Information security as a target of terrorist attack

Bezpieczeństwo informacyjne jako cel ataku terrorystycznego

Krzysztof Liderman, Andrzej Malik

Wojskowa Akademia Techniczna, Wydział Cybernetyki,
lider@ita.wat.edu.pl

Sztab Generalny Wojska Polskiego, andrzej.malik@mon.gov.pl

Abstract

One of the components of the widely understood security is the information security that due to the increasing utilization of technical means in the transmission, storage and processing of information, is vulnerable to various forms of so-called cyber threats. Such real cyber threats are now terrorist attacks conducted on networks and information systems. The article presents a brief review of basic national ("National Security Strategy of the Republic of Poland" and "Cyber Security Governmental Program) and foreign ("US Department of Defense Strategy for Operating in Cyberspace", "Consensus Audit Guidelines" and ISO/IEC 27000 series) documents related to threats in cyberspace in order to intentionally underline deficiencies in the current Polish solutions. Additionally, as a pessimistic forecast, there is high probability that the terrorist attacks on networks and information systems will succeed due to broad, not effectively controlled "destruction box" of potential attacks, incoherent scope of responsibilities of different security institutions, too complex security organizational structure, luck of standardization of terminology, and finally, lack of a proper technical knowledge among the national lawmakers.

KEYWORDS: *computer security, cybersecurity, security management, cyberterrorism, information warfare*

Wprowadzenie

Jak słusznie zauważyli organizatorzy konferencji „*Jakość w działaniach na rzecz bezpieczeństwa wewnętrznego państw grupy wyszehradzkiej z perspektywy europejskiej*", problem bezpieczeństwa jako najwyższa wartość

współczesnego społeczeństwa międzynarodowego nie występował w tak ostrej formie, jak obecnie, w XXI wieku. Jednym ze składowych tego bezpieczeństwa jest *bezpieczeństwo informacyjne*, które ze względu na coraz większy udział w transmisji, przechowywaniu i przetwarzaniu informacji środków technicznych, jest podatne na różne formy tzw. *cyberzagrożeń*, w tym tych związanych z działaniami terrorystycznymi.

Rozpatrując wizję polityki i strategii bezpieczeństwa państw Grupy Wyszehradzkiej w kontekście przyjętej koncepcji strategicznej NATO z 2010 roku z uwzględnieniem postawionej tezy o cyberzagrożeniach, należy, jako podbudowujące tę tezę stwierdzenia, zacytować przede wszystkim następujące zapisy[1]:

(…) 12. Ataki cybernetyczne stają się coraz częstsze, lepiej zorganizowane i bardziej kosztowne, biorąc pod uwagę szkody, jakie wyrządzają administracjom rządowym, biznesowi, gospodarce, a potencjalnie także transportowi, sieciom dostaw i innej infrastrukturze krytycznej; mogą one osiągnąć poziom, którego przekroczenie zagraża narodowemu i euroatlantyckiemu dobrobytowi, bezpieczeństwu i stabilności. Źródłem takich ataków mogą być obce siły wojskowe i służby wywiadowcze, zorganizowane grupy przestępcze, terrorystyczne i/lub grupy ekstremistyczne (…).

14. Niektóre znaczące trendy związane z technologią – włączając w to rozwój broni laserowej, walkę elektroniczną oraz technologie hamujące dostęp do przestrzeni kosmicznej, najprawdopodobniej będą w poważny sposób oddziaływać na planowanie wojskowe i operacje NATO (…).

19. Zapewnimy, aby NATO dysponowało pełnym zakresem zdolności niezbędnych do odstraszania i obrony przed jakimkolwiek zagrożeniem bezpieczeństwa naszych społeczeństw. Dlatego będziemy: (...) Rozwijać dalej nasze możliwości zapobiegania, wykrywania, obrony przed atakami cybernetycznymi oraz odtwarzania zdolności po nich, w tym wykorzystując proces planowania NATO na rzecz wzmocnienia i koordynacji narodowych zdolności w dziedzinie obrony cybernetycznej, włączając instytucje NATO w scentralizowany system ochrony cybernetycznej oraz integrując system monitorowania, ostrzegania i reagowania cybernetycznego NATO z państwami członkowskimi.

Zatem jednym z kluczowych obszarów, na których działania terrorystyczne czy też „cyberprzestępcze" mogłyby być realizowane, są sieci i sys-

1 „Koncepcja strategiczna obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego, przyjęta przez szefów państw i rządów w Lizbonie", Lizbona 19-20 listopada 2010 r.

temy teleinformatyczne, będące kluczowym elementem infrastruktury wszystkich rozwiniętych cywilizacyjnie państw. Temat możliwości takich działań podchwyciły mass media (bo temat jest nośny medialnie), przy okazji z zapałem tworząc wraz z politykami nowe, bogate słownictwo, obfitujące w słowa z przedrostkiem *cyber-* (cyberterroryzm, cyberatak, cyberobrona, cyberprzestrzeń, cyberprzestępstwo itp.)[2]. Wydaje się jednak, że ataki na systemy i sieci teleinformatyczne są skazane na powodzenie, co jest zresztą dobrą wiadomością dla mass mediów („dobra wiadomość to zła wiadomość"). Uzasadnienie tezy o niezawodnym powodzeniu ataków jest w dalszej części artykułu.

1. Wybrane dokumenty z zakresu cyberbezpieczeństwa

Również polskie opracowania wskazują na wzrost zagrożenia działalnością przestępczą w cyberprzestrzeni[3]. Wysiłek administracji państwa polskiego w zakresie ochrony polskich zasobów informacyjnych dobrze ilustrują dwa dokumenty: „*Strategia*"[4] i „*Rządowy program ochrony cyberprzestrzeni*"[5]. W „*Strategii*" znajduje się rozdział 3.8 „*Bezpieczeństwa informacyjne i telekomunikacyjne*" (paragrafy 78-82[6]) oraz rozdział 4.3 „*Podsystemy wykonawcze*", gdzie znajduje się paragraf 114 „*Informatyzacja i telekomunikacja*". Podstawową wadą przywołanych zapisów, naszym zdaniem, jest brak usystematyzowania problemów do rozwiązania oraz przesadne akcentowanie znaczenia bezpieczeństwa telekomunikacyjnego – oprócz tytułu, sformułowanie „bezpieczeństwo informacyjne" nigdzie w paragrafach 78-82 się nie pojawia.

Drugi z przywołanych dokumentów zawiera zarys podstaw, na których ma być budowany system ochrony „cyberprzestrzeni". Pomijając zasadniczą, dla sprawy skutecznej ochrony, ułomność definicji zamieszczonych na stronie 6 tego dokumentu (w tym kluczową definicję „cyberprzestrzeni"), w dokumencie proponuje się skoordynowanie przedsięwzięć natury legislacyjnej, organizacyjnej, edukacyjnej i technicznej obligatoryjnych dla or-

2 Liderman K., *O zagrożeniach dla skutecznej ochrony informacji, przetwarzanej w sieciach i systemach teleinformatycznych, powodowanych nowomową. Studia Bezpieczeństwa Narodowego. Nr 2. Str. 401-409. IOiZ. WAT. Warszawa. 2011.*
3 Raport MSWiA o stanie bezpieczeństwa w Polsce w 2010 r.
4 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*. Warszawa. 2007.
5 *Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016.* Wersja 1.1. Warszawa. Czerwiec. 2010.
6 Godny uwagi jest zapis z paragrafu 79: *„Priorytetem państwa będzie wspieranie narodowych programów i technologii informacyjnych"*.

ganów władzy publicznej i operatorów infrastruktury krytycznej i dobrowolnych dla pozostałych podmiotów – użytkowników cyberprzestrzeni. Należy mieć nadzieję, że docelowa wersja ww. programu zostanie dobrze dopracowana, ponieważ w obecnej postaci, poza rozrostem biurokracji, nie rokuje innych, oprócz propagandowych, „sukcesów".

Z wysiłków innych państw w zakresie ochrony informacji, i ogólniej cyberprzestrzeni, należy wymienić przede wszystkim działania USA. Podstawowymi są tutaj *„Strategia działania w cyberprzestrzeni"*[7] oraz wydany w lutym 2009 roku „techniczny" dokument *„Consensus Audit Guidelines"* (CAG). Pierwszy z dokumentów prezentuje pięć inicjatyw traktujących o: cyberprzestrzeni jako kolejnej domenie operacyjnej – obok ziemi, morza, powietrza i przestrzeni kosmicznej; wdrożeniu nowej koncepcji operacyjnej; współpracy z instytucjami rządowymi i krajowymi agencjami oraz sektorem prywatnym; budowaniu relacji z sojusznikami USA i innymi partnerami zagranicznymi oraz działaniu na rzecz rozwoju technologii służących bezpieczeństwu cyberprzestrzeni. Głównym założeniem tej strategii jest wzmocnienie zdolności obronnych w cyberprzestrzeni i zniechęcenie potencjalnych agresorów do „cyberataku" na USA.

W drugim z dokumentów, promowanym np. przez instytut SANS, można przeczytać:

This consensus document is designed to begin the process of establishing that prioritized baseline of information security measures and controls. The consensus effort that has produced this document has identified twenty specific security controls that are viewed as essential for blocking known high priority attacks.

W CAG wyspecyfikowano 20 przedsięwzięć niezbędnych (zdaniem autorów opracowania) do szybkiego zabezpieczenia systemu i sieci komputerowej przed „cyberatakami". Każdy z 20 punktów (przedsięwzięć), zatytułowany *Critical Control xx***,** składa się z trzech części:

– *How do attackers export the lack of this control?*; opisującej sposób wykorzystania niezabezpieczonej podatności,

– *How can this control be implemented, automated, and its effectiveness measured?*; podającej, w postaci czterech grup zaleceń, sposoby minimalizowania wyspecyfikowanej podatności,

– *Procedures and tools for implementing this control*; zawierajacej

7 Department Of Defense Strategy For Operating In Cyberspace, lipiec 2011 r.

wskazówki na temat możliwości wspomagania procesu zabezpieczania narzędziami programowymi i przedsięwzięciami organizacyjnymi.

Także gremia ponadpaństwowe poczyniły wysiłki mające na celu opracowanie standardów w dziedzinie zarządzania ochroną informacji. Należą do nich przede wszystkim normy serii ISO/IEC 27000 oraz standard *Common Criteria* (standardowi temu odpowiadają normy ISO/IEC oraz normy polskie).

W zaprezentowanych kierunkach działania mieści się także inicjatywa polskiego prezydenta B. Komorowskiego dotycząca zmian w polskim prawie. Celem bezpośrednim prezydenckiego projektu ustawy jest stworzenie podstaw prawnych do uwzględniania problematyki cyberprzestrzeni w przygotowaniu się państwa na ewentualność działania w takich sytuacjach szczególnych zagrożeń, w których konieczne byłoby wprowadzenie jednego ze stanów nadzwyczajnych: stanu klęski żywiołowej, stanu wyjątkowego lub stanu wojennego[8].

2. Systemy informacyjne jako potencjalny cel ataku terrorystycznego

Podstawą działania struktur politycznych i administracyjnych są pieniądze i informacja[9]. Jej gromadzeniu, przetwarzaniu i przesyłaniu służą systemy informacyjne, których integralną częścią są systemy i sieci teleinformatyczne. Dla uproszczenia rozważań przyjmuje się założenie, że połączone systemy tworzą sieci w taki sposób, że jest możliwa pomiędzy nimi wymiana informacji.

Na system teleinformatyczny składa się:

1. *Informacja* (w postaci danych) przetwarzana[10], przechowywana i przesyłana w systemie;

2. *Sprzętowe* elementy umożliwiające przetwarzanie, przechowywanie i przesyłanie informacji: komputery, pamięci zewnętrzne, łącza, urządzenia sieciowe (rutery, koncentratory, bezprzewodowe punkty dostępowe, itp.);

8 Patrz: wystąpienie szefa BBN ministra Stanisława Kozieja na wspólnym posiedzeniu Komisji Sejmowych: Obrony Narodowej, Komisji Spraw Zagranicznych oraz Komisji Administracji i Spraw Wewnętrznych na temat cyberprzestrzeni w ustawach o stanach nadzwyczajnych, Warszawa 13 lipca 2011.
9 Dla struktur gospodarczych, oprócz informacji i pieniędzy, istotne są przede wszystkim zasoby materialne.
10 W literaturze często używa się też terminu „przetwarzana" w rozumieniu „przetwarzana, przesyłana i przechowywana".

3. *Programowe* elementy umożliwiające przetwarzanie, przechowywanie i przesyłanie informacji: systemy operacyjne, oprogramowanie narzędziowe, aplikacje;

4. *Infrastruktura*: budynki, zasilanie w energię elektryczną i wodę, systemy ochrony przed nieuprawnionym dostępem fizycznym do elementów systemu teleinformatycznego itd.;

5. *Ludzie*-operatorzy korzystający z możliwości oferowanych przez system teleinformatyczny (potocznie nazywani użytkownikami) oraz pracownicy zajmujący się „utrzymaniem w ruchu" systemu teleinformatycznego (administratorzy techniczni).

Każdy z wymienionych pięciu podstawowych elementów składowych systemu teleinformatycznego może być potencjalnym celem ataku terrorystycznego. W zależności od przeznaczenia i konstrukcji systemu teleinformatycznego, na określenie ogółu zagadnień szeroko rozumianej ochrony, używa się terminów *bezpieczeństwo na zewnątrz* oraz *bezpieczeństwo do wewnątrz*.

Termin „bezpieczeństwo na zewnątrz" określa ochronę przed zagrożeniami dla środowiska, w tym dla człowieka, w którym pracuje system komputerowy, spowodowanymi nieprawidłowym działaniem tego systemu. Dotyczy to głównie tzw. przemysłowych systemów sterowania (ICS, od ang. *Industrial Control System*; zwykle są to systemy czasu rzeczywistego), np. monitorujących stan pacjenta w szpitalu, sterujących robotami na zautomatyzowanej taśmie produkcyjnej, nadzorujących ruch kolejowy itd[11]. W języku angielskim ogół zagadnień związanych z ochroną tego typu (w sensie niedopuszczania do katastrof) określa się zwykle terminem *safety*. Warto zwrócić uwagę, że systemy tego typu są często elementami towarzyszącymi obiektom z tzw. *infrastruktury krytycznej państwa*.

Termin „bezpieczeństwo do wewnątrz" określa ochronę przed zagrożeniami dla informacji przechowywanej, przetwarzanej i przesyłanej w systemie teleinformatycznym. Dotyczy to głównie sieci teleinformatycznych biur, banków, organizacji naukowych itd. W języku angielskim ogół zagadnień związanych z ochroną tego typu (w sensie niedopuszczania do utraty tajności, integralności, dostępności informacji) określa się zwykle terminem *security*. To rozróżnienie znajduje swoje odbicie w praktyce nie tylko w różnych unormowaniach, ale także

11 W tej klasie mieszczą się też tzw. *komputery pokładowe*, montowane na jednostkach latających, pływających i jeżdżących po lądzie. Przykładem mogą być pokładowe komputery nawigacyjne albo komputery sterujące bronią pokładową.

w strukturze cyklu życia systemów i sposobie ich wytwarzania oraz utrzymywania.

Zagrożenia to wszystkie możliwe działania (sił natury, ludzi, maszyn itp. lub zaniechanie wymaganych działań przez człowieka) dotyczące jakiegoś zasobu lub procesu, które mogą spowodować szkody. Zagrożenie spowoduje szkody tylko wtedy, jeżeli istnieją wady lub luki, czyli tzw. podatności, w infrastrukturze organizacji, procedurach, obsadzie stanowisk pracy personelem, zarządzaniu i administrowaniu, sprzęcie, oprogramowaniu itd., które to wady lub luki mogą być wykorzystane przez zagrożenia do spowodowania szkód w systemie teleinformatycznym lub działalności użytkownika.

Podstawowe klasy zagrożeń dla poprawnego działania sieci i systemów informacyjnych stanowią:

1. Siły wyższe (w tym katastrofy naturalne),
2. Błędy ludzi wykorzystujących lub obsługujących systemy informacyjne (w tym błędy w organizacji pracy),
3. Celowe, szkodliwe działania ludzi skierowane na systemy informacyjne,
4. Awarie sprzętu (elementów i podzespołów mechanicznych, elektronicznych, elektromechanicznych) i wady oprogramowania.

Zagrożenia terrorystyczne w podanej klasyfikacji mieszczą się w punkcie 3, (chociaż, ze względu na skutki, czasami w innych klasyfikacjach są umieszczane w punkcie 1, tzn. przyjmuje się, że skutki ataku terrorystycznego są porównywalne z katastrofa naturalną).

W ostatnich latach obserwuje się włączanie do przemysłowych systemów sterowania (ICS) rozwiązań stosowanych dotąd w „klasycznych" sieciach biurowych: wykorzystanie Internetu jako medium komunikacyjnego oraz powszechnie używanych popularnych systemów operacyjnych i sprzętu komputerowego. Dodatkowo wydzielone dotąd ICS łączy się z sieciami biurowymi. Dwa podstawowe powody takiego postępowania to:

– kierownictwo firmy chce nie tylko mieć wpływ na sterowanie procesami produkcyjnymi, ale chce mieć także dostęp do jak największej ilości informacji o tych procesach w dowolnym miejscu i o każdym czasie;

– te informacje powinny być bezpośrednio dostępne dla systemów typu MES (ang. *Manufacturing Execution Systems*) czy ERP (ang.

Enterprise Resorce Planning).

Wymienione fakty dają nowy jakościowo obraz współczesnych sieci przemysłowych – pojawiły się w nich nowe problemy z zapewnianiem bezpieczeństwa. **Razem – klasyczne sieci teleinformatyczne oraz sieci przemysłowe korzystające z nowych sposobów komunikacji** (Internet, sieci Wi-Fi, sieci komórkowe), **jako element systemów informacyjnych różnej skali** (obiektu, organizacji, państwa), **tworzą potencjalny obszar ataku terrorystycznego**.

Podstawową przesłanką pesymistycznej prognozy co do skuteczności ataków terrorystycznych na systemy informacyjne jest to, że tzw. „pole rażenia" jest niezwykle szerokie. Celem ataku, ze względu na oczekiwane skutki, może być:

1. uniemożliwienie przesyłania informacji,
2. uniemożliwienie przetwarzania informacji,
3. ingerencja w informację:

a) (nieuprawnione) zapoznanie się z treścią informacji, tzn. naruszenie *tajności*,

b) (nieuprawnione) zmodyfikowanie informacji, tzn. naruszenie *integralności*.

Celem ataku, ze względu na sposób przeprowadzenia i cel (ang. *target*) może być (specyfikacja, na potrzeby przykładu, została ograniczona do punktu 1 poprzedniej listy, tj. uniemożliwienia przesyłania informacji):

a) atak fizyczny (zniszczenie) na linie przesyłowe (łącza),

b) atak fizyczny (modyfikacja) na linie przesyłowe,

c) atak fizyczny (zniszczenie) na sieciowe urządzenie nadawcze/odbiorcze,

d) atak fizyczny (modyfikacja) na sieciowe urządzenie nadawcze/odbiorcze,

e) atak logiczny (modyfikacja) na sieciowe urządzenie nadawcze/odbiorcze,

f) atak logiczny (DDoS, ang. *Distributed Denial of Services*) na serwery i inne przetwarzające informację urządzenia w sieci,

g) atak fizyczny (np. zniszczenie linii energetycznych, obiektów budowlanych, urządzeń zapasowych) na infrastrukturę zasilającą urządzenia sieciowe.

Każdy z wymienionych ataków może mieć wiele „wariantów wykonawczych", np. dla c) może to być:

– bezpośredni atak terrorystyczny (nieuprawniona osoba dostała się do urządzeń i je zniszczyła);

– pośredni atak terrorystyczny, np. spowodowanie zalania i tym samym zniszczenia urządzeń, zniszczenie (np. wysadzenie) budynku, w którym znajdują się urządzenia itp.;

– zniszczenie urządzeń przez personel obsługujący na skutek sprowokowanego błędu obsługi (np. użycie odpowiednio spreparowanej instrukcji obsługi lub, ogólnie, działania socjotechniczne);

– zniszczenie urządzeń przez personel obsługujący, zmuszony np. porwaniem rodziny.

Do tego należałoby uwzględnić możliwość ataków złożonych oraz przeciążeniowych[12]. Łatwo zauważyć, analizując np. odpowiednie drzewo zagrożeń, że znaczącą rolę zaczyna odgrywać efekt skali, przejawiający się gwałtownym wzrostem liczby elementów, które, chcąc skutecznie atak zneutralizować, należałoby monitorować. Kłopot w tym, że takie monitorowanie wymaga:

1. wiedzy o zagrożeniach, podatnościach i możliwych scenariuszach realizacji zagrożeń oraz umiejętności analitycznych i technicznych;

2. operacyjnej współpracy w poziomych (a nie pionowych!) strukturach organizacyjnych raportowania, monitorowania i podejmowania decyzji z zakresu ochrony informacji (i ogólnie „bezpieczeństwa");

3. odpowiedniego wyposażenia narzędziowego.

Skuteczna współpraca operacyjna (punkt 2 listy) wymaga ukierunkowanego i szybkiego przepływu informacji. Można, jako pewnik, przyjąć, że wraz ze wzrostem liczby osób uwikłanych w taką współpracę, przepływ informacji i cykl decyzyjny będzie się wydłużał. Niestety, polskie prawo, również to aktualnie tworzone, nie przyczynia się do optymalizacji współpracy w ramach struktur z punktu 2 ww. listy.

Warto zwrócić także uwagę, że jeżeli weźmie się pod uwagę system informacyjny, w jego zakresie mieści się także oddziaływanie psychologiczne terrorystów poprzez treści umieszczane na stronach WWW i portalach

12 Np. wyłączenie, poprzez odpowiedni atak, z eksploatacji współpracujących urządzeń, być może słabiej chronionych, powoduje przeciążenie i, przynajmniej czasowe, wyłączenie działania tych urządzeń, które są głównym celem napastnika.

społecznościowych.

Podsumowanie

Uzasadnienie pesymistycznej prognozy, wyrażonej w tym artykule, można podsumować następująco:

1. Szerokie, w praktyce nie do skutecznego kontrolowania, pole ataku dla terrorystów.

2. „Poszatkowane", niespójne widzeniem problemu – spojrzenie przez pryzmat infrastruktury krytycznej państwa, „cyberprzestrzeni RP" (cokolwiek by to miało znaczyć), kategorii informacji (niejawne, dane osobowe, tajemnice prawnie chronione), rodzajów zabezpieczeń technicznych i fizycznych oraz zakresów kompetencji i odpowiedzialności urzędów i urzędników różnych. Daje to dobrą podstawę przesłankom z punktu 3 i 4.

3. Przerosty organizacyjne – jak uczy historia, w USA zorientowano się o tym dopiero po ataku na WTC, który udał się, pomimo dużej ilości różnych instytucji, agencji i ludzi dbających o „bezpieczeństwo" USA. W praktyce sprawdza się to, co jest proste. Do skutecznego przeciwdziałania potrzebna jest np. szybka reakcja, która w proponowanym systemie hierarchicznym[13] i w proponowanym cyklu oceny i zbierania danych[14] na pewno nie będzie miała miejsca.

4. Bałagan terminologiczny – mnożenie pojęć, szczególnie tych z przedrostkiem „cyber", przyczynia się tylko do powstania chaosu informacyjnego.

5. Brak wśród ludzi tworzących prawo znajomości technicznej strony problemu, np. wydaje im się, że Internet to jest coś, w czym można wytyczyć granice państwowe (stąd np. „cyberprzestrzeń RP"[15]) oraz powierzenie zarządzania bezpieczeństwem informacyjnym urzędnikom, a nie fachowcom.

Uważamy, że kolejność wymienionych pięciu przesłanek określa jednocześnie ich wagę dla problemu.

13 Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. z dn. 21.05.07).
14 Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. *w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego* (Dz. U. nr 83).
15 *Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016.* Wersja 1.1, Warszawa. Czerwiec 2010.

References

1. *Koncepcja strategiczna obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego, przyjęta przez szefów państw i rządów w Lizbonie*, Lizbona 19-20 listopada 2010 r.
2. Liderman K., *O zagrożeniach dla skutecznej ochrony informacji, przetwarzanej w sieciach i systemach teleinformatycznych, powodowanych nowomową*, Biuletyn IOZ. Nr 2, WAT, Warszawa 2011 (w druku).
3. Raport MSWiA o stanie bezpieczeństwa w Polsce w 2010 r.
4. *Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016*. Wersja 1.1. Warszawa. Czerwiec 2010.
5. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa. 2007 r.
6. *Strategy for Operating in Cyberspace*. USA Department Of Defense, Lipiec 2011 r.