

**Prof. dr inż. Tadeusz JEMIOŁO**

## **WYZWANIA I ZAGROŻENIA DLA GLOBALNEGO BEZPIECZEŃSTWA INFORMACYJNEGO W PIERWSZYCH DEKADACH XXI WIEKU**

### **1.1. Ogólne uwarunkowania globalnego bezpieczeństwa informacyjnego**

Ataki terrorystyczne na *World Trade Center* w Nowym Jorku i Pentagon w Waszyngtonie z 11 września 2001 roku spowodowały gwałtowną zmianę sytuacji bezpieczeństwa w skali globalnej. Bezpośrednio po zamachach większość państw NATO, w tym Polska zostało zmuszonych do wprowadzenia w życie elementów narodowych systemów gotowości obronnej. Tragedia ta stała się też źródłem głębokiej refleksji społeczności międzynarodowej obejmującej zarówno przyczyny jak i konsekwencje tego wydarzenia, któremu mając na uwadze stosunki międzynarodowe, można nadać charakter niezaprzeczalnie przełomowy.

Zamach na symbole amerykańskiej potęgi w sposób jednoznaczny udowodnił, że "...dzisiejsze zagrożenia posiadają inną naturę i skalę niż dotychczas, a współczesna odpowiedź na te zagrożenia jest nieadekwatna. Broń projektowana w celu przeciwstawienia się zagrożeniom, w końcu ostatniego tysiąclecia, nie będzie w stanie sprostać im w pierwszych dekadach XXI wieku. Nowe często o asymetrycznym charakterze zagrożenia dla bezpieczeństwa globalnego wymagają nowego myślenia<sup>1</sup>".

Konieczność nowego podejścia jest nagląca, gdyż terroryzm jest tylko, jednym z wielu nietradycyjnych wyzwań dla bezpieczeństwa. Stanowią je także: konflikty etniczne i religijne, przemyt narkotyków, masowe migracje, regionalna niestabilność, pranie brudnych pieniędzy, działania różnych grup

---

<sup>1</sup> Por. R.Hall, C.Fox: Ponownie przemyśleć bezpieczeństwo, "Przegląd NATO", Zima 2001/2002, s.8.

ekstremistycznych oraz kradzież informacji. Najczęściej bardzo trudno jest zidentyfikować przywódcę lub region, gdzie można by skoncentrować zainteresowanie w celu przeciwstawienia się im. Co więcej skala tych zagrożeń jest tak duża, że stanowi zagrożenie dla wielu krajów. Zagrożenia te nie znają bowiem granic państwowych i kontynentalnych. Istnieje też zasadnicza trudność we właściwej identyfikacji zjawisk (organizacji, przywódców) w celu podjęcia skutecznego przeciwdziałania im. Zagrożenia te mogą podważać istotę i podwaliny funkcjonowania instytucji narodowych i międzynarodowych, a także doprowadzić do ruiny gospodarki wielu państw<sup>2</sup>.

Jednocześnie także legalne organizacje działające w skali ponadpaństwowej zyskują na sile i wpływach dysponując technicznymi możliwościami dostosowania się do nowego środowiska bezpieczeństwa. Spekulanci giełdowi, handlowcy, korporacje międzynarodowe, firmy świadczące usługi internetowe posiadają obecnie możliwości znaczącego, globalnego wpływu na życie codzienne obywateli wielu państw. Globalizacja wspólnie z rewolucją w technologii informatycznej, dała tym instytucjom przewagę. Ich kontrola jest bardziej sprawowana za pośrednictwem rynków finansowych niż przez struktury globalne, a zakłócenia powstają według takiej samej zasady. Dlatego też nie powinno dziwić, że tradycyjne mechanizmy państwa oparte na idei granic, porządku, władzy, policji, struktur siłowych są zagrożone. Wydają się one także ze swojej natury niezdolne do przeciwstawienia się współczesnym wyzwaniom dla bezpieczeństwa. W miarę jak owa niezdolność staje się coraz bardziej widoczna, narasta rozczarowanie poprzednim systemem, i może powstać przekonanie, że wszystko w dziedzinie bezpieczeństwa zmierza ku gorszemu<sup>3</sup>.

Można zatem wnioskować, że w dającej się przewidzieć przyszłości jednym z najistotniejszych problemów dla głównych aktorów współczesnej

---

<sup>2</sup> Ibidem.

<sup>3</sup> R.Hall, C.Fox, Op.cit., s.8.

polityki światowej jest analiza trendów globalnych głównie politycznych i ekonomicznych. Kwestie globalne na początku obecnego stulecia mają także pierwszoplanowe znaczenie dla bezpieczeństwa światowego. Globalizacja oznacza bowiem wzrost różnego rodzaju powiązań między podmiotami życia międzynarodowego oraz wzajemne, najczęściej asymetryczne oddziaływania we wszystkich sferach życia społeczeństwa, od umiędzynarodowienia rynków i kapitału po kulturę masową, migracje, finanse i zapewnienie pokoju. Globalizacja w dziedzinie bezpieczeństwa wymusza konieczność większej coraz szybszej, wszechstronniejszej i bardziej skomplikowanej reakcji na zachodzące wydarzenia. Lapidarną ale bardzo wymowną formułę współzależności jakie tworzy globalizacja zdefiniował były zastępca sekretarza stanu USA S.Talbot: "co się dzieje tam, ma znaczenie tutaj" (*what happens there matters here*).

Spośród bogatego katalogu zagrożeń dla bezpieczeństwa Polski coraz bardziej realne stają się zagrożenia w sferze teleinformatycznej. Rośnie zagrożenie operacjami mającymi na celu dezorganizację kluczowych systemów informacyjnych instytucji rządowych oraz niektórych sfer sektora prywatnego, oddziałujących na system bezpieczeństwa państwa, a także operacjami związanymi z penetracją baz danych i prowadzenia działań dezinformacyjnych<sup>4</sup>.

Dynamiczny rozwój infrastruktury systemów komputerowych wpłynął w zdecydowany sposób na wzrost efektywności niemal każdej dziedziny ludzkiej działalności. Wraz z rozwojem informatyzacji pojawiły się nowe problemy związane z niewłaściwym zastosowaniem osiągnięć elektronicznego przetwarzania danych. Wzrost wykorzystania zaawansowanej technologii, a w szczególności systemów komputerowych i całej towarzyszącej przy tym infrastrukturze informatycznej spowodował pojawienie się nowego obszaru do nielegalnej działalności. Wraz ze wzrostem wykorzystania tej technologii pojawia się coraz częściej problem zapewnienia ich bezpieczeństwa.

---

<sup>4</sup> Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej.

Dostępność rozproszonych sieciowych ośrodków obliczeniowych nie ograniczonych tylko do jednego pomieszczenia, rozległość sieci, a także rozmycie pewnych działań związanych z komputerami i telekomunikacją powoduje, że dokonywanie przestępstw w "obszarze *hi-tech*" nie jest już rzadkością, lecz staje się podstawą działalności coraz większej ilości grup przestępczych. Wzrastająca liczba tej grupy przestępstw jest wynikiem wielu przesłanek, do których zaliczyć można:

- kompatybilność coraz większej ilości zdalnych systemów;
- dostępność niezbyt drogiego sprzętu i oprogramowania;
- przyjmowane standardy dla sprzętu i oprogramowania.

Z dotychczasowych badań zagrożeń związanych z oddziaływaniem przestępstw na systemy komputerowe wynika, że najczęściej wykorzystują oni informacje uzyskane w wyniku prowadzonego rozpoznania dotyczącego podatności na uszkodzenia określonego rodzaju oprogramowania. Prowadzi to do sytuacji, w której zanim producent zdoła zaimplementować, a klient zainstalować odpowiednią łatę (*ang. patch*), przestępca z reguły zdoła do tego czasu uzyskać dostęp do informacji przechowywanych w danym systemie. Nie ulega wątpliwości, że o wzroście ilości przestępstw decydują także takie elementy jak kompetencje *hackerów*, łatwość użytkowania systemów oraz unifikowalność narzędzi.

W wielu przypadkach samo środowisko stworzone przez zaawansowaną technologię, ułatwia sposób dokonania przestępstwa. Zdarza się często, że informacje przechowywane w postaci papierowej są lepiej chronione od tych utrzymywanych w postaci elektronicznej. Pomimo, że w systemach są dane o przeprowadzonych transakcjach, numerach kart kredytowych, zawartych umowach, klientach, a także inne, które mogą być atrakcyjne, nie tylko dla przestępcy, co do konkurencji, to rzadko stosuje się silne mechanizmy zabezpieczeń pozwalające na utrzymanie poufności i integralności danych. Tam,

gdzie się to stosuje, to znowu zapomina się o samej ochronie poszczególnych elementów zastosowanych zabezpieczeń, jak np. kluczy szyfrujących.

Ważnym zjawiskiem jest bezpieczeństwo informacyjne oraz legalność dokumentu elektronicznego i operacji elektronicznych. Autoryzacja przez podpis elektroniczny, personalizacja dostępu do sieci teleinformatycznej, systemy publicznych i prywatnych kluczy kryptograficznych, instytucja zaufanej trzeciej strony - to pilne zagadnienia związane z poufnością i wiarygodnością transmisji oraz z zabezpieczeniem osobistych praw użytkowników. Nie ulega wątpliwości, że brak ograniczeń terytorialnych jest jednym z podstawowych ułatwień dla wszelkiego rodzaju nadużyć dokonywanych przy wykorzystaniu sieci informacyjnych. Dlatego też istnieje duże zainteresowanie grup przestępczych wykorzystaniem infrastruktury sieciowej, jako nowego instrumentu nielegalnej działalności.

Z analiz przeprowadzonych przez specjalistów, jednoznacznie wynika, że grupy przestępcze prowadzą zakrojone na szeroką skalę rozpoznanie warunków ekonomicznych, prawnych i społecznych na obszarach, w których zamierzają długofalowo prowadzić nielegalną działalność. Dla dokonania obiektywnej oceny przestępcy opracowują swoiste wykazy problemów wymagających bliższego zbadania, co pozwala im na przeprowadzenie szybkiej oceny możliwości wykorzystania systemów informatycznych do prowadzenia działalności przestępczej na określonych obszarach. Najczęściej branymi pod uwagę elementami są:

- poziom wykształcenia policji i służb finansowych państwa w zakresie zwalczania przestępczości komputerowej, finansowej itp.;
- stan przestrzegania dyscypliny w utrzymaniu tajemnicy np. bankowej;
- zakres współpracy i szybkość wymiany informacji o podejrzanych transakcjach pomiędzy np. instytucjami finansowymi a policją lub innymi organami odpowiedzialnymi za zwalczanie przestępczości finansowej;

- rzeczywista sprawność wewnętrznych mechanizmów kontroli instytucji finansowych przede wszystkim systemów ochrony oraz monitorowania wykonywanych transakcji.

Z dotychczasowej oceny działalności przestępczej wynika, że główna jej uwaga skoncentrowana jest na obszarach funkcjonowania państwa pod kątem prowadzenia nielegalnych operacji finansowych. Większość istotnych informacji stanowiących niekiedy tajemnice finansowe czy też handlowe jest przechowywana w postaci elektronicznej. Dlatego też grupy przestępcze w celu uzyskania istotnych dla nich informacji wynajmują wyspecjalizowanych w tej działalności włamywaczy (*hackerów*). Począwszy od uzyskania takich informacji najprostszymi rodzajami ataków od zewnątrz (poprzez sieć o ile docelowy system ma połączenie ze "światem zewnętrznym"), a skończywszy na zatrudnieniu włamywacza w firmie pozostającej w zainteresowaniu przestępców (tzw. atak od środka). Warto także zauważyć, że grupy przestępcze do swoich działań wykorzystują często "starych" pracowników firmy (zdarza się, że są to administratorzy systemów komputerowych), którzy kierując się chęcią np. łatwego zarobku przekazują w niepowołane ręce "ważne" dla państwa informacje. Na ogół działania ich mają charakter działań operacyjnych. Często pracownik firmy, który jest w środku systemu informatycznego pozostającego w zainteresowaniu, uzyskuje legalnie bądź też nie, kolejne poziomy zabezpieczeń (np. najpierw jedno hasło do systemu - zwykłego użytkownika, a potem nawet hasło superużytkownika). Na ogół zdarza się, że głównym zadaniem skorumpowanego użytkownika jest wprowadzenie do systemu specjalnie przygotowanego oprogramowania (*konia trojańskiego, bomby logicznej itp.*), pozwalającego przestępcom osiągnąć zamierzony cel. Z reguły prowadzi to do "wykradania" informacji.

Nie można także pominąć działań prowadzonych przez grupy przestępcze, których głównym zadaniem jest uzyskanie jak największej ilości informacji

o danym systemie informatycznym. Ma to na celu dokonanie ataku i w konsekwencji tego "wykradnięcia" danych lub unieruchomienia systemu.

Oprócz zorganizowanych grup przestępczych, interesujących się systemami komputerowymi mamy również do czynienia z pojedynczymi przestępcami tzw. "*crackerami*"<sup>5</sup> którzy wykorzystują swoje umiejętności, np. do zabawy lub do potwierdzenia swojej wiedzy. Tego typu przestępcy tworzą najczęściej ściśle powiązane grupy na skalę międzynarodową. Relacje pomiędzy członkami takich grup ograniczają się najczęściej do wymiany wszelkich informacji na temat nowych metod łamania zabezpieczeń, odkrytych słabych punktów ogólnie znanego i wykorzystywanego oprogramowania, a także wielu innych informacji ułatwiających penetrowanie systemów bez konieczności posiadania specjalnych uprawnień. Przełamywanie zabezpieczeń lub zdalna destrukcja dowolnego systemu staje się dla nich bagatelą.

## **1.2. Terroryzm informacyjny**

Organizacje terrorystyczne coraz częściej dostrzegają infrastrukturę teleinformatyczną jako cenny do zaatakowania obiekt. Ze względu na dotychczasowe niskie możliwości działalności terrorystów w cyberprzestrzeni, główną uwagę skupiają oni na destrukcji fizycznej infrastruktury technicznej takich obiektów jak elementy stacji nadawczych i przekaźnikowych oraz kluczowe serwery internetowe. Niszczenia tych obiektów dokonują metodą ich wysadzania lub bezpośredniego pozbawiania cech ich używalności.

Fizyczne niszczenie wybranych elementów sieci komputerowych i infrastruktury teleinformatycznej pozwolić może terrorystom na osiągnięcie efektów wyłącznie w skali lokalnej. Osiągnięcie przez terrorystów większego

---

<sup>5</sup> "cracker" jest to osoba uzyskująca dostęp do systemu, do którego nie ma uprawnień i zwykle posiadająca intencje mające na celu manipulację lub uszkodzenie przechowywanych w nim danych.

zakresu zniszczeń jest mało prawdopodobne ze względu na konieczność posiadania przez nich szczegółowych informacji dotyczących lokalizacji obiektów, dostępu do nich oraz sposobów ich chronienia. Nie bez znaczenia jest również fakt, iż w przypadku zniszczenia linii komunikacyjnych ruch w Internecie jest automatycznie przekierunkowany dzięki dużej liczbie systemów awaryjnych oraz heterogenicznej organizacji sieci internetowej.

Fizyczne niszczenie obiektów nazywane jest często terroryzmem technicznym. Pomimo lokalnych jego obiektów, główną jego zaletą jest fakt łatwości jego przeprowadzenia. Mogą tego dokonać terroryści nie legitymujący się nawet wykształceniem technicznym. Znaczenie lokalnego zasięgu akcji terrorystycznych rośnie wówczas, gdy stanowią one element wspierający główną operację terrorystyczną. Może nią być np. tymczasowe zdezorganizowanie systemów powiadamiania służb ratowniczych lub komunikacji między siłami ochrony atakowanego obiektu. Należy więc przypuszczać, że z tego powodu ilość ataków terrorystycznych o charakterze technicznym będzie mieć tendencję rosnącą. Klasycznym przykładem ataku terrorystycznego o charakterze technicznym było zniszczenie przez terrorystów Al Qaidy systemów identyfikacji samolotu podczas zamachów w dniu 11 września 2001 roku.

### **1.3. Rodzaje atakowanych systemów informatycznych.**

Stosunkowo niewielka liczba ataków cybernetycznych w porównaniu do konwencjonalnych aktów terroru uwarunkowana jest wieloma czynnikami, do których można zaliczyć:

- stosunkowo niską wiedzę kierownictw organizacji terrorystycznych z zakresu działań w cyberprzestrzeni;
- stosunkowo niską medialność ataków cybernetycznych w porównaniu do konwencjonalnych aktów terroru;

- brak specjalistów z zakresu stosowania terroryzmu cybernetycznego.

W ostatnim okresie dostrzega się wyraźnie próby zainteresowania się organizacjami terrorystycznymi nowymi technologiami łącznie ze szkoleniem specjalistów w zakresie telekomunikacji i informatyki. Wynika z powyższego, iż cyberterroryzm będzie przybierał na znaczeniu stając się ważnym elementem podejmowanych wspólnie aktów terrorystycznych. W oparciu o analizę dotychczasowej strategii działań terrorystycznych należy przypuszczać, że prawdopodobnymi celami ataków terrorystycznych będą systemy informatyczne wykorzystywane w sferze wojskowej.

Nie ulega również wątpliwości, że w przeciwieństwie do większości systemów informatycznych stosowanych w sferze militarnej, systemy cywilne nie są fizycznie odseparowane od innych sieci komercyjnych i publicznych co w znacznym stopniu ułatwia dostęp do nich.

Do najbardziej zagrożonych systemów informatycznych zaliczyć można:

- systemy wspomagające zarządzanie ruchem powietrznym oraz transportem zwłaszcza zaś kolejowym;
- systemy wykorzystywane w instytucjach państwowych pracujące na rzecz baz danych oraz powiadamiania służb ratowniczych i reagowania antykryzysowego;
- systemy pracujące w różnych sektorach jak w bankowości czy też stosowane przy produkcji i dystrybucji dóbr o znaczeniu strategicznym, jak ropa, energia elektryczna, gaz oraz woda pitna.

Biorąc pod uwagę zaprezentowane powyżej obszary zastosowań systemów informatycznych, łatwo jest dostrzec, że mogą być one obiektami szczególnego zainteresowania ze strony różnych grup terrorystycznych. Wywołanie zakłóceń w pracy tych systemów spowodować może duże straty ekonomiczne oraz negatywne zjawiska w sferze społecznej. Dlatego też pilnym zadaniem władz państwowych oraz kierownictw różnych instytucji prywatnych jest prowadzenie skutecznych działań na rzecz utrzymania wysokiego poziomu bezpieczeństwa

zarówno w odniesieniu do sprzętu jak też i programów wykorzystywanych w systemach informatycznych.

#### **1.4. Terroryzm informacyjny i jego wpływ na globalne środowisko bezpieczeństwa**

Współcześni teoretycy i praktycy wojskowi mówiąc o sztuce wojennej "czwartej generacji" najczęściej mają na uwadze globalne, transnarodowe zagrożenia zwłaszcza zaś terroryzm. Spośród wielu zagrożeń o charakterze globalnym bardzo często wymienia się możliwość stosowania terroryzmu informacyjnego.<sup>6</sup> Terroryzm informacyjny lub "piractwo informacyjne" są odmianami wojny informacyjnej pozwalającej osiągnąć założone cele terroryzmu. Często są nimi przemoc względem obiektów cywilnych i wojskowych. Ryzyko ingerencji w systemy informatyczne będzie wzrastało wraz z rozwojem technologii informatycznych.

W przyszłości działania terrorystyczne będą prawdopodobnie miały na celu zapewnienie terrorystom dostępu do najnowszych technologii stanowiących swoistą "ochronę bogactwa" państw uprzemysłowionych. Dlatego też grupy terrorystyczne oprócz dotychczasowych zainteresowań bronią masowego rażenia, systemu komunikacji i innymi odmianami osiągnięć technologicznych będą uciekały się do terroryzmu informacyjnego. Ponieważ funkcjonowanie społeczeństw, zwłaszcza w państwach bogatych, staje się w coraz większym stopniu uzależnione od systemów informatycznych, stąd też terroryzm informacyjny przybiera formę szczególnego niebezpieczeństwa określonego nawet katastroficznym.

---

<sup>6</sup> M.G.Devost, Political violence in the Information Age, University of Vermont 1995, s.75.

Skutki konwencjonalnych działań terrorystycznych, jakkolwiek wielce dotkliwe i bolesne mają na ogół ograniczony zasięg. Natomiast w przypadku piractwa informatycznego (cyberterrorism) skala destrukcyjnych działań może mieć ogromny zasięg, co jest oczywiste, gdy uwzględni się postępujące uzależnienie społeczeństw od technologii informatycznych.

Równie groźną odmianą terroryzmu informacyjnego stanowić może ingerencja w sieci informatyczne z zamiarem zniszczenia lub uniemożliwienia ich funkcjonowania czy też sprawowania nad nimi kontroli (cyber-attack). Ten rodzaj terroryzmu może być realizowany generalnie przy zastosowaniu dwóch metod:

- fizycznego zniszczenia systemu informatycznego,
- objęcia całkowitej kontroli nad funkcjonowaniem systemu.

Przykładem drugiej metody może być przejęcie kontroli nad informatycznym systemem samolotowym przez terrorystów islamskich wykonujących uderzenie na Światowe Centrum Handlowe 11 września 2001 r.

Można zakładać, że cywilnymi obiektami zainteresowań tego rodzaju terroryzmu będą systemy informatyczne decydujące o bezpieczeństwie społeczeństwa, takie jak ochrony żywności, wody, transportu ruchu lotniczego itp. W odniesieniu do obiektów wojskowych . mogą to być systemy dowodzenia i kontroli (C2) oraz logistyki.

Wielce prawdopodobnym obiektem zainteresowań terroryzmu informacyjnego może być sieć internetowa, która stopniowo przybiera charakter globalny. Pierwszymi oznakami tego typu działań są tzw. hakersi. Nie można także wykluczyć, że "cyber-terrorism" będzie swego rodzaju logicznym modelem przyszłego konfliktu, który prowadzony będzie w "cyberprzestrzeni" .

"Cyber-wojna" może się stać ekwiwalentem wojen prowadzonych do tej pory między państwami.

Wzrastające uzależnianie się sił zbrojnych, rządów i organizacji od systemów informatycznych stanowi dużą przestrzeń oddziaływań ze strony

terrorystów. Niekoniecznie muszą to być działania dużych grup terrorystycznych. Tego typu zaplanowane operacje skierowane przeciwko społeczeństwu Zachodu wydają się wielce prawdopodobne. Przykładem tego typu operacji był atak terrorystyczny z września 2001 roku. Przeprowadzone w ostatnich latach w Stanach Zjednoczonych badania dotyczące możliwości włamania się do systemów informatycznych dużych organizacji dowiodły, że w 80% było ono możliwe do przeprowadzenia.<sup>7</sup> Świadczy to o niemożliwości pełnej ochrony systemów przed działaniami terrorystycznymi typu "*cyber-terrorist attack*".

W czasie konfliktu kosowskiego otwarte sieci dowodzenia stanowiły znakomitą pokusę dla hakerów. W tydzień po rozpoczęciu operacji NATO poniosło istotną porażkę prestiżową. Atakujący hackerzy z Serbii i Czarnogóry zablokowali oficjalny serwer WWW Sojuszu. Uczynili to wysyłając przez łącza poczty elektronicznej kilkadziesiąt tysięcy listów protestujących przeciwko operacji NATO w Jugosławii.

Kiedy informatycy Sojuszu odcięli możliwość wysyłania poczty, zaczęły się próby wejścia na stronę WWW z zamiarem jej zniekształcenia lub zniszczenia. Były one tak częste a hackerzy na tyle groźni, że po tygodniu działanie serwera trzeba było zawiesić na trzy dni. W tym czasie zmieniono strukturę sieci i oficjalną stronę internetową Sojuszu. Informatycy NATO założyli odpowiednie filtry wzmacniające moc serwerów.

Komputery NATO musiały odpierać ataki wirusów, które codziennie wysyłali hackerzy. Brytyjski analityk wojskowych technik i zastosowań cywilnych technik informatycznych w Alacan Perarson stwierdził, że wojna ta może dokonać "rewolucyjnych zmian w internecie" stwierdził również, że "dotychczasowa otwarta formuła stron WWW nie da się prawdopodobnie utrzymać".

---

<sup>7</sup> Willam H. Kennedy, *The New Threat the Millenium*, (w:) *Technology and terrorism*, USA 2008, s.6.

Może się także okazać, że do zadań wojsk walki radioelektronicznej należy również niszczenie stron i serwerów WWW należących do firm działających na terytorium przeciwnika. Obecnie jako przeciwdziałania zalecono "odgraniczenie internetu od firmy", czyli wydzielenie fragmentu sieci pracującego stale on-line lub stosowanie przynajmniej trójstopniowych zabezpieczeń z *firewalkami* jako bramami systemu.

Powyższe każe zwracać uwagę na zmianę poglądów dotyczących wojny i sposobów planowania strategicznego. Nowe konflikty będą w coraz większym stopniu konfliktami informatycznymi.

Innym aspektem bezpieczeństwa informacyjnego pojawiającym się w ostatnim czasie jest terroryzm elektromagnetyczny. Obecnie w świecie jak i w Polsce zaczyna pojawiać się coraz więcej informacji z tego zakresu. Terroryzm elektromagnetyczny jest umyślnym, wytwarzaniem i wprowadzeniem elektromagnetycznej energii zakłócającej w pole emisji<sup>8</sup> pracującego sprzętu lub systemów elektronicznych w zamiarze uszkodzenia albo zniszczenia. Przy tym chodzi tu o akcje umotywowane terrorystycznie albo kryminalnie. Terroryzm elektromagnetyczny może być również rozpatrywany jako sposób (rodzaj) ofensywnej nowoczesnej walki informacyjnej. Bezprawne użycie energii elektromagnetycznej może być skierowane przeciw osobom, rządowi, cywilnej gospodarce lub wybranym obiektom w połączeniu z politycznymi lub socjalnymi żądaniami. Tak postrzegany "terroryzm - elektromagnetyczny" charakteryzuje tylko jego ekstremalny kierunek, może on jednak również dotyczyć wandalów, elementów kryminalnych lub kręgów społecznych.

Terroryzm elektromagnetyczny jako termin pojawił się w 1996 roku, wówczas to Generał Loborev wygłosił plenarny wykład podczas konferencji

---

<sup>8</sup> Każde elektroniczne urządzenie cyfrowe wytwarza, w zależności od częstotliwości pracy, szybkości impulsów sterujących, wielkości amplitudy tych impulsów, elektromagnetyczne pole emisji zakłócającej w ściśle określonym zakresie częstotliwości. Im większa jest szybkość impulsów sterujących i wyższa częstotliwość pracy, tym wyższa częstotliwość promieniowania zakłócającego.

AMEREM w Albuquerque (USA). W wykładzie tym użył jako pierwszy terminu "terroryzm elektromagnetyczny" wskazując publicznie na problem, który do tej pory budził zaniepokojenie jedynie środowisk, zajmujących się problemami kompatybilności elektromagnetycznej. Komentarz generała na temat możliwości zastosowania energii elektromagnetycznej do pokonywania systemów alarmowych i systemów porozumiewania się przeciwnika, doprowadził do tego, że sprawa ta stała się przedmiotem ożywionej dyskusji zarówno podczas samej konferencji AMEREM, jak i po jej zakończeniu. Problem ten podnoszono w następnych latach w ramach spotkań różnych komisji i w czasie sympozjów EMC na temat kompatybilności elektromagnetycznej między innymi: w Tel Avivie rok 1998, Zurichu rok 1999 jak również we Wrocławiu w latach 1998 i 2000.

W chwili obecnej nie jest jasne jak łatwo lub jak skutecznie można wykorzystać tego typu potencjalną broń, ale oczywiste jest, że środowiska zajmujące się problematyką kompatybilności elektromagnetycznej muszą być przygotowane (także w kraju) na poradzenie sobie z tym zagrożeniem, w momencie jego zaistnienia. Badania pokazują, że możliwe jest za pomocą generatorów mikrofalowych zakłócanie bądź ingerowanie w pracę większości dostępnych handlowo urządzeń stosowanych w technologii informacyjnej. Przynieść to może następujące efekty:

- zniszczenie lub przepalenie urządzeń technicznych systemu informacyjnego,
- czasowe błędy lub zakłócenia urządzeń technicznych systemu informacyjnego,
- zredukowanie wydajności urządzeń technicznych systemu informacyjnego, np. ograniczenie możliwości systemów ochrony.

Należy stwierdzić, że w ostatnich pięciu latach technika mikrofalowa poczyniła ogromne postępy na polu miniaturyzacji tak, że obecnie silne impulsy można uzyskać przy wykorzystaniu stosunkowo niewielkich urządzeń. Stąd też potencjalnie dużym i coraz bardziej realnym zagrożeniem staje się

wykonanie ataku terrorystycznego z wykorzystaniem promieniowania elektromagnetycznego. Możliwości te uzyskujemy wykorzystując urządzenia mikrofalowe o dużej sprawności (*High Power Microwave = HPM*) w celu niszczenia lub przynajmniej zakłócania.

Badania w zakresie technologii HPM prowadzone są przede wszystkim w Stanach Zjednoczonych głównie w obszarze militarnym na kierunku tworzenia nowych broni (oraz zabezpieczeń przed nią). Są to bronie dalekiego zasięgu do niszczenia elektroniki sterującej w raketach. Przy okazji nie zapomniano o sektorze cywilnych technologii i odpowiedniej ochronie (zabezpieczeniu) przed atakiem mikrofalowym przeprowadzanym z małej odległości (mniej niż 1000m.). Atak taki może być przeprowadzany np. przez grupę terrorystów na budynek rządowy (pełen elektroniki) kompletnie do tego nie przygotowany.