Rafał Klimek

Demokracja czy bezpieczeństwo w sieci : aspekty społeczno-polityczne bezpieczeństwa informacyjnego w XXI wieku

Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa nr 4, 53-61

2012

Rafał KLIMEK
Wyższa Szkoła Bezpieczeństwa z siedzibą w Poznaniu

DEMOKRACJA CZY BEZPIECZEŃSTWO W SIECI. ASPEKTY SPOŁECZNO-POLITYCZNE BEZPIECZEŃSTWA INFORMACYJNEGO W XXI WIEKU

Bezpieczeństwo informacyjne stało się dziś jedną z najważniejszych, a według wielu opinii najważniejszą kategorią bezpieczeństwa narodowego oraz bezpieczeństwa dotyczącego poszczególnych: organizacji, przedsiębiorstw, administracji i wreszcie poszczególnych jednostek w społeczeństwie.

Świat ulegał w ostatnich kilkunastu latach dynamicznym, wręcz rewolucyjnym zmianom związanym z komunikacją. Upowszechnienie komputerów osobistych oraz wszelkiego rodzaju narzędzi komunikacyjnych przy jednoczesnym rozwijaniu sieci Internetu doprowadziło do sytuacji, gdzie nastąpić musiała zmiana dotychczasowych kanonów związanych z tworzeniem, przechowywaniem i rozpowszechnianiem informacji.

Ludzkość przebyła do lat dziewięćdziesiątych XX wieku[1] bardzo powolną, ewolucyjną drogę zmian w obszarze komunikacji. Przez stulecia wykorzystywano na potrzeby związane z administrowaniem danym terytorium, czy prowadzeniem wojen w zasadzie te same metody tworzenia i przekazywania informacji. W procesie tym uczestniczyły w zasadzie tylko nieliczne grupy najbardziej uprzywilejowanych społecznie obywateli, którzy potrafili pisać i czytać (czyli tworzyć i interpretować informacje) dostarczenie owych informacji odbywało się najczęściej przy pomocy gońców, którzy niejednokrotnie byli narażeni na różnego rodzaju niebezpieczeństwa czyhające na nich w drodze. Wiedza na temat działań suwerena nie mogła z przyczyn obiektywnych szybko i precyzyjnie docierać do obywateli, zatem ich uczestnictwo w życiu politycznym danego terytorium, czy też państwa musiało być znikome. Stopniowo wraz z epoką Oświecenia, a w szczególności za sprawą wynalezienia druku udział podmiotów zdolnych do wytwarzania i udostępniania informacji na szerszą skalę znacznie się poszerzył.

Kolejnym krokiem milowym w dziedzinie informacji stało się powszechne nauczenie oraz rozwój techniki, co jak Zasze związane było z prowadzeniem wojen. Telegraf i telefon choć dostępne przez długi czas jedynie nielicznym stały się kolejnym ważnym elementem rozwoju społeczeństwa w zakresie wytwarzania i przekazywania informacji. Każdy kolejny etap życia ludzkości miał prowadzić do stanu, w którym znajdujemy się dziś. Stanu, kiedy zdecydowana większość z nas potrafi samodzielnie wytwarzać i udostępniać wszystkim, w dowolnym czasie i z każdego miejsc na Ziemi różnego rodzaju informacje. Świat stał się przez to jakby mniejszy - wrosła partycypacja obywateli w życiu społeczno – politycznym, co można odebrać, jako pozytywny element na rzecz umacniania demokracji na świecie.

Ilość informacji, jaka codziennie powstaje jest ogromna, toteż coraz trudniej jest poszczególnym reżimom i organizacjom kontrolować globalną sieć informacyjną. Tempo rozwoju społeczeństwa informacyjnego jest niewspółmiernie wysokie do budowania świadomości wśród podmiotów odpowiedzialnych za

[1] Lata dziewięćdziesiąte XX wieku to moment dynamicznego, rewolucyjnego wręcz rozwoju Internetu.

wytwarzanie, przechowywanie i udostępnianie różnego rodzaju informacji. Taki stan rzeczy wiąże się z poważnymi zagrożeniami natury: politycznej, militarnej, i ekonomicznej. Dzisiejsze konflikty zbrojne oraz działania na płaszczyźnie finansowej są nierozerwalnie związane z systemami teleinformatycznymi. Świat biznesu i administracji w państwach wysokorozwiniętych, jak i rozwijających się opiera się dziś na szybkim przetwarzaniu informacji w oparciu o odpowiednią infrastrukturę techniczną, dlatego też tak istotna stała się dziś zmiana paradygmatu bezpieczeństwa państwa, podmiotów gospodarczych, jak i poszczególnych obywateli. Skoro większość dzisiejszego świata opiera się na globalnych zależnościach sieciowych, to stało się oczywiste, że priorytetem powinno stać się bezpieczeństwo informacyjne, toteż tradycyjny model budowania bezpieczeństwa państwa – przede wszystkim na sile obronnej i liczebności armii, stracił swoją aktualność. Czym było by dziś nowoczesne państwo bez systemu łączności? Czym byłaby armia bez możliwości korzystania z sytemu GPS, czy najnowszych urządzeń opartych na komputerach i sieci Internet?

Mając powyższe na uwadze, oczywista wydaje się konstatacja, że kluczowym elementem bezpieczeństwa współczesnego państwa, jak i współczesnych organizacji, powinna być odpowiednia polityka bezpieczeństwa informacji.

W literaturze związanej z bezpieczeństwem pojawia się wiele różnego rodzaju definicji tego pojęcia. W szerokiej interpretacji bezpieczeństwo informacyjne rozumiane jest jako stan wolny od zagrożeń, które definiowane są głównie jako:

- przekazywania informacji nieuprawnionym podmiotom;
- szpiegostwo;
- działalność dywersyjna lub sabotażowa.[2]

Bezpieczeństwem informacyjnym nazywa się także wszelkie działania, systemy oraz metody zmierzające do zabezpieczenia zasobów informacyjnych gromadzonych, przetwarzanych, przekazywanych, przechowywanych w pamięciach komputerów oraz w sieciach teleinformatycznych.[3] Bezpieczeństwo, w tym także bezpieczeństwo informacyjne jest zarówno podstawową wartością i potrzebą, jak i prawem każdego człowieka i każdej organizacji społecznej.[4] Globalizacja, szybkość przepływu danych, powszechność dostępu do informacji i totalny (wszechogarniający) charakter zasobów informacji zagrażający jednostkom ludzkim i organizacjom wywołuje konieczność zwiększenia bezpieczeństwa informacji, czyli prawnej i faktycznej ochrony informacji niejawnych i zastrzeżonych oraz danych osobowych.[5]

Bezpieczeństwo informacyjne bardzo często rozumiane jest przez praktyków jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania.[6]

Tworzenie różnego rodzaju aktów prawnych, elektronicznych i fizycznych zabezpieczeń chroniących nas przed włamaniem się osób niepożądanych do systemów elektronicznych, baz danych, serwerowni, jak i poszczególnych

---

[2] P. Bączek, *Zagrożenia informacyjne, a bezpieczeństwo państwa polskiego*. Toruń 2006, s. 71
[3] Ibidem
[4] L.F. Korzeniowski (w:) *Ochrona informacji niejawnych biznesowych i danych osobowych, materiały VII Kongresu Krajowego Stowarzyszenia Ochrony Informacji Niejawnych.* Katowice 2011, s. 59
[5] Ibidem
[6] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego.* Toruń 2006, s. 19

pomieszczeń instytucji, w których przechowywane są dane jest katalogiem działań, które nie gwarantują w 100% bezpieczeństwa informacji. Powyższą tezę udowadnia w swej znakomitej książce najsłynniejszy haker świata Kevin Mitnick. W oparciu o swoje niezwykle pasjonujące, bogate i wieloletnie doświadczenia życiowe w zakresie legalnego, jak również nielegalnego pozyskiwania rożnego rodzaju informacji zastrzeżonych dla osób niepowołanych – postawił on tezę, że najsłabszym ogniwem we wszystkich możliwych systemach bezpieczeństwa informacji jest człowiek. W związku z powyższym Mitnick proponuje, że celem ochrony informacji należy inwestować w podnoszenie świadomości społecznej w zakresie coraz częściej stosowanych przez podmioty nieuprawnione metod socjotechniczny, na które większość z nas jest bardzo podatna.

Do typowych metod socjotechnicznych pozwalających na zdobycie informacji chronionych zaliczył on wymienione poniżej.

- udawanie pracownika tej samej firmy;
- udawanie przedstawiciela dostawcy, firmy partnerskiej lub agencji rządowej;
- udawanie kogoś, kto ma władzę;
- udawanie nowego pracownika proszącego o pomoc;
- udawanie przedstawiciela producenta systemu operacyjnego zalecającego pilną aktualizację;
- oferowanie pomocy w razie wystąpienia jakiegoś problemu, sprawienie, by problem wystąpił, i manipulacja ofiarą w taki sposób, aby sama zadzwoniła z prośbą o pomoc;
- wysłanie darmowego programu do aktualizacji lub zainstalowania;
- wysłanie wirusa lub konia trojańskiego w załączniku do poczty;
- użycie fałszywego okna dialogowego wyświetlającego prośbę o powtórne załogowanie się lub wprowadzenie hasła;
- przechwytywanie naciśniętych klawiszy za pomocą specjalnego programu;
- podrzucenie w okolicach stanowiska pracy ofiary dyskietki lub płyty CD-ROM zawierającej niebezpieczny kod;
- używanie wewnętrznej terminologii i żargonu w celu zbudowania zaufania;
- oferowanie nagrody za rejestrację, poprzez wprowadzenie nazwy użytkownika i hasła na stronie internetowej;
- podrzucenie dokumentu lub pliku w pomieszczeniu poczty wewnętrznej firmy, aby dotarł do miejsca przeznaczenia jako korespondencja wewnętrzna;
- zmiana ustawień nagłówka w faksie tak, aby wydawał się pochodzić z wewnątrz;
- prośba do recepcjonistki o odebranie i przesłanie faksu dalej;
- prośba o transfer pliku do lokalizacji, która wydaje się wewnętrzna;
- ustawienie skrzynki poczty głosowej w taki sposób, że w trakcie oddzwaniania napastnik jest identyfikowany, jako osoba z wewnątrz;
- podawanie się za pracownika z innego oddziału i prośba o tymczasowe otwarcie konta e-mail.[7]

[7] K. Mitnick, W. Simon, *Sztuka Podstępu*. Gliwice 2011, s. 368-369

Najsłynniejszy haker świata podaje wiele sposobów, które poprawiają bezpieczeństwo informacji na poziomie społecznym (socjotechnicznym). Sugeruje on, że poza odpowiednim systemem szkoleń i tworzeniem polityk bezpieczeństwa informacji w państwie, czy też organizacji bardzo istotnym elementem powodzenia w obszarze bezpieczeństwa danych jest permanentne podtrzymywanie świadomości wśród zespołu osób mających wpływ pośredni lub bezpośredni na bezpieczeństwo informacyjne danego podmiotu. Program stałego podtrzymywania świadomości musi wykorzystywać wszelkie możliwości komunikowania o sprawach bezpieczeństwa, w taki sposób, żeby przekazywana treść była solidnie zapamiętywana i w pracownikach zostały wyrobione właściwe nawyki związane z tą kwestią.[8] Kevin Mitnick w tym celu proponuje następującą listę rozwiązań:

- zawarcie elementów informacyjnych w wewnętrznych publikacjach;
- firmy: artykułach, ramkach (krótkich w treści i przyciągających uwagę) lub np. komiksach;
- opublikowanie zdjęcia Mistrza Bezpieczeństwa na dany miesiąc;
- wieszanie plakatów w miejscach wykonywania pracy;
- przesyłanie uwag poprzez wewnętrzne fora firmy;
- dołączanie ulotek do kopert zawierających np. premię;
- wysyłanie przypominających e-maili;
- stosowanie wygaszaczy ekranu o tematyce związanej z bezpieczeństwem;
- zostawianie komunikatów w skrzynkach poczty głosowej pracowników;
- wydrukowanie nalepek na telefony z napisami typu: „Czy Twój rozmówca jest na pewno tym, za kogo się podaje?”;
- wprowadzenie komunikatów przypominających, pojawiających się na komputerze podczas logowania do systemu, np. „Jeżeli wysyłasz poufną informację poprzez e-mail, koniecznie ją zaszyfruj!”;
- uwzględnienie świadomości bezpieczeństwa jako standardowego elementu składającego się na ocenę pracownika;
- umieszczenie elementów „przypominających” o zasadach bezpieczeństwa w intranecie, np. za pomocą kreskówek, humorystycznych obrazków lub w inny skłaniający do zainteresowania się nimi;
- korzystanie z elektronicznych wyświetlaczy np. w stołówce lub w firmowym bufecie, które od czasu do czasu prezentują komunikaty dotyczące bezpieczeństwa;
- dystrybucja broszur;
- inne pomysłowe chwyty, np. darmowe ciasteczka szczęścia zawierające zamiast wróżby którąś z zasad bezpieczeństwa.

Dążenie do uregulowania od strony przepisów prawa, jak i, co za tym idzie stworzenie i wyposażenie w odpowiednie kompetencje organów i służb administracji publicznej, które mają być odpowiedzialne za nadzór i kontrolę szeroko rozumianej polityki bezpieczeństwa – jest odpowiedzią państw wysokorozwiniętych i rozwijających się na coraz większe zagrożenia związane z: wytwarzaniem, przechowywaniem, przesyłaniem i kopiowaniem szeroko rozumianych wartości niematerialnych i prawnych.

[8] Ibidem, s. 288

W Polsce kwestię bezpieczeństwa informacyjnego państwa regulują między innymi następujące akty prawne:

- Ustawa o ochronie informacji niejawnych, (Dz.U. 2010 nr 182 poz. 1228.);
- Ustawa z 29 sierpnia 1997r .O ochronie danych osobowych (Dz.U. Nr 133, poz. 883 z późn. zm.);
- Ustawa z 16 kwietnia 1993r. O zwalczaniu nieuczciwej konkurencji (Dz.U., Nr 47, poz.211 z póź. zm.);
- Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553, z późn. zm.);
- Ustawa z 29 sierpnia 1997r. Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665, z późn. zm.1).

Kwestie bezpieczeństwa społeczeństwa informacyjnego uwzględniono również w dokumencie pod nazwą Strategia Rozwoju Społeczeństwa Informacyjnego. Misja społeczeństwa informacyjnego w Polsce została zdefiniowana następująco: *Umożliwienie społeczeństwu powszechnego i efektywnego wykorzystania wiedzy i informacji do harmonijnego rozwoju w wymiarze społecznym, ekonomicznym i osobistym.*[9]

Jednocześnie przyjęto, że rozwojowi społeczeństwa informacyjnego w Polsce powinny trwale towarzyszyć:

- **dostępność, bezpieczeństwo i zaufanie** – możliwość uzyskania dostępu do rzetelnej informacji lub bezpiecznej usługi niezbędnej obywatelowi oraz przedsiębiorcy,
- **otwartość i różnorodność** – brak dyskryminacji w dostępie do informacji, a w szczególności do informacji publicznej,
- **powszechność i akceptowalność** – dążenie, aby udział w dobrach społeczeństwa informacyjnego był oczywisty i jak najszerszy, a także by oferta produktów i usług społeczeństwa informacyjnego była maksymalnie szeroka,
- **komunikacyjność i interoperacyjność** – zapewnienie dotarcia do pożądanej informacji w sposób bezpieczny, szybki, prosty i niezależny od zastosowanej technologii.[10]

W ramach obszaru strategicznego CZŁOWIEK, wyszczególnione zostały następujące cele:

► **Cel 1:** Podniesienie poziomu motywacji, świadomości, wiedzy oraz umiejętności w zakresie wykorzystywania technologii informacyjnych i komunikacyjnych. *Miarą osiągnięcia celu jest wzrost umiejętności korzystania z narzędzi teleinformatycznych (mierzona umiejętnością wykonania 5-6 podstawowych czynności wymienianych przez Eurostat).*

► **Cel 2:** Podniesienie poziomu i dostępności edukacji (od przedszkola do uczelni wyższej) oraz upowszechnienie zasady nauki przez całe życie poprzez wykorzystanie technologii informacyjnych i komunikacyjnych *Miarą osiągnięcia celu jest wzrost procentowego udziału osób w wieku 25-64 uczących się i dokształcających w ogólnej liczbie ludności w tym wieku.*

[9] *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013 (streszczenie),* Ministerstwo Spraw Wewnętrznych i Administracji, grudzień 2008, s. 1

[10] Ibidem

► **Cel 3:** Dopasowanie oferty edukacyjnej do wymagań rynku pracy, którego istotnym elementem są technologie informacyjne i komunikacyjne. *Miarą osiągnięcia celu jest wzrost poziomu dopasowania polskiego systemu edukacji do potrzeb globalnie konkurencyjnej gospodarki.*[11]

Bezpieczeństwo informacyjne znalazło także miejsce w Strategii Bezpieczeństwa Narodowego Rzeczpospolitej. Należy tworzyć i rozwijać długofalowe plany ochrony kluczowych systemów teleinformatycznych przed uzyskiwaniem dostępu do danych przez podmioty do tego niepowołane, zakłócaniem normalnego ich funkcjonowania, kradzieżą tożsamości i sabotażem.[12] Trzeba stale oceniać możliwości wtargnięcia do systemów teleinformatycznych, przygotować możliwe formy odpowiedzi na ataki oraz rozwijać metody ewaluacji poniesionych strat informacyjnych. Priorytetem państwa będzie wspieranie narodowych programów i technologii informacyjnych.

Współczesne systemy prawno-polityczne państwa nie nadążają często za dynamicznymi zmianami dokonującymi się w społeczeństwach, toteż istnieje wiele luk prawnych, które w doskonały sposób wykorzystują w celach ideologicznych i czysto ekonomicznych specjaliści z branży informatycznej.

Jednym z najgłośniejszych przykładów ostatnich lata jest sprawa pewnego Niemca - Kima Dotcoma,[13] twórcy portalu ,,Magaupload", który dzięki swemu talentowi i sprytowi zarabiał miliony dolarów na udostępnianiu użytkownikom z całego świata treści w postaci różnego rodzaju plików elektronicznych, które nigdy nie były jego własnością i do których nie posiadał żadnych praw. Serwis ,,Megaupload", który stworzył, w krótkim czasie przyniósł mu milionowe zyski. Poza podejrzeniami o łamanie praw autorskich Departament Sprawiedliwości USA oskarżył Dotcoma o „gangsterstwo" oraz „spiskowanie w celu prania pieniędzy".[14] Dzięki zarzutom kryminalnym władze amerykańskie mogły złożyć wniosek o ekstradycję szefa serwisu internetowego Megaupload – w USA grozi mu 55 lat więzienia – na co nie pozwoliłby pozew cywilny.[15] Jednak mimo upływu roku Amerykanie wciąż nie potrafią poprzeć swoich oskarżeń żadnymi dowodami. Prawo nie nadąża za rewolucją teleinformatyczną, o czym osoby takiej, jak Kim Dotcom doskonale wiedzą i dlatego tak trudno jest w dzisiejszym świecie walczyć z piractwem komputerowym oraz innego typu przestępczością sieciową.[16]

Wiele emocji wywołała także sprawa WikiLeaks, portalu, którego twórca Julian Assange postanowił zgodnie ze swoimi poglądami udostępniać całemu światu bezpłatnie najbardziej strzeżone przez poszczególne państwa (w tym wiodące mocarstwa światowe) informacje wywiadowcze i depesze dyplomatyczne. Portal WikiLeaks w 2010 roku opublikował poufne raporty wojsk USA w Iraku i Afganistanie, a także ok. 250 tys. amerykańskich depesz dyplomatycznych.[17] Przypadek WikiLeaks wywołał na świecie dyskusję. Pojawiło się podstawowe

[11] *Strategia rozwoju społeczeństwa*…, op. cit., 2
[12] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej.* Warszawa 2007, s. 20
[13] Jego prawdziwe imię i nazwisko brzmi Kim Schmitz.
[14] M. Herma, *Zemsta króla piratów,* „Polityka" z 01.01.2013, s. 25
[15] Ibidem
[16] Więcej pod adresem *http://www.polityka.pl/spoleczenstwo/artykuly/1534033,2,kim-dotcom-wraca-do-sieci.read#ixzz2JFp8mrjp*
[17] *Powstała fundacja wolności prasy. Będzie finansować WikiLeaks*, Rzeczpospolita z 17.12.2012. *http://www.rp.pl/artykul/236296,962350-Powstala-fundacja-wolnosci-prasy--Bedzie-finansowac-WikiLeaks.html*

pytanie – czy istnieje granica między prawem jednostek w demokratycznym państwie do wiedzy na temat wszystkich, nawet najbardziej strzeżonych jego tajemnic, a bezpieczeństwem tego państwa jak i jego obywateli?

Dziś świat Internetu sprawia, że żyjemy w epoce indywidualizmu sieciowego. Sieciowy indywidualista to człowiek skoncentrowany na swoim prywatnym życiu i jednocześnie prowadzący bardzo aktywne życie społeczne, tyle tylko, że nie potrzebuje on do tej aktywności pośrednictwa tradycyjnych organizacji społecznych, partii politycznych, czy instytucji kultury – wystarczy mu sieć.[18] Polityka bezpieczeństwa informacji dąży do coraz większego kontrolowania zasobów sieci, jak również użytkowników z nich korzystających w sposób niezgodny z prawem – w tym miejscu rodzi się sprzeczność interesów. Państwo i różnego rodzaju organizacje, a także wiele osób fizycznych wytwarzających i upowszechniających informacje chce mieć kontrolę nad procesami sieciowymi. Z drugiej strony dynamiczne zmiany społeczne zachodzące w społeczeństwach w dużej mierze wpływają na internautów, którzy często oczekują pełnego dostępu do informacji, argumentując to demokracją i społeczeństwem obywatelskim.

W ostatnim czasie bardzo głośna stała się sprawa młodego amerykańskiego hakera Aarona Swartza, który w 2010 roku włamał się do bazy prac naukowych MIT (Massachusetts Institute of Technology) i skopiował kilka tysięcy z nich. Chociaż uczelnia nie złożyła oskarżenia przeciwko niemu, to sprawa skończyła się oskarżeniem na wniosek FBI. Wcześniej Swartz miał na swoim koncie wyrok za inne przestępstwo komputerowe, co ostatecznie spowodowało, że w perspektywie pojawiła się dla niego groźba, że spędzi on nawet 30 lat swego życia w celi. Wizja tak długiego pozbawienia wolności w połączeniu z depresją na którą cierpiał, doprowadziły do tego, że Aaron Swartz w styczniu 2013 roku popełnił samobójstwo. Sprawa stała się przyczynkiem do ogólnoświatową dyskusji na temat bezwzględnego karania za przestępstwa komputerowe ludzi, którzy złamali prawo nie dla własnego zysku, ale dla idei demokratycznych. Powoływano się na przykłady, że za najcięższe przestępstwa, takie, jak: gwałty, rozboje i zabójstwa w USA orzekane są łagodniejsze kary niż za kradzież danych, co wiele środowisk lewicowych uznało za wysoce niesprawiedliwe.

Z prowadzonych nad bezpieczeństwem informacyjnym badań wynika, że istnieje sposób na odnalezienie równowagi pomiędzy liberalną i realistyczną koncepcją bezpieczeństwa. Należy w tym celu prowadzić działania zmierzające do tworzenia globalnych instytucji i porozumień przeciwko działaniom wojennym, a jednocześnie dbać o ciągłą świadomość własnych słabości i zwiększanie poziomu ochrony systemów informacyjnych.[19]

Zgodnie z najnowszymi badaniami World Internet Project Poland 2012, wśród Polaków do 29 roku życia Internet stał się najważniejszym medium, detronizują telewizję, rządzącą ciągle w starszych pokoleniach.[20]

Młode pokolenie tworzy w sieci swoją przestrzeń autonomii, miejsce które od czasu do czasu powoduje, że rodzi się aktywny protest, rodzaj antysystemowego buntu przeciw ograniczeniom tej autonomii. Tak jak zmieniają się dzisiejsze społeczeństwa, tak powinna zmieniać się polityka państwa w zakresie

[18] E. Bendyk, *Oburzeni wszystkich krajów łączcie się,* „Polityka" z 12.12.2012, s. 78
[19] K. Liedl, *Bezpieczeństwo informacyjne*…, op. cit., s. 21
[20] E. Bendyk, *Oburzeni wszystkich*…, op. cit., s. 78

bezpieczeństwa informacyjnego. Wydaje się, że proces liberalizacji przepisów w tej dziedzinie nie jest jedynie pieśnią dalekiej przyszłości, gdyż pokolenia dzisiejszych dwudziestolatków będą z czasem mieć coraz większy wpływ na politykę, a przez to na otaczający nas świat.

Nie sposób prowadzić i wygrywać wojnę[21] bez wcześniejszego określenia na forum społeczeństwa jej celów oraz bez uświadomienia o tych celach (jak i skutkach realizacji owych celów) zainteresowanych obywateli. Rozsądni politycy powinni pamiętać o ponadczasowych słowach pruskiego stratega Karla von Clausewitza: ,,Żołnierz, choćby najbardziej mężny, sprawny i oddany ojczyźnie, jest tylko jednym z elementów pewnej triady, aby nasze przedsięwzięcia mogły zakończyć się powodzeniem, wszystkie trzy elementy, czyli: wojsko, rząd i społeczeństwo, muszą działać razem.[22] Państwo i korporacje transnarodowe powinny dostrzegać zmieniającą się rzeczywistość społeczną – obywatele muszą w sposób szczególnie odpowiedzialny korzystać z praw i przywilejów wynikających z reguł społeczeństwa demokratycznego. Z drugiej jednak strony wielkim wyzwaniem pozostaje znalezienie złotego środka pomiędzy bezpieczeństwem państwa i jego obywateli, a wolnością jednostek w sieci. Tak, czy inaczej punktem wyjścia do osiągnięcia konsensusu powinien być wielostronny, otwarty dialog oraz budowanie świadomości po wszystkich stronach.

Streszczenie

Na przestrzeni ostatnich kilkunastu lat mamy do czynienia ogólnoświatową dynamiką rozwoju społeczeństwa informacyjnego. Informacja stała się dziś dostępna dla bardzo dużej rzeszy obywateli, podczas gdy przez wieki była często zastrzeżona tylko dla wybranych podmiotów sprawujących władzę. Sytuacja ta ma wiele zalet, natomiast posiada ona także jedną zasadniczą wadę, którą jest zwiększające się (proporcjonalnie do ilości użytkowników informacji) zagrożenie związane z nieuprawnionym i szkodliwym pozyskiwaniem i udostępnianiem informacji przez różnego rodzaju podmioty do tego nieuprawnione.

W związku z powyższym jesteśmy świadkami zmiany dotychczasowego paradygmatu postrzegania bezpieczeństwa. Nowoczesne organizacje, podmioty gospodarcze, a przede wszystkim państwa i ich armie stoją obecnie przed nowym, niezwykle ważnym wyzwaniem, jakim jest stworzenie efektywnego systemu bezpieczeństwa informacyjnego. Niniejszy artykuł ma na celu przybliżenie konkretnych przykładów naruszenia bezpieczeństwa informacji we współczesnym świecie oraz zwrócenie uwagi na fakt, że współczesne regulacje prawne nie nadążają za zmianami wywołanymi przez ogólnoświatową rewolucję teleinformatyczną. Bezpieczeństwo informacyjne staje się bardzo szybko jednym z najistotniejszych elementów większości systemów bezpieczeństwa, dlatego też należy traktować je zdecydowanie priorytetowo.

Summary

In the past few years, we have seen the worldwide dynamic development of information society. Information has become available to a large number of citizens while it was reserved for the chosen authorities over the centuries. This situation

[21] Także wojnę informacyjną w zakresie bezpieczeństwa informacyjnego państwa, czy organizacji.
[22] H. Strachan, *Carl Von Clausewitz O wojnie. Biografia*. Warszawa 2009, s. 8

has many advantages, yet it also has one significant disadvantage. And this would be the increasing (in proportion to the number of information users) danger relating to unauthorized and harmful gaining and sharing information by numerous subjects.

Therefore, we have seen changes in the previous paradigm of perceiving security. Modern organizations, companies and most of all countries and their armies face new and very important challenge, that is to create an efficient information security system. The purpose of this article is to give definite examples of violating information security in modern world and to pay attention to the fact that modern laws and regulations do not follow changes caused by the worldwide ICT revolution. Information security has become one of the most significant elements of most security systems, thus it should be given priority.

Bibliografia

1. Bączek P., *Zagrożenia informacyjne, a bezpieczeństwo państwa polskiego*. Toruń 2006
2. Bendyk E.*, Oburzeni wszystkich krajów łączcie się,* „Polityka" z 12.12.2012
3. Herma M., *Zemsta króla piratów,* „Polityka" z 01.01.2013
4. Korzeniowski L.F., *Ochrona informacji niejawnych biznesowych i danych osobowych materiały VII Kongresu Krajowego Stowarzyszenia Ochrony Informacji Niejawnych.* Katowice 2011
5. Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego.* Toruń 2006
6. Mitnick K., Simon W., *Sztuka Podstępu.* Gliwice 2011
7. *Powstała fundacja wolności prasy. Będzie finansować WikiLeaks*, Rzeczpospolita z 17.12.2012 r. *http://www.rp.pl/artykul/236296,962350-Powstala-fundacja-wolnosci-prasy--Bedzie-finansowac-WikiLeaks.html*
8. Strachan H., *Carl Von Clausewitz O wojnie. Biografia*. Warszawa 2009
9. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*. Warszawa 2007
10. *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013* (streszczenie), Ministerstwo Spraw Wewnętrznych i Administracji, grudzień 2008
11. Ustawa o ochronie informacji niejawnych, (Dz.U. 2010 nr 182 poz. 1228.)
12. Ustawa z 16 kwietnia 1993r. O zwalczaniu nieuczciwej konkurencji (Dz.U., Nr 47, poz.211 z póź. zm.)
13. Ustawa z 29 sierpnia 1997r .O ochronie danych osobowych (Dz.U. Nr 133, poz. 883 z późn. zm.)
14. Ustawa z 29 sierpnia 1997r. Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665, z późn. zm.1)
15. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553, z późn. zm.)