetowych, za pomocą których hakerzy czyszcza konta klientów banków. Wyspecjalizowani przestępcy wysyłają też fałszywe listy elektroniczne oferujące klientom kredyty hipoteczne, pożyczki i inne oferty z upadających banków. Tego typu przestępcy czerpią korzyści z mizernej sytuacji gospodarczej, atakując niczego niepodejrzewające ofiary<sup>41</sup>. Raport międzynarodowego koncernu Panda Security, który tworzy oprogramowanie antywirusowe, nie pozostawia złudzeń: niestabilność na giełdzie ożywiła cyberprzestępców. Przykładowo, tylko w okresie czterech dni, kiedy to giełdy odnotowały pięcioprocentowe spadki, liczba niebezpiecznych wirusów wzrosła o połowę. Były to głównie fałszywe witryny internetowe, ludożę podobne do serwisów banków. Logując się na taką stronę, nieuważny klient podaje przestępcom jak na tacy swój PIN i dane osobowe. Hakerzy, którzy według ekspertów miesięcznie na nielegalnym procederze zarabiają 10 mln euro, poszli jednak o krok dalej. Dotychczas podrabiali strony instytucji, teraz bezpośrednio atakują oryginalne witryny banków.

Panuje powszechne i uzasadnione przekonanie, że polskie banki ukrywają hakerskie ataki, ale medialne informacje i policyjne akcje nie pozostawiają złudzeń. To już drugi rok z rzędu napływają informacje o systematycznych akcjach policji i zatrzymaniach Rumunów, Bułgarów, Ukraińców, a także Polaków, którzy okradali przez Internet konta bankowe, sklepy internetowe i inne firmy, a także systematycznie skanują karty bankomatowe i realizują wypłaty za granicą Polski. Niezwykle istotne są wyniki badań przeprowadzonych przez Panda Security wśród firm, które dokonują przelewów pieniężnych. Okazało się, że znaczny odsetek firm korzystających z transferów finansowych *online* nie posiada aktualnego oprogramowania antywirusowego. Brak odpowiednich zabezpieczeń umożliwia cyberprzestępcom zdobywanie poufnych danych bankowych i opróżnianie firmowych kont.

Wspomniane badanie, przeprowadzone przez Panda Security, światowego lidera w dziedzinie zabezpieczeń IT, dotyczyło grupy ponad 300 firm korzystających z usługi międzynarodowych transferów finansowych. Przeanalizowano ponad 1500 komputerów. Wyniki były alarmujące bowiem 30% z nich dysponowało przestarzałymi systemami zabezpieczeń, których bazy sygnatur nie uwzględniały najnowszych zagrożeń, a 60% już było zainfekowanych<sup>42</sup>.

#### 8.5. Cyberbank? - tak: Dominion of Melchizedek i wiele innych

Spośród wszystkich oszustw pojawiających się w Internecie nic jeszcze nie było tak wielkim oszustwem jak fikcyjne państwo, jego banki, uniwersytet, placówki dyplomatyczne i inne instytucje.

Pomysłowość przestępców, a szczególnie oszustów finansowych nie zna granic. Wraz z powstaniem i rozwojem Internetu, kolejne, jak się wydawało niektórym przestępcom, wręcz doskonale pole działania, zaistniało w cyberprzestrzeni. To ogromne środowisko i technologie stały się przedmiotem penetracji i

<sup>41</sup> Jednakże istotnym niedopatrzeniem byłoby zachwycać się kilkuletnim już statystycznym spadkiem przestępczości stwierdzonej. Por.: [www.kgp/statystyka.pl](http://www.kgp/statystyka.pl) oraz E. Siedlecka, *Lawinowy spadek przestępczości*, Gazeta Wyborcza z 3 marca 2009 r. Jednakże kryzys ekonomiczny uruchamia różne kręgi i grupy przestępcze także te, które dokonują przestępstw pospolicznych. Szerzej: J. Blikowska, M. Kozubal, *Kryzys: przestępcy ruszyli na złodziejskie łowy*, Rzeczpospolita – Życie Warszawy z 12 marca 2009 r. Autorzy starają się wykazać, że zanotowany ostatnio wzrost przestępczości w Stolicy ma istotne związki z narastającym bezrobociem.

<sup>42</sup> M. Sobianek, *Panda Security ujawnia poważne luki w zabezpieczeniach firm wykonujących przelewy pieniężne* <http://prportal.pl/2009/01/...#more-9382>

działań zorganizowanych oszustów finansowych. Wprawdzie jeszcze nie wszystkie formy działania oszustów w Internecie zostały dogłębnie rozpoznane, to jednak nie ma wątpliwości, że do aktualnych technik należy dodać nie tylko fikcyjne sklepy, lecz nawet fikcyjne państwa, fikcyjne banki, firmy ubezpieczeniowe, uczelnie, ambasady, konsorcja handlowe itp.

Fikcyjne państwa i księstwa także znane są z wydawania "dokumentów" bankowych. Przykładowo, już w 1996 roku Generalny Inspektor Nadzoru Bankowego NBP i Komenda Główna Policji, a także Interpol ostrzegły wszystkie polskie banki o pojawieniu się dokumentów wystawionych przez instytucje finansowe zarejestrowane w fikcyjnym państwie Dominion of Melchizedek. Bank ten istnieje współcześnie i prowadzi ożywioną działalność. Znany jest przede wszystkim z cyberbankingu i wielu tego typu oszustw.

Literatura przedmiotu zbyt mało miejsca poświęca oszustwom w cyberprzestrzeni. Wpływa to na zbyt małe oddziaływanie profilaktyczne, a zatem umożliwia sukcesy przestępcom. Dziennikarz śledczy Bertil Lintner trafnie określił, iż spośród wszystkich oszustw pojawiających się w Internecie nic jeszcze nie było tak wielkim oszustwem jak fikcyjne państwo Dominion of Melchizedek. Taką właśnie tezę uzasadnił w swoim opracowaniu<sup>43</sup>. Wciąż jednak Dominion of Melchizedek reklamuje swoje ambasady, szkoły wyższe, paszporty z możliwością ubiegania się o obywatelstwo, a także transakcje bankowe we własnych bankach<sup>44</sup>. Obszerna literatura dotycząca zarówno przeszłości kryminalnej szefów banku, jak i ich ofiar wykazuje, że bank ten działa skutecznie.

## 9. MODUS OPERANDI SPRAWCÓW

Znaczenie różnorodnych zarówno rozpoznanych, jak i nadchodzących zagrożeń w cyberprzestrzeni nie jest jeszcze należycie doceniane. Warto zatem zwrócić uwagę na słowa dr Malcolma Davisa z King's College w Londynie - eksperta ds przyszłej wojny. Bardzo trafnie określił on, że „do trzech klasycznych teatrów działań wojennych: morza, ziemi i powietrza, dojdzie niedługo czwarty: cyberprzestrzeń.” Jego zdaniem hakerzy, jak komandosi, mają największą szansę działania poza linią wroga. Żyjemy w czasach, gdy niemal wszystko jest kontrolowane przez komputery. Zatem dobrze wymierzony cyberatak będzie mógł sparaliżować nieprzyjacielską armię.<sup>45</sup>

Mając na względzie aspekty codziennych przedsięwzięć we współczesnych realiach nie możemy zapominać o rozpoznanych dotychczas atakach na serwery rządowe, wojskowe, bankowe, placówek naukowych, a także komputery osobiste. Dochodzi wówczas najczęściej do ich blokady, zawirusowania, kradzieży cennych informacji o charakterze strategicznym, ekonomicznym, marketingowym, a ostatnio także o charakterze politycznym. Wiele z nich jest istotnych z punktu widzenia zbierania informacji w ramach szpiegostwa gospodarczego czy nieuczciwej konkurencji, a jeszcze inne mogą mieć charakter terroru cybernetycznego. Inne, lecz również przynoszące szkody finansowe to oszustwa w trakcie aukcji internetowych czy w ramach zakupu ze sklepów internetowych. Charakter wspomnianych zagrożeń wykazuje wyraźną tendencję wzrastającą. Jest to wystarczający powód nie tylko do poszukiwania i stosowania zapobiegawczych metod w ramach osiągnięć informatyki, lecz także w ramach kryminalistyki i kryminologii.

Oprócz powszechnie znanych już słynnych ataków hakerów na różne obiekty, a także aktów *phishingu* na placówki bankowe i ich skutki, zawirusowania komputerów osobistych, niezbędne jest podkreślenie wagi zagadnienia przynajmniej na poniższych przykładach ataków o charakterze międzynarodowym, które miały miejsce w lecie 2007 roku. Według agencji zachodnich sprawcami tych ataków byli wyspecjalizowani hakerzy z sił zbrojnych lub innych instytucji rządowych, a mianowicie :

- naruszenie suwerenności Estonii przez rosyjskich hakerów rządowych w związku z usunięciem z centrum Tallina pomnika żołnierzy radzieckich poprzez internetową blokadę wielu instytucji państwowych, a szczególnie: banków, gazet i partii politycznych. Wynikające z tego straty z powodu zakłócenia działalności tych instytucji wynoszą miliony euro;
- hakerzy chińskiej armii, po kilku miesiącach przygotowań w zakresie rozpoznawania systemów zabezpieczeń, dokonali zmasowanego i najpoważniejszego w historii USA ataku na komputery. Tylko dzięki szybkiej reakcji Pentagon nie utracił ściśle tajnych danych. Jednakże na skutek ataku Departament Obrony na tydzień zawiesił działania w swojej sieci, lecz na razie trudno jest ustalić rzeczywiste straty;

---

<sup>43</sup> B. Lintner, *Cyberfraud: The fictitious "Dominion of Melchizedek"*, The Nation z 30 maja 1999 r.

oraz [http://www.asiapacificms.com/articles/cyberfraud\\_melchizedek/](http://www.asiapacificms.com/articles/cyberfraud_melchizedek/), a także J.W. Wójcik, *Oszustwa finansowe*, wyd. cyt, s. 364-372.

<sup>44</sup> <http://www.melchizedek.com>.

<sup>45</sup> Cytuję za: P. Zychowicz, *Wirtualna trzecia wojna światowa*, Rzeczpospolita z 5 września 2007 r.

- próba blokady i kradzieży informacji z niemieckich instytucji państwowych przez chińskich hakerów służących w armii. Celem ataku były serwery urzędu kanclerskiego, resortu spraw zagranicznych, instytucji o charakterze gospodarczym i naukowym dla zdobycia tajnych informacji wyłącznie o charakterze gospodarczym, a w tym nowe technologie i dane marketingowe.

Nie są to odosobnione ataki hakerów na systemy informatyczne. Przykładowo, The Guardian z 6 września 2007 r. podał informację o próbie zatuszowania informacji przez rząd Wielkiej Brytanii o ataku chińskich hakerów, w wyniku których unieruchomiono systemy parlamentu, resortu spraw zagranicznych i kilku innych ministerstw. Ustalono, że był to atak grupy hakerów z Pekinu, której działalność prawdopodobnie popierana jest przez rząd i określana jest jako „patriotyczne hakowanie”. Swoimi działaniami podejmują oni ataki na najważniejsze sieci swoich wrogów.

O narastającej powadze zagrożeń może świadczyć wiele przykładów, a w tym fakt ujawnienia w listopadzie 2007 r. 18 letniego hakera o pseudonimie Akill z Nowej Zelandii, który kierował międzynarodowym gangiem przestępców. Grupa włamała się do ponad miliona komputerów i ukradła około 25 mln USD z internetowych rachunków bankowych. Sprawcy instalowali za pośrednictwem Internetu specjalne programy w komputerach osobistych na całym świecie i rozpoznawali numery rachunków bankowych, hasła dostępu oraz numery kart kredytowych.

W USA 17-letni uczeń Cole A. Bartiromo mieszkający z rodzicami w Kalifornii założył witrynę internetową, która nosiła nazwę „Inwestuj lepiej ...”. Był to system zakładów sportowych, który pozwolił mu wyłudzić od inwestorów ponad milion dolarów od przeszło 1000 osób. Młody oszust sprzedawał „gwarantowane” i „wolne od ryzyka” oferty inwestycyjne, polegające na obstawianiu imprez sportowych. Zapewniał on zyski od 125 do 2500 procent. Przedstawiciel Komisji papierów wartościowych USA - SEC, oświadczył, że przypadek ten potwierdza tezę, iż nawet uczeń jest zdolny do oszustw finansowych dokonywanych przy użyciu Internetu.

W Polsce również nie brakuje działań hakerów. Zdaniem eMetro.pl to właśnie oni 21 października 2007 r. na pięćdziesiąt minut przed zakończeniem wyborów i oficjalnym ogłoszeniem wyników znali ich wyniki. Podobno zdołali odczytać zrzut danych do jednej ze stacji telewizyjnych.

Uzasadniona jest teza, że więcej uwagi należy poświęcać chociażby wybranym zagrożeniom związanym z ochroną danych osobowych i bezpieczeństwem obrotu gospodarczego, a także w wielu dziedzinach życia społecznego posługujących się powszechnie komunikacją internetową. Jedną z form wspomnianych zagrożeń powszechnie określa się jako spamy, czyli niechciane informacje nadsyłane pocztą elektroniczną. Wśród najpoważniejszych rozpoznanych zagrożeń jest przykładowo blokada komputerów będących w rękach spamerów, która może być niezwykle istotnym narzędziem w rękach terrorystów.

## **10. SPECYFIKA PRZESTĘPSTW KOMPUTEROWYCH A DOWODOWE ŚLADY TRANSAKCYJNE**

Niezmierzalnie interesująca jest problematyka związana ze specyfiką przestępstw komputerowych, kryminalistycznymi śladami transakcyjnymi, a szczególnie śladami elektronicznymi.

Atrakcyjność Internetu dla przestępców polega również na tym, że wielu osobom wydaje się wciąż jeszcze, że mogą pozostać anonimowe, czyli nierozpoznawalne. Innym udaje się wciąż jeszcze otwierać anonimowe konta i kontaktować się za pomocą *nicka*, czyli pseudonimu, czy kradzionej tożsamości. Wykorzystują zatem Internet poprzez wszystkie sposoby i techniki, które daje im ten wynalazek. A także wynajdują własne sposoby i techniki komunikowania się. Stosują własne szyfry i klucze nie tylko w celu wymiany informacji, lecz także dla składania zamówień na towary czy usługi, których nabywanie i zbywanie jest prawnie zabronione. Ponadto, realizują należności za wspomniane zabronione usługi czy transakcje.

Do badania wielu czynów kryminalnych mają zastosowanie klasyczne środki i metody kryminalistyczne, w wielu innych są one przydatne tylko częściowo. Jednakże poszukiwane są wciąż nowe metody i techniki dowodowe. Warto przy tym wskazać, że rozwój nauki sprzyja takiemu stanowisku. Ostatnim przykładem w tej mierze może być chociażby rozwijająca się aktualnie identyfikacja biometryczna czy kryminalistyka informatyczna (a może poprawną nazwą okaże się informatyka śledcza). Ta ostatnia dziedzina, z punktu widzenia kryminalistyki, powinna mieć na uwadze ujawnianie i zabezpieczanie śladów elektronicznych.

Mając na względzie *modus operandi* sprawców przestępstw gospodarczych, bankowych, a szczególnie oszustw finansowych powiemy więc, przeciwstawiając je przestępstwu kryminalnemu, że te pierwsze charakteryzują się „śladami transakcyjnymi”, które z pozoru istnieją pomiędzy instytucjami finansowymi, przedsiębiorstwami i osobami fizycznymi. Przykładowo, transakcje wynikające z *modus operandi* sprawców prania pieniędzy mają najczęściej charakter legalny, lecz niezmiernie trudno jest je rozpoznać. Zatem ślady dokumentacyjne transakcji związanych z praniem pieniędzy, zarówno w instytucjach

finansowych, jak i niefinansowych, mają charakter jawny i jak się wydaje zgodny z prawem i obowiązującymi procedurami. Jednakże źródła pochodzenia pieniędzy mają charakter utajony, gdyż związane są z przestępstwami bazowymi, tj. pierwotnymi i wtórnymi, czyli poprzedzającymi i następczymi pranie pieniędzy. Ich ujawnienie grozi dekonspiracją grupy przestępczej. Z tych względów niezwykle ważne znaczenie ma opinia biegłego, którą zawsze analizuje się w relacji do innych środków dowodowych i ustalonych faktów istotnych dla postępowania.<sup>46</sup>

Poszukiwanie dowodowego śladu transakcyjnego w postępowaniach o oszustwa finansowe to złożone zagadnienie. Niejednokrotnie wśród tysięcy kontraktów, faktur, dowodów wpłaty czy wypłaty, poleceń przelewu, czy innych dokumentów, należy wyłonić ten jeden, który ma znaczenie dowodowe, czyli od określonego nadawcy czy pośrednika, określona kwota, za jaki towar czy rodzaj usługi, do określonego rzeczywistego beneficjenta.

Należy również brać pod uwagę, że od dawna wiadomo, iż we wszelkiego rodzaju transakcjach podejrzanych istotną rolę odgrywa faktura i przesyłane pieniądze<sup>47</sup>. Towar czy usługa nie są ważne, a mają często charakter fikcyjny, czyli prosty jest już wniosek, że faktura może być fałszywa. Można to określić poprawnie, że nastąpiło fakturowanie bez współudziału dostawcy. Fakturowanie elektroniczne jest dużym ułatwieniem dla fałszerzy i oszustów.

Wydaje się uzasadniona teza, że jednym z podstawowych warunków skutecznego przeciwdziałania tym zjawiskom są odpowiednio przygotowane kadry policyjne, skarbowe i innych służb państwowych oraz organów wymiaru sprawiedliwości. Od dawna wiadomo, że mamy stały dylemat: czy Polska posiada takie wyspecjalizowane kadry, czy dopiero (wciąż jeszcze, czyli po wielu reorganizacjach) przygotowujemy się do realizacji takiego zadania. Kolejnym krokiem ma być utworzenie policji podatkowej zwalczającej szarą strefę gospodarczą oraz utworzenie specjalnych wydziałów ds. ujawniania majątków przestępców.

Oszustwa finansowe są tą kategorią przestępstw, która ze względu na ich różnorodność form, zmienność i złożoność *modus operandi* sprawców, czy wreszcie wielkość strat, jakie powodują, są szczególnie dotkliwe dla gospodarki, państwa i obywateli. Z drugiej strony zauważalne są trudności wykrywcze i dowodowe, z którymi muszą zmierzyć się organy i instytucje powołane do zwalczania tego rodzaju patologii. Niedostateczna znajomość mechanizmów działania sprawców, uchybienia proceduralne, brak biegłych dysponujących odpowiednim przygotowaniem merytorycznym, w ostatecznym rozrachunku skutkuje, nie tylko przewlekłością postępowań karnych, ale często ich niedostatecznym poziomem dowodowym. Świadczy o tym dobitnie znikoma liczba spraw prawomocnie osądzonych przy wielkiej liczbie afer gospodarczych już wykrytych, nie mówiąc o tych, które pozostają poza wiedzą organów ścigania.

Wydaje się uzasadniona teza, że jednym z podstawowych warunków skutecznego przeciwdziałania tym zjawiskom są odpowiednio przygotowane kadry policyjne, skarbowe i innych służb państwowych oraz organów wymiaru sprawiedliwości. Czy Polska posiada takie wyspecjalizowane kadry, czy dopiero (wciąż jeszcze, czyli po wielu reorganizacjach) przygotowujemy się do realizacji takiego zadania. Mamy jednak gotowe i wielce profesjonalne wzorce. Czy warto skorzystać przykładowo z włoskiej policji skarbowej podległej Ministerstwu Gospodarki i Finansów, a której nazwa brzmi *Guardia di Finanza*? Jej kompetencje odpowiadają polskim służbom celnym, izbie skarbowej i wydziałom ds. przestępstw gospodarczych w jednostkach policji. Na razie planowane jest utworzenie policji podatkowej zwalczającej szarą strefę gospodarczą.

Autorzy, a także recenzenci współczesnych podręczników kryminalistyki wyraźnie podkreślają, że należy mieć świadomość, iż tradycyjna kryminalistyka, koncentrująca swoją uwagę na takich działach, jak np.: daktyloskopia, traseologia, mechanoskopia, osmologia, badania pismoznawcze, a nawet chemia czy też genetyka adoptowana do potrzeb kryminalistycznych, w niewielkim tylko stopniu może mieć zastosowanie w wykrywaniu i dowodzeniu przestępstw gospodarczych i zorganizowanych oszustw finansowych, w których nie ślad biologiczny, a ślad transakcyjny w postaci dokumentów odgrywa najważniejszą rolę wykrywcą i dowodową.

Omawiana problematyka, obok wielu innych, jak np.: oszustwa bankowe, giełdowe i w ramach akredytywy, analiza oszustw kredytowych, kredytów w systemie argentyńskim, nowych form oszustw inwestycyjnych na tle wyrafinowanego wykorzystywania aktualnych potrzeb społecznych, wielu nowych form zagrożeń w cyberprzestrzeni, niezwykle podstępnych form zagrożeń związanych z inwestowaniem w łańcuszki, piramidy i parabanki, a także niezwykle wyrafinowanych i wcale nie egzotycznych nigeryjskich oszustw zaliczkowych – oczekuje na kolejne postępy nauki sprzyjające sprawnemu rozpoznawaniu i

<sup>46</sup> Szerzej: J. W. Wójcik, *Przeciwdziałanie praniu pieniędzy*, wyd. cyt., s. 378 i n.

<sup>47</sup> J.T. Wells, *Nadużycia w firmach. Vademecum*, LexisNexis, Warszawa 2006, s. 189-202.

zabezpieczeniu zarówno transakcyjnych, a w tym dowodów elektronicznych, niezwykle przydatnych dla dowodowych celów śledczych.

Przestępstwa w obrocie gospodarczym, a szczególnie wyrafinowane oszustwa finansowe stwarzają szczególne trudności rozpoznawcze i wykrywczo-dowodowe, a rozmiary „ciemnej” i „złotej” liczby przestępstw z tym związanych są wciąż bardzo znaczące, niełatwe do analiz i badań, prezentowane najczęściej w formie szacunków i muszą wywoływać zrozumiąły niepokój nie tylko znawców przedmiotu, lecz również wielu grup społecznych. Nie tylko pracownicy organów ścigania, także biegli sądowi wciąż mają problemy z ujawnianiem dowodów z różnorodnych dokumentów, a przede wszystkim finansowych, czyli ze znalezieniem dla celów wykrywczych i dowodowych „śladu transakcyjnego”<sup>48</sup>.

Nadszedł już czas by zastanowić się nad rozważaniami dotyczącymi definicji takiego śladu, jego opisu i klasyfikacji przydatnej dla ekspertów z zakresu kryminalistyki innych biegłych, jak np. głównych księgowych, biegłych rewidentów czy specjalistów z zakresu audytu śledczego, którzy wydają opinie dla postępowania przygotowawczych czy przed sądem.

Uzasadniony jest zatem wniosek, że omawiana kwestia powinna stać się przedmiotem rozważań, a być może polemiki zainteresowanych specjalistów, w ramach której może być dokonana ocena z punktu widzenia sygnalizowanych wyżej niedostatków tradycyjnej kryminalistyki w rozpoznawaniu i zwalczaniu przestępstw ekonomicznych. Warto również zastanowić się czy kryminalistyczna koncepcja *śladu transakcyjnego*, a niezbędnego aktualnie już we wszystkich prawie dziedzinach życia społecznego *śladu elektronicznego*, jest konstruktywną propozycją metod badań kryminalistycznych w złożonej problematyce przeciwdziałania przestępczości ekonomicznej.

Dotychczasowa praktyka śledcza oraz orzecznictwo sądowe wskazują na ograniczone możliwości ścigania sprawców omawianych przestępstw. Przyczyny takiego stanu rzeczy są bardzo zróżnicowane, a wynikają przede wszystkim ze specyfiki przestępstw komputerowych. Ta specyfika stwarza poważne trudności wykrywcze i dowodowe w sensie tradycyjnym.

Specyficzne *modus operandi* sprawców przestępstw komputerowych polega przede wszystkim na niekonwencjonalnym sposobie działania, a w związku z tym konieczne są nowe, również niekonwencjonalne, tj. inne niż w klasycznej kryminalistyce - metody wykrywania. Specyfika przestępstw komputerowych polega przede wszystkim na:

- ponadnarodowym charakterze czyli transgranicznym działaniu sprawców,
- możliwości zdalnego działania sprawców,
- istniejące wciąż jeszcze możliwości łatwego kamuflowania swojego czynu.

Ponadto, jeżeli sprawca przestępstwa nie musi być obecny na miejscu przestępstwa, a zatem nie zostawia śladów (daktyloskopijnych, mechanoskopijnych, traseologicznych itp.), a nawet posiada możliwość usuwania śladów przestępnego działania w ramach procedury samolikwidacji dokonanego zapisu to nie podlega kwestii, że w tym przedmiocie stwarza się dodatkowe trudności wykrywcze i dowodowe. Są to trudności zarówno natury ogólnej (przykładowo, ciągły brak jeszcze świadomości występujących zagrożeń, a zatem o konieczności stosowania i aktualizowania zabezpieczeń) oraz natury szczegółowej poprzez:

- różnorodność systemów operacyjnych oraz oprogramowania użytkowego,
- trudności związane z umiejętnym zabezpieczeniem elektronicznych materiałów dowodowych,
- brak odpowiednich (specjalistycznych) procedur w tym zakresie,
- trudności z uzyskaniem specjalistycznych opinii kryminalistycznych,
- odczuwalnym wciąż brakiem profesjonalistów w organach ścigania i wymiaru sprawiedliwości.

## **11. DWADZIEŚCIA JEDEN ZŁOTYCH RECEPT CZYLI JAK SKUTECZNIE CHRONIĆ SYSTEMY TELEINFORMATYCZNE**

Obowiązujący stan prawny nie jest wystarczającym czynnikiem do skutecznych działań zapobiegawczych tym bardziej, że nie ma już dziedziny życia społecznego, która nie korzysta z sieci teleinformatycznych.

Właściwe rozważania prawnozapobiegawcze i profilaktyczne należy prowadzić przede wszystkim na podstawie:

- konwencji Rady Europy o cyberprzestępczości z 23 listopada 2001 roku zawartej w Budapeszcie, w której najważniejsze postanowienia dotyczą<sup>49</sup>:

<sup>48</sup> J. W. Wójcik, *Weryfikacja podejrzenia popełnienia przestępstwa prania pieniędzy*, Prokuratura i Prawo 2005, nr 9.

<sup>49</sup> A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, TNOiK, Toruń 2001.

- a) harmonizacji narodowych systemów prawnych w sprawie zdefiniowania przestępstw,
- b) wypracowania standardów prowadzenia śledztw oraz procedur sądowych dostosowanych do zasad działania globalnej sieci,
- c) stworzenia szybkiego i skutecznego systemu współpracy międzynarodowej<sup>50</sup>;
- cytowanego wcześniej Komunikatu Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów KOM(2007) 267 wydanego w Brukseli dnia 22 maja 2007 r. w sprawie ogólnej strategii zwalczania cyberprzestępczości;
- ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym<sup>51</sup>. Ustawa określa infrastruktury krytyczne jak systemy zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych;
- właściwych artykułów kodeksu karnego.

Natomiast inspiracją do kryminologicznego i kryminalistycznego spojrzenia na ochronę systemów teleinformatycznych jest wiele zagadnień, z których podstawowe to:

- rozmiary zagrożeń przestępczością w cyberprzestrzeni oraz jej związki z instytucjami finansowo – bankowymi i biznesem są wciąż niedoceniane;
- rzeczywiste rozmiary przestępczości komputerowej są trudne do określenia, gdyż sprawcy działają w stosunkowo długim czasie i powodują zarówno poważne straty materialne, jak i niematerialne;
- charakterystyczny brak kompleksowej i profesjonalnej analizy i oceny istniejących zagrożeń, a zatem kryminologicznej diagnozy i prognozy;
- wspomniane przestępstwa ujawniane są przypadkowo, najczęściej z powodu błędów popełnianych przez sprawców;
- organy ścigania odgrywają minimalną rolę w ujawnianiu tych przestępstw i przede wszystkim z tego względu przewencyjna rola śledztwa i wyroku sądowego jest niezwykle ograniczona;
- największa rola w zapobieganiu wspomnianej przestępczości przypada samym użytkownikom systemów informatycznych, bowiem sprawcy najczęściej wykorzystują błędy w administrowaniu i ochronie systemów;
- jednym z podstawowych mankamentów jest brak dostatecznej świadomości na temat realnych potrzeb i możliwości stosowania profesjonalnych zabezpieczeń;
- wciąż niedostateczną wagę przykładają się do osiągnięć specjalistycznych firm w zakresie ochrony oraz stosowania nowoczesnych zabezpieczeń;
- niedostateczna lub bardzo ogólnikowa jest świadomość społeczna na temat występujących zagrożeń, na które narażone są wszystkie instytucje i przedsiębiorstwa z powodu atrakcyjności ich produkcji, prowadzonej działalności, czy innych form inspirujących zainteresowania konkurencji, wywiadu gospodarczego itp.;
- szefowie wielkich organizacji, jak i małych firm wciąż zbyt małą rolę przykładają nie tylko do właściwej ochrony informacji i ochrony systemów teleinformatycznych, lecz także do kompleksowego systemu ochrony i zabezpieczeń, czyli do polityki bezpieczeństwa organizacji;
- nie należy zapominać, że mamy do czynienia z profesjonalnym przeciwnikiem. To również intelektualista, który jest wykształcony i niejednokrotnie znane mu są zarówno procedury bankowe, jak i innych instytucji finansowych;
- wciąż zbyt małą rolę przykładają się do edukacji, a szczególnie profesjonalnych szkoleń mających na celu wyjaśnianie rodzajów i rozmiarów zagrożeń, dążenie do opracowywania diagnozy i prognozy, a także *modus operandi* sprawców, stosowania obowiązującego prawa oraz wdrażania nowoczesnych zasad zapobiegania.

Poszukiwanie skutecznych recept w zakresie zapobiegania powinno uwzględniać najbardziej podstawowe działania, które nie zawsze są respektowane. Już na tym etapie uwidacznia się brak profesjonalizmu. Zatem z kryminologicznego i kryminalistycznego punktu widzenia:

<sup>50</sup> Wcześniejsze dokumenty Rady Europy w tej kwestii to: Zalecenie nr R (89) 9 Computer-Related Crime, o przestępczości komputerowej i końcowe sprawozdanie Komitetu Problemów Przestępczości Rady Europy, Strasbourg 1989 oraz Zalecenie nr R (95) 13 Problems of Criminal Procedural Law Connected with Information Technology przyjęte przez Komitet Ministrów Rady Europy 11 września 1995 r.

<sup>51</sup> Dz. U. Nr 89, poz. 590.

1. Rozpoznaj i oceń zagrożenia.
2. Opracuj strategię działania, czyli politykę bezpieczeństwa.
3. Dostosuj konstrukcję bezpieczeństwa systemów do struktury organizacji.
4. Powołaj administratora ds. zabezpieczenia systemów teleinformatycznych.
5. Nie lekceważ podstawowych elementów bezpieczeństwa.
6. Pamiętaj o zagrożeniach ze strony personelu.
7. Stosuj właściwe hasła.
8. Stosuj inne nowoczesne środki mające wpływ na zapobieganie włamaniom do systemów.
9. Zapewnij bezpieczne metody przesyłania chronionych informacji.
10. Stosuj profilaktykę antywirusową.
11. Pamiętaj o stałych zagrożeniach płynących z Internetu.
12. Nie daj się zaskoczyć, czyli opracuj plan zarządzania sytuacją kryzysową.
13. Kieruj się ekonomiką zabezpieczeń lecz uwzględniaj nowoczesne rozwiązania.
14. Przestrzegaj zaleceń audytorów i konsultantów.
15. Niezłomnie inspiruj zarząd do realizacji siedmiu naczelnych zadań w zakresie zarządzania bezpieczeństwem.
16. Pamiętaj o systematycznej edukacji nt. bezpieczeństwa systemów teleinformatycznych.
17. Ubezpiecz się od ryzyka związanego z przestępstwami komputerowymi oraz zniszczeniem sprzętu elektronicznego.
18. Zawsze pamiętaj o znanych słabych stronach systemu zabezpieczeń i obsługi.
19. Unikaj podstawowych błędów w zarządzaniu bezpieczeństwem systemów teleinformatycznych.
20. Jeśli stwierdziłeś naruszenie zabezpieczeń systemów obowiązkowo zawiadom prokuraturę lub policję.
21. Poszukaj kolejnych mankamentów w systemie bezpieczeństwa, gdyż technika nie zna granic, a ludzie popełniają błędy<sup>52</sup>.

Ponadto, należy mieć na uwadze fakt, że bezpieczny system teleinformatyczny - nie istnieje, a jeśli jesteś zadowolony ze stanu zabezpieczeń - miej się na baczności!

---

<sup>52</sup> Szerzej: J.W. Wójcik, *Przestępstwa komputerowe, cz. II – Techniki zapobiegania*, CIM, Warszawa 1999, s. 145-172.