Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011

Założenia

Warszawa, marzec 2009

Spis treści

1. Wprowadzenie

W obliczu globalizacji walka z terroryzmem stała się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa każdego państwa. W czasie, gdy terroryści działają ponad granicami państw, a w Europie panuje swoboda przepływu osób, towarów, informacji i kapitału - bezpieczeństwo demokratycznego państwa zależy od wypracowania mechanizmów pozwalających skutecznie zapobiegać i zwalczać akty terroryzmu.

Rada Europejska w przyjętej w 2003 roku *Europejskiej Strategii Bezpieczeństwa* uznała zjawisko terroryzmu za podstawowe zagrożenie dla interesów UE. Ostatnim efektem prac w zakresie przeciwdziałania aktom terroru jest specjalny program *"Zapobieganie, gotowość i zarządzanie skutkami aktów terroryzmu"* przyjęty w ramach programu ogólnego *"Bezpieczeństwo i ochrona wolności" na lata 2007-2013.* Polska jest również stroną międzynarodowych i europejskich porozumień w sprawie zwalczania terroryzmu (jest sygnatariuszem *Europejskiej Konwencji o zwalczaniu terroryzmu* - Dz. U. z 1996 r. Nr 117, poz. 557) oraz ratyfikowała *Konwencję Rady Europy o zapobieganiu terroryzmowi,* sporządzoną w Warszawie dnia 16 maja 2005 r.

Cyberterroryzm, czyli terroryzm wymierzony przeciwko newralgicznym dla państwa systemom, sieciom i usługom teleinformatycznym, stanowi kluczową i stale rosnącą postać ataków terrorystycznych.

W niniejszym dokumencie c*yberprzestrzeń* rozumiana jest jako przestrzeń komunikacyjna tworzona przez system powiązań internetowych. Jako *cyberprzestrzeń państwa* przyjmuje się przestrzeń komunikacyjną tworzoną przez system wszystkich powiązań internetowych znajdujących się w obrębie państwa. Cyberprzestrzeń państwa w przypadku Polski określana jest również mianem *cyberprzestrzeni RP*.

Cyberprzestrzeń RP obejmuje między innymi systemy, sieci i usługi teleinformatyczne o szczególnie ważnym znaczeniu dla bezpieczeństwa wewnętrznego państwa, system bankowy, a także systemy zapewniające funkcjonowanie w kraju transportu, łączności, infrastruktury energetycznej, wodociągowej i gazowej oraz systemy informatyczne ochrony zdrowia, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne.

Systemy i sieci teleinformatyczne eksploatowane przez administrację rządową, organy władzy ustawodawczej, władzy sądowniczej, samorządu terytorialnego, a także strategiczne z punktu widzenia bezpieczeństwa państwa podmioty gospodarcze (np. podmioty działające w obszarze telekomunikacji, energii, gazu, bankowości, a także podmioty o szczególnym znaczeniu dla obronności i bezpieczeństwa państwa oraz podmioty działające w obszarze ochrony zdrowia) stanowią zasoby krytycznej infrastruktury teleinformatycznej państwa.

Z uwagi na wzrost zagrożeń ze strony sieci publicznych, od których całkowita separacja jest niemożliwa, a także fakt rozproszonej odpowiedzialności za bezpieczeństwo teleinformatyczne, niezbędne jest skoordynowanie działań w zakresie zapobiegania i zwalczania cyberterroryzmu, które umożliwią szybkie i efektywne reagowanie na zagrożenia i ataki wymierzone przeciwko krytycznym systemom i sieciom teleinformatycznym.

Przedmiotem niniejszego *Rządowego programu ochrony cyberprzestrzeni RP na lata 2009-2011*, zwanego dalej *Programem* - są propozycje działań o charakterze prawno-organizacyjnym, technicznym i edukacyjnym, których celem jest zwiększenie zdolności

do zapobiegania i zwalczania cyberterroryzmu oraz innych pochodzących z publicznych sieci teleinformatycznych zagrożeń dla państwa.

1.1 Cele *Programu*

Celem strategicznym Programu jest wzrost poziomu bezpieczeństwa cyberprzestrzeni państwa.

Osiągnięcie celu strategicznego wymaga stworzenia ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy podmiotami administracji publicznej oraz innymi podmiotami, których zasoby stanowią krytyczną infrastrukturę teleinformatyczną kraju, na wypadek ataków terrorystycznych wykorzystujących publiczne sieci teleinformatyczne.

Lista szczegółowych celów Programu przedstawia się następująco:

a) zwiększenie poziomu bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa skutkujące zwiększeniem poziomu odporności państwa na ataki cyberterrorystyczne,

b) stworzenie i realizacja spójnej dla wszystkich zaangażowanych podmiotów administracji publicznej oraz innych współstanowiących krytyczną infrastrukturę teleinformatyczną państwa polityki dotyczącej bezpieczeństwa cyberprzestrzeni,

c) zmniejszenie skutków ataków cyberterrorystycznych, a przez to kosztów usuwania ich następstw,

d) stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy publicznymi i prywatnymi podmiotami odpowiedzialnymi za zapewnianie bezpieczeństwa cyberprzestrzeni państwa oraz władającymi zasobami stanowiącymi krytyczną infrastrukturę teleinformatyczną państwa,

e) zwiększenie kompetencji odnośnie bezpieczeństwa cyberprzestrzeni podmiotów zaangażowanych w ochronę krytycznej infrastruktury teleinformatycznej państwa oraz innych systemów i sieci administracji publicznej,

f) zwiększenie świadomości użytkowników (w tym obywateli) systemów dostępnych elektronicznie i sieci teleinformatycznych w zakresie metod i środków bezpieczeństwa.

Cele Programu będą realizowane poprzez:

a) stworzenie systemu koordynacji zwalczania, przeciwdziałania i reagowania na zagrożenia i ataki na cyberprzestrzeń państwa, w tym ataki o charakterze cyberterrorystycznym, oraz poprzez inne działania organizacyjno-prawne przedstawione w rozdziale 2,

b) powszechne wdrożenie wśród jednostek administracji mechanizmów służących zapobieganiu i wczesnemu wykrywaniu zagrożeń teleinformatycznych oraz poprzez inne działania techniczne przedstawione w rozdziale 3,

c) edukację społeczną i specjalistyczną w zakresie bezpieczeństwa teleinformatycznego, a także poprzez inne działania przedstawione w rozdziale 4.

1.2 Założenia Programu

Założenia *Programu* zdefiniowane zostały poprzez przedstawienie adresatów i realizatorów *Programu*, przytoczenie powiązanych aktów prawnych i ustalenie ram

czasowych dla realizacji *Programu*.

Adresaci *Programu*

Ze względu na charakter programu, którego istotą jest zapobieganie, wykrywanie i łagodzenie skutków zjawisk i zdarzeń dotyczących ograniczenia dostępności systemów teleinformatycznych, z których część ma umożliwiać komunikację obywatel-państwo oraz przedsiębiorca-państwo, adresatami programu są praktycznie wszyscy obywatele RP. Ze względu na charakter i istotę celów *Programu* należy wyróżnić dwie grupy adresatów:

1. administrację publiczną i inne podmioty zarządzające zasobami krytycznej infrastruktury teleinformatycznej państwa,
2. beneficjentów systemów, sieci i usług teleinformatycznych stanowiących krytyczną infrastrukturę teleinformatyczną państwa.

Realizatorzy *Programu*

Realizacja *Programu* wymaga zaangażowania i współpracy wielu resortów i instytucji kontrolowanych przez państwo. Z uwagi na cel i przedmiot *Programu*, realizacja zadań oraz osiągnięcie zakładanych skutków wymagać będzie również stworzenia mechanizmów zaangażowania i współpracy podmiotów pozostających poza administracją publiczną, w szczególności przedsiębiorstw zarządzających krytyczną infrastrukturą teleinformatyczną.

Realizatorami programu będą podmioty odpowiedzialne za ochronę infrastruktury krytycznej kraju, w tym przede wszystkim krytycznej infrastruktury teleinformatycznej. Z tego względu wiodące role w realizacji programu odgrywać będą: Ministerstwo Spraw Wewnętrznych i Administracji (MSWiA) jako podmiot odpowiedzialny za informatyzację państwa oraz infrastrukturę krytyczną oraz Agencja Bezpieczeństwa Wewnętrznego (ABW) jako podmiot odpowiedzialny za bezpieczeństwo wewnętrzne państwa.

Ponieważ jedynie nieznaczna część infrastruktury krytycznej, w tym teleinformatycznej, jest własnością państwa, natomiast większość zasobów stanowi własność prywatną, dużą rolę w realizacji programu powinny mieć te podmioty prywatne, które są właścicielami zasobów stanowiących infrastrukturę państwa.

Podsumowując, jako realizatorów programu przyjmuje się:

a) Ministerstwo Spraw Wewnętrznych i Administracji,
b) Agencję Bezpieczeństwa Wewnętrznego,
c) Ministerstwo Obrony Narodowej,
d) Służbę Kontrwywiadu Wojskowego,
e) inne organy administracji publicznej,
f) podmioty prywatne - właścicieli zasobów stanowiących krytyczną infrastrukturę teleinformatyczną państwa.

Koordynacja wdrożenia *Programu*

Podmiotem koordynującym wdrożenie Programu będzie Minister Spraw Wewnętrznych i Administracji, a za realizację programu odpowiadać będą: Minister Spraw Wewnętrznych i Administracji, Minister Obrony Narodowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Służby Kontrwywiadu Wojskowego i inne organy

administracji publicznej zgodnie z właściwością działania.

Kontekst prawny

Podstawowymi w obszarze bezpieczeństwa zasobów teleinformatycznych są następujące akty prawne:

- Konstytucja Rzeczypospolitej Polskiej z dn. 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz.483, z późn. zm.),
- Ustawa z dn. 6 czerwca 1997 r. Kodeks karny (Dz.U. z 1997, Nr 88, poz. 53 z późn. zm),
- Ustawa z dn. 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz.1800 z późn. zm.),
- Ustawa z dn. 24 marca 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (Dz.U. z 2002 r. Nr 74, poz. 676 z późn. zm.),
- Ustawa z dn. 6 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego (Dz.U. z 2006 r. Nr 104, poz. 709 z późn. zm.),
- Ustawa z dn. 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590),
- Ustawa z dn. 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm.),
- Ustawa z dn. 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. z 2005 r. Nr 196, poz.1631 z późn. zm.),
- Rozporządzenie Prezesa Rady Ministrów z dn. 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. z 2005 r. Nr 171, poz. 1433),
- Rozporządzenie Rady Ministrów z dn. 28 marca 2005 r. w sprawie Planu Informatyzacji Państwa na lata 2007-2010 (Dz.U. z 2007 Nr 61, poz. 415),
- Rozporządzenie Rady Ministrów z dn. 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2005 r. Nr 212, poz. 1766),
- Decyzja Ministra Obrony Narodowej nr 357/MON z dnia 29 lipca 2008 roku w sprawie organizacji systemu reagowania na incydenty komputerowe w resorcie obrony narodowej.

Należy podkreślić, iż obowiązujące regulacje prawne dotyczące zasobów teleinformatycznych mają głównie charakter branżowy regulujący poszczególne aspekty związane z funkcjonowaniem zasobów. Z tego powodu powyższy wykaz aktów prawnych nie ma charakteru wyczerpującego. Przepisy prawne mające znaczenie dla funkcjonowania zasobów teleinformatycznych istnieją również w innych dziedzinach prawa, np. przepisach o ochronie danych osobowych, prawie bankowym, itd.

Należy również zaznaczyć, iż Polska jest stroną konwencji międzynarodowych, które również mają znaczenie dla bezpieczeństwa teleinformatycznego. Na potrzeby niniejszego dokumentu należy wymienić w szczególności:

- Konwencję Rady Europy o zwalczaniu terroryzmu z dn. 27 stycznia 1977 r. (Dz.U. z 1996 r. Nr 117, poz. 557) i

- Konwencję Rady Europy o zapobieganiu terroryzmowi z dn. 16 maja 2005 r. (Dz.U. z 2007 r. Nr 191, poz.1364).

Ponadto Polska podpisała Konwencję Rady Europy o cyberprzestępczości z dn. 23 listopada 2001 r., którą ratyfikuje w roku 2009.

Ramy czasowe

Przyjmuje się, że zawarte w dokumencie cele zostaną osiągnięte w latach 2009-2011. Należy jednak zaznaczyć, że bezpieczeństwo powinno być pojmowane jako proces a nie stan. Zmieniające się w czasie uwarunkowania wymagają ciągłej dbałości o właściwą adaptację wdrożonych rozwiązań.

Niniejszy program przedstawia działania niezbędne do ustanowienia ładu prawnego i organizacyjnego, umożliwiającego wdrożenie mechanizmów ochrony cyberprzestrzeni RP i to dla tych działań przewiduje się podane ramy czasowe. Natomiast sam proces ochrony zasobów teleinformatycznych powinien być traktowany jako proces ciągły, niezmiennie istotny z punktu widzenia funkcjonowania państwa i przez to nieograniczany żadną datą zakończenia programu.

2. Działania organizacyjno-prawne

Działania organizacyjno-prawne powinny obejmować między innymi:

a) prawne zdefiniowanie pojęć dotyczących cyberprzestępczości i cyberterroryzmu,

b) prawne uregulowanie zasad ochrony krytycznej infrastruktury teleinformatycznej,w odniesieniu do celów zdefiniowanych w 2.5 niniejszego opracowania,

c) ustalenie odpowiedzialności za ochronę cyberprzestrzeni RP i krytycznej infrastruktury teleinformatycznej,

d) ustalenie metod i zakresu współpracy z podmiotami prywatnymi posiadającymi elementy krytycznej infrastruktury teleinformatycznej państwa,

e) stworzenie sektorowych punktów kontaktowych oraz ustalenie sposobów i form współpracy,

f) stworzenie podstaw prawnych umożliwiających skuteczne realizowanie zadań na rzecz ochrony cyberprzestrzeni przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL,

g) zdefiniowanie roli kierowników i administratorów w jednostkach posiadających elementy krytycznej infrastruktury teleinformatycznej,

h) zdefiniowanie zakresu wymaganej współpracy jednostek posiadających fragmenty krytycznej infrastruktury teleinformatycznej z instytucjami odpowiedzialnymi za ochronę cyberprzestrzeni państwa,

i) wyznaczenie priorytetów i podjęcie działań w zakresie współpracy krajowej i międzynarodowej odnośnie ochrony cyberprzestrzeni,

j) zapewnienie spójności polityk bezpieczeństwa jednostek administracji publicznej posiadających elementy krytycznej infrastruktury teleinformatycznej,

k) kontynuowanie i uruchomienie programów badawczych dotyczących ochrony cyberprzestrzeni.

2.1 Cyberprzestępstwa a kodeks karny

Na określenie przestępstw związanych z funkcjonowaniem systemów i sieci teleinformatycznych w doktrynie prawa, literaturze fachowej i języku potocznym przyjęte zostały pojęcia „cyberprzestępstwo", „przestępstwo komputerowe" lub „przestępstwo internetowe". Do przestępstw powyższych typów zaliczane są m. in. hacking, fałszerstwo, sabotaż lub piractwo komputerowe, przestępstwa związane z kartami magnetycznymi, pornografia dziecięca i inne. W kodeksie karnym zagadnienie ścigania przestępstw komputerowych zawarte jest w rozdziałach:

a) Przestępstwa przeciwko Rzeczypospolitej Polskiej (Rozdział XVII),

b) Przestępstwa przeciwko bezpieczeństwu powszechnemu (Rozdział XX),

c) Przestępstwa przeciwko ochronie informacji (Rozdział XXXIII),

d) Przestępstwa przeciwko wiarygodności dokumentów (Rozdział XXXIV),

e) Przestępstwa przeciwko mieniu (Rozdział XXXV).

Wśród grupy artykułów kodeksu karnego dotyczących przestępstw komputerowych najistotniejsze z punktu widzenia ochrony cyberprzestrzeni państwa są następujące:

Art. 165 § 1 pkt 3 i 4 kk przewidujący odpowiedzialność karną za sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach:

a) powodując uszkodzenie lub unieruchomienie urządzenia użyteczności publicznej, w szczególności urządzenia dostarczającego wodę, światło, ciepło, gaz, energię albo urządzenia zabezpieczającego przed nastąpieniem niebezpieczeństwa powszechnego lub służącego do jego uchylenia,

b) zakłócając, uniemożliwiając lub w inny sposób wpływając na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych,

Art. 269 kk przewidujący odpowiedzialność karną za:

a) niszczenie, uszkadzanie, usuwanie lub zmienianie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych;

b) nie będąc do tego uprawnionym, zakłócanie pracy systemu komputerowego lub sieci teleinformatycznej,

c) wytwarzanie i obrót urządzeniami i programami umożliwiającymi popełnienie przestępstw opisanych w artykule 165, oraz

grupa przepisów stanowiących implementację przepisów Decyzji Rady Unii Europejskiej z dn.24 lutego 2005 r. w sprawie ataków na systemy informatyczne (2005/222/WSiSW) –

Art. 268a, 269a i 269b kk, przewidujące odpowiedzialność karną za czyny powodujące szkody w bazach danych, zakłócanie pracy w sieci oraz bezprawne wykorzystanie urządzeń i programów komputerowych.

Czyny zabronione określone we wskazanych powyżej przepisach mogą być potraktowane jako akty terroru, jeżeli ich charakter odpowiadać będzie ustawowej definicji przestępstwa mającego charakter terrorystyczny ustalonej w **art. 115 § 20 kk**.

Kodeks karny przestępstwo o charakterze terrorystycznym definiuje jako czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu:

1) poważnego zastraszenia wielu osób,
2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,
3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej - a także groźbę popełnienia takiego czynu.

Jak widać o charakterze terrorystycznym czynu zabronionego decyduje przede wszystkim jego skala (poważne zakłócenia, poważne zastraszenie) i cel czynu, który wymierzony jest bezpośrednio w ustrój lub istotne i podstawowe funkcje państwa oraz funkcje życia społecznego i gospodarczego.

2.2 Wymóg prawnej definicji pojęć

W celu sprecyzowania zakresu i przedmiotu działań mających na celu ochronę cyberprzestrzeni, niezbędne jest prawne zdefiniowanie podstawowych pojęć dotyczących ochrony cyberprzestrzeni, takich jak:

- cyberterroryzm,
- cyberprzestępstwo.

Zdefiniowanie powyższych pojęć umożliwi ścisłe określenie zakresu działań i katalogu zadań podmiotów odpowiedzialnych za ochronę cyberprzestrzeni.

W praktyce brak precyzyjnych definicji może powodować wątpliwości polegające na trudności w ustaleniu organu właściwego dla ścigania sprawców cyberprzestępstwa.

Kontekst cyberprzestrzeni utrudnia rozróżnienie czynu będącego przestępstwem o charakterze terrorystycznym i pospolitego przestępstwa komputerowego, gdyż o ile zdarzenia o małej skali i znaczeniu jednoznacznie można zaklasyfikować jako czyny, za których ściganie odpowiedzialna jest Policja, o tyle duża skala, efekt czy widoczność działań niekoniecznie implikują terrorystyczny charakter czynu (ściganego przez ABW).

W cyberprzestrzeni szczególnie często zdarzenia pozornie o charakterze terrorystycznym okazują się być zdarzeniami o charakterze ledwie kryminalnym. Zdarza się również, iż działania pierwotnie uznane za kryminalne okazują się być fragmentem skorelowanych działań o większej skali bądź poważniejszych skutkach. Sfera cyberprzestrzeni wymaga szczególnej koordynacji działań organów powołanych do ścigania sprawców przestępstw.

Niezbędne jest również zdefiniowanie pojęcia *krytycznej infrastruktury teleinformatycznej państwa*. Aktem prawnym nawiązującym do infrastruktury krytycznej jest *Ustawa o zarządzaniu kryzysowym*. Ustawa definiuje pojęcia infrastruktury krytycznej i ochrony infrastruktury krytycznej oraz podaje ogólne zadania z zakresu ochrony infrastruktury krytycznej. Ustawa nie definiuje jednak pojęcia krytycznej infrastruktury teleinformatycznej państwa i w żaden sposób nie rozpatruje jej specyfiki.

2.3 Wymóg ustalenia odpowiedzialności

Realizacja *Programu* wymaga wypracowania podstaw prawnych definiujących role poszczególnych podmiotów, zakres ich działań oraz obowiązki w ramach programu

ochrony cyberprzestrzeni RP oraz krytycznej infrastruktury teleinformatycznej. Akty normatywne powinny jednoznaczne wskazywać podmioty odpowiedzialne za ściganie cyberprzestępstw oraz za koordynację działań ochrony cyberprzestrzeni w skali państwowej, definiować zadania i obowiązki administracji publicznej w tym zakresie, określać zakres działań w przypadku wystąpienia poważnych incydentów komputerowych oraz zagrożenia funkcjonowania państwa.

Zgodnie z założeniami *Programu* odpowiedzialność za koordynację działań przeciw cyberprzestępczości oraz realizację *Programu* sprawować będzie Minister Spraw Wewnętrznych i Administracji jako minister właściwy dla zagadnień dotyczących informatyzacji państwa i bezpieczeństwa publicznego.

Odpowiedzialność za podejmowanie działań przeciw cyberterroryzmowi, jako szczególnych przypadków cyberprzestępstw, sprawować będzie Szef Agencji Bezpieczeństwa Wewnętrznego.

2.4 Wymóg zapisów o współpracy z sektorem prywatnym

Niezbędne jest zdefiniowanie obowiązków tych podmiotów sektora prywatnego, których ochrona przed zagrożeniami z cyberprzestrzeni jest istotna z punktu widzenia prawidłowego funkcjonowania państwa. Do grupy tej zaliczyć należy na przykład operatorów telekomunikacyjnych dysponujących infrastrukturą telekomunikacyjną stanowiącą podstawę zapewnienia komunikacji w państwie. Należy jednak podkreślić, że zagadnienie ochrony cyberprzestrzeni nie dotyczy jedynie sfery teleinformatycznej, ale również sfery innych usług, np. usług sektora bankowego.

Osiągnięcie rzeczywistej współpracy administracji państwowej i sektora prywatnego stanowi prawdziwe wyzwanie. Współdziałanie takie możliwe jest tylko w sytuacji, gdy w przyjętym rozwiązaniu korzyści z współpracy przeważają nad ryzykiem wynikającym z choćby częściowej utraty kontroli nad informacją. Skutkiem realizacji *Programu* będzie wypracowanie rozwiązań organizacyjno-prawnych sprzyjających rzeczywistej współpracy podmiotów prywatnych z administracją publiczną w kontekście ochrony krytycznej infrastruktury teleinformatycznej państwa.

W związku z powyższym podjęte zostaną działania aktywizujące współpracę pomiędzy podmiotami prywatnymi władającymi fragmentami krytycznej infrastruktury teleinformatycznej o podobnym charakterze, a przez to narażonymi na podobne typy podatności i metody ataków. Jedną z form współpracy mogłoby być tworzenie gremiów powoływanych do wewnętrznej wymiany informacji i doświadczeń oraz współpracy z administracją publiczną w zakresie ochrony krytycznej infrastruktury teleinformatycznej.

2.5 Wymóg prawnego uregulowania zasad ochrony krytycznej infrastruktury teleinformatycznej

Zgodnie z założeniami *Programu* wypracowana zostanie koncepcja ochrony newralgicznej dla funkcjonowania państwa infrastruktury teleinformatycznej oraz przygotowane zostaną podstawy prawne do wykonywania zadań w tym zakresie przez jednostki państwowe. Polityka ochrony cyberprzestrzeni w zakresie krytycznej infrastruktury teleinformatycznej powinna dotyczyć również podmiotów prywatnych.

Celem ochrony krytycznej infrastruktury teleinformatycznej powinno być zapewnienie poprawności i ciągłości funkcjonowania systemów i sieci teleinformatycznych, obiektów i instalacji o szczególnie ważnym znaczeniu dla bezpieczeństwa wewnętrznego państwa

lub zapewniających niezakłócone funkcjonowanie w państwie transportu, łączności, infrastruktury energetycznej, wodociągowej i gazowej oraz systemów informatycznych ochrony zdrowia, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa. Krytyczna infrastruktura teleinformatyczna powinna być chroniona przed zniszczeniem, uszkodzeniem oraz dostępem osób nieuprawnionych. Winny być również określone mechanizmy regulujące przygotowanie, testowanie i uruchomienie rozwiązań zapasowych na wypadek uszkodzenia, zniszczenia, lub niedostępności krytycznej infrastruktury teleinformatycznej. Do takich rozwiązań należą zapasowe ośrodki przetwarzania danych i łącza awaryjne, zdolne przejąć realizację procesów realizowanych przez podmiot dotknięty zdarzeniem.

Obecnie w *Ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* zdefiniowane jest pojęcie krytycznej infrastruktury bez wyszczególnienia pojęcia krytycznej infrastruktury teleinformatycznej oraz zadań i roli poszczególnych podmiotów biorących udział w systemie jej ochrony. W związku z tym MSWiA zainicjuje i przygotuje propozycje zmian legislacyjnych określających cele, zasady i formy ochrony krytycznej dla funkcjonowania państwa infrastruktury teleinformatycznej, a także określenie kompetencji podmiotów właściwych dla ochrony tejże infrastruktury. Zakres zastosowania aktów normatywnych powinien odnosić się do wszystkich organów, których będzie dotyczyć polityka cyberbezpieczeństwa, włączając w to również podmioty sektora prywatnego. Prawo powinno regulować w tym zakresie działalność:

a) organów władzy i administracji rządowej,

b) państwowych i komunalnych osób prawnych,

c) państwowych i komunalnych jednostek organizacyjnych,

d) organów samorządu terytorialnego,

e) jednostek organizacyjnych nie posiadających osobowości prawnej,

f) organizacji społecznych oraz przedsiębiorców realizujący zadania publiczne, jeżeli wykorzystują system, obiekt lub instalację wchodzącą w skład infrastruktury krytycznej.

2.6 Ustalenie sposobów i form współpracy

W ramach *Programu* podjęte zostaną koordynowane przez MSWiA w latach 2009-2010 działania skutkujące określeniem prawnych ram współdziałania podmiotów uczestniczących w procesie ochrony infrastruktury krytycznej państwa w celu zapewnienia jej poprawności i ciągłości funkcjonowania oraz wypracowania metod podnoszenia jej poziomu bezpieczeństwa. Określone zostaną sposoby i formy współdziałania w szczególności polegające na:

a) współpracy w zakresie zapobiegania i zwalczania istotnych ataków komputerowych, zwłaszcza ochrony eksploatowanych systemów i sieci teleinformatycznych, zarówno wydzielonych jak i podłączonych do sieci Internet,

b) udziale systemów i sieci teleinformatycznych, eksploatowanych przez organy administracji rządowej, w programach ochrony,

c) wspieraniu działań zmierzających do ustalenia sprawców cyberterroryzmu,

d) realizowaniu zaleceń dotyczących konfiguracji teleinformatycznych systemów zabezpieczających,

e) przekazywaniu istotnych informacji dotyczących poważnych incydentów naruszenia bezpieczeństwa teleinformatycznego wykrytych we własnych systemach lub sieciach teleinformatycznych oraz o innych istotnych faktach dla bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa,

f) prowadzeniu szkoleń na temat zagrożeń cyberterrorystycznych oraz szpiegostwa prowadzonego przy użyciu systemów i sieci teleinformatycznych.

2.7 Stworzenie sektorowych punktów kontaktowych

W ramach współdziałania jednostek organizacyjnych w zakresie ochrony cyberprzestrzeni zostaną w latach 2009-2010 stworzone sektorowe (resortowe) punkty kontaktowe. Sektorowe punkty kontaktowe staną się elementem systemu komunikacji instytucji związanych z ochroną krytycznej infrastruktury teleinformatycznej. Zadaniem punktów sektorowych będzie raportowanie do nadrzędnego organu ochrony cyberprzestrzeni RP, a z drugiej strony zbieranie informacji od podległych im w ramach resortu i sektora administratorów systemów krytycznych – stanowiących punkty kontaktowe w jednostkach organizacyjnych. Szczegółowe wytyczne dotyczące formy współpracy oraz procedur komunikacji w ramach reakcji na incydent komputerowy określą: Minister Spraw Wewnętrznych i Administracji wraz z Ministrem Obrony Narodowej w porozumieniu z Szefem ABW i Szefem SKW.

2.8 Zapisanie obszaru działania CERT.GOV.PL

Istotne z punktu widzenia wdrożenia *Programu* będzie wskazanie podmiotów odpowiedzialnych za realizację zadań w obszarze krytycznej infrastruktury teleinformatycznej. W tym celu koordynator *Programu* zaproponuje rozwiązania prawne ustalające organizację krajowego systemu ochrony krytycznej infrastruktury teleinformatycznej, oraz powierzy nadzór i koordynację działań w zakresie krajowego systemu ochrony krytycznej infrastruktury teleinformatycznej Szefowi Agencji Bezpieczeństwa Wewnętrznego.

Obecnie Szef ABW właściwy w sprawach ochrony bezpieczeństwa teleinformatycznego państwa dysponuje zasobami w postaci pionu informatycznego ABW, a konkretnie powołanego w lutym 2008 r. w strukturze Departamentu Bezpieczeństwa Teleinformatycznego (DBTI) ABW, Rządowego Zespołu Reagowania na Incydenty Komputerowe – CERT.GOV.PL.

Osiągnięcie wskazanych powyżej celów możliwe będzie poprzez prawne określenie kompetencji, oraz procedur dla funkcjonującego w ABW zespołu CERT.GOV.PL do działania w obszarze całego państwa. Do zadań Rządowego zespołu CERT.GOV.PL należeć będzie:

a) kreowanie polityki w zakresie ochrony przed cyberzagrożeniami,

b) koordynowanie przepływu informacji pomiędzy podmiotami w tym zakresie,

c) wykrywanie, rozpoznawanie i przeciwdziałanie cyberzagrożeniom,

d) współpraca z krajowymi instytucjami, organizacjami oraz podmiotami resortowymi w zakresie ochrony cyberprzestrzeni,

e) reprezentacja RP w kontaktach międzynarodowych (w zakresie współpracy wojskowej, w porozumieniu z Centrum Koordynacyjnym Systemu Reagowania na Incydenty Komputerowe resortu obrony narodowej).

Zadania zespołu CERT.GOV.PL będą obejmować dodatkowo:

a) gromadzenie wiedzy dotyczącej stanu bezpieczeństwa i zagrożeń dla krytycznej infrastruktury teleinformatycznej,

b) reagowanie na incydenty bezpieczeństwa teleinformatycznego ze szczególnym uwzględnieniem krytycznej infrastruktury teleinformatycznej państwa,

c) prowadzenie analiz powłamaniowych,

d) tworzenie polityki ochrony systemów i sieci teleinformatycznych,

e) szkolenia i podnoszenie świadomości odnośnie cyberzagrożeń,

f) przygotowywanie okresowych raportów w zakresie bezpieczeństwa teleinformatycznego państwa,

g) konsulting i doradztwo w zakresie cyberbezpieczeństwa.

Zadania Szefa ABW (oraz Szefa SKW dla sfery wojskowej) realizowane poprzez zespół CERT.GOV.PL w zakresie ochrony krytycznej infrastruktury teleinformatycznej obejmować będzie takie czynności jak:

a) Opracowanie oraz zarządzanie systemem koordynacji zwalczania, przeciwdziałania i reagowania na zagrożenia i ataki na cyberprzestrzeń państwa, w tym prowadzenie rejestru systemu krytycznej infrastruktury teleinformatycznej państwa.

   Szef ABW powinien dokonywać wpisu do powyższego rejestru – z urzędu – w przypadku organów administracji rządowej, samorządowej, państwowych osób prawnych jak i – na wniosek – w przypadku przedsiębiorstw i organizacji społecznych realizujących zadania publiczne,

b) gromadzenie i przetwarzanie informacji w rejestrze oraz ich udostępnianie,

c) opracowywanie analiz w zakresie krytycznej infrastruktury teleinformatycznej państwa,

d) kontrolę ochrony systemu lub sieci teleinformatycznej wpisanej do rejestru,

e) współpracę międzynarodową w zakresie ochrony teleinformatycznej infrastruktury krytycznej państwa. Szef ABW w stosunkach międzynarodowych powinien pełnić funkcję krajowej władzy ochrony systemu krytycznej infrastruktury teleinformatycznej państwa.

2.9 Rola kierowników jednostek organizacyjnych

Zmiany regulacji prawnych obejmą również katalog zadań kierowników jednostek organizacyjnych w zakresie ochrony elementów krytycznej infrastruktury teleinformatycznej posiadanych przez daną jednostkę. W resorcie obrony narodowej odpowiadać za to będzie wyznaczona przez Ministra Obrony Narodowej komórka. Zadania powinny obejmować swoim zakresem:

a) realizację obowiązków wynikających z przepisów aktów prawnych właściwych dla krytycznej infrastruktury teleinformatycznej,

b) ustalenie wewnętrznych procedur obowiązujących w jednostce organizacyjnej, zabezpieczających system lub sieć teleinformatyczną przed zniszczeniem, uszkodzeniem lub dostępem osób nieuprawnionych,

c) zidentyfikowanie i przeanalizowanie zagrożeń i ryzyk, na które mogą być narażone system lub sieć teleinformatyczna wpisane do rejestru krytycznych zasobów teleinformatycznych,

d) przygotowanie i cykliczne weryfikowanie i testowanie rozwiązań zapasowych na wypadek uszkodzenia, zniszczenia lub niedostępności systemów lub sieci wpisanych do rejestru (w szczególności zapasowych ośrodków przetwarzania danych oraz łącz zapasowych),

e) wyznaczenie administratora systemu,

f) niezwłoczne informowanie służby ochrony państwa o:

    a) każdej zmianie siedziby jednostki organizacyjnej,

    b) zaprzestaniu działalności jednostki organizacyjnej,

    c) każdej zmianie administratora systemu,

    d) wydarzeniach mogących mieć wpływ na ochronę systemu lub sieci teleinformatycznej wpisanych do rejestru.

2.10 Rola administratorów w jednostkach organizacyjnych

W każdej jednostce organizacyjnej w ramach systemu ochrony krytycznej infrastruktury teleinformatycznej zostanie powołany administrator systemu. W tym celu określone zostaną minimalne wymagania do obsady stanowiska administratora. Wśród wymagań dla administratorów, które będzie musiał spełnić kandydat na to stanowisko będzie obowiązek posiadania stosownego certyfikatu poświadczającego odbycie specjalistycznego przeszkolenia przez ABW lub SKW w ramach swojego obszaru kompetencyjnego określonego przez odpowiednie akty prawne m. in. z zakresu:

a) podstawowych zagrożeń dla infrastruktury teleinformatycznej,

b) zagadnień związanych z reagowaniem na incydenty komputerowe,

c) zarządzania ryzykiem teleinformatycznym,

d) standardów i polityki bezpieczeństwa.

Zadania wyznaczonego przez kierownika jednostki organizacyjnej administratora systemu wchodzącego w skład krytycznej infrastruktury teleinformatycznej będą obejmować:

a) bezpośredni nadzór nad systemem lub siecią teleinformatyczną wpisaną do rejestru zasobów krytycznej infrastruktury teleinformatycznej,

b) przestrzeganie zasad bezpieczeństwa systemu lub sieci teleinformatycznej wpisanej do rejestru, określonych w wewnętrznych procedurach obowiązujących w jednostce organizacyjnej.

c) niezwłoczne informowanie kierownika jednostki organizacyjnej o:

    a) wydarzeniach mogących mieć wpływ na prawidłowość działania wpisanych do rejestru systemu lub sieci teleinformatycznej danej jednostki,

    b) każdej zmianie dokonanej w systemie lub sieci teleinformatycznej mającej wpływ na bezpieczne ich działanie w jednostce organizacyjnej,

d) monitorowanie działania zabezpieczeń wdrożonych w celu ochrony systemu lub

sieci teleinformatycznej wpisanych do rejestru,

e) zapewnienie sprawności i gotowości działania rozwiązań zapasowych,

f) wykrywanie i reagowanie na przypadki niszczenia lub naruszania bezpieczeństwa systemu lub sieci teleinformatycznej wpisanych do rejestru.

2.11 Rola instytucji koordynującej w jednostkach organizacyjnych

Organy odpowiedzialne za nadzór i koordynację działań odnośnie ochrony krytycznej infrastruktury teleinformatycznej zostaną uprawnione do wykonywania kontroli we wszystkich jednostkach organizacyjnych posiadających zasoby stanowiące elementy krytycznej infrastruktury teleinformatycznej państwa. W trakcie projektowania zmian legislacyjnych należy uwzględnić następujące uprawnienia:

a) wstęp do obiektów i pomieszczeń jednostki organizacyjnej dla wyznaczonych kontrolerów,

b) wgląd do dokumentacji technicznej,

c) udostępnienie do kontroli systemu lub sieci teleinformatycznej wpisanych do rejestru krytycznej infrastruktury teleinformatycznej,

d) współpracę jednostek organizacyjnych w zakresie przygotowywania i przeprowadzania testów bezpieczeństwa włącznie z testami penetracyjnymi systemów lub sieci teleinformatycznej wpisanych do powyższego rejestru,

e) żądanie od kierownika jednostki organizacyjnej (odpowiedzialnego za ochronę krytycznej infrastruktury teleinformatycznej) złożenia ustnych lub pisemnych wyjaśnień,

f) wydawanie zaleceń pokontrolnych,

g) kontrolę stanu realizacji zaleceń pokontrolnych.

2.12 Współpraca międzynarodowa

Szef ABW wraz z kadrowym zapleczem technicznym stanowił będzie Krajowy Punkt Centralny (*Focal Point*) w ramach polityki ochrony cyberprzestrzeni NATO. Z kolei podmiotem odpowiedzialnym za koordynację reagowania na incydenty w sieciach i systemach komputerowych podłączonych do sieci rozległej NATO będzie Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputerowe umiejscowione w Wojskowym Biurze Bezpieczeństwa Łączności i Informatyki podlegającym pod Ministerstwo Obrony Narodowej. Jednocześnie dla obszaru krajowej teleinformatycznej infrastruktury krytycznej, właściwym podmiotem będzie Departament Infrastruktury Teleinformatycznej w Ministerstwie Spraw Wewnętrznych i Administracji.

Szef ABW i Minister Obrony Narodowej przy współpracy z ministrem właściwym do spraw wewnętrznych będą występować jako bezpośredni partner powołanej w 2008 roku władzy odpowiedzialnej za zarządzanie i koordynację działań NATO i jego państw członkowskich w zakresie obrony cyberprzestrzeni - *NATO Cyber Defence Management Authority* (w skrócie: *CDMA*).

Dla prawidłowej realizacji zadań Krajowego Punktu Centralnego pożądane będzie pozyskanie wykwalifikowanych ekspertów i w miarę możliwości delegowanie krajowych ekspertów do prac ośrodka badawczo-szkoleniowego NATO w zakresie ochrony cyberprzestrzeni (*Cooperative Cyber Defence Centre of Excellence, CCD CoE*). Należy również zapewnić ekspertom krajowym możliwości poszerzania wiedzy i doświadczenia

poprzez aktywny udział w pracach grup roboczych Unii Europejskiej oraz szkoleniach z zakresu bezpieczeństwa teleinformatycznego.

W tym celu, Rządowy Zespół Reagowania na Incydenty Komputerowe - CERT.GOV.PL m. in. współpracował będzie na forum międzynarodowym i krajowym w zakresie ochrony cyberprzestrzeni z organizacjami zrzeszającymi zespoły CERT z różnych krajów, takimi jak np. FIRST (*Forum of Incident Response and Security Teams*).

2.13 Współpraca krajowa

W ramach realizacji Programu zostaną wypracowane formy współpracy pomiędzy organami odpowiedzialnymi za cyberbezpieczeństwo RP – ABW, MON, SKW oraz odpowiedzialnymi za zwalczanie przestępczości komputerowej o charakterze kryminalnym Policją i Żandarmerią Wojskową. Powyższe formy współpracy będą miały zarówno postać roboczą, w celu zminimalizowania opóźnień, jak i sformalizowaną służącą eliminowaniu problemów kompetencyjnych.

Istotną formą współpracy w zakresie ochrony cyberprzestrzeni będą bezpośrednie robocze kontakty krajowych zespołów reagowania na incydenty komputerowe, między innymi takich jak:

- Rządowy Zespół Reagowania na Incydenty Komputerowe – CERT.GOV.PL,
- Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputerowe resortu obrony narodowej,
- CERTy powołane przez operatorów telekomunikacyjnych:
  - CERT Polska – działający w ramach NASK,
  - TP CERT – działający w ramach Telekomunikacji Polskiej S.A.,
  - Pionier-CERT – działający w ramach Poznańskiego Centrum Superkomputerowo-Sieciowego w Poznaniu.

2.14 Zapewnienie spójności polityk bezpieczeństwa

Zgodnie z obowiązującymi przepisami jednostki administracji publicznej zobowiązane są do posiadania własnych polityk bezpieczeństwa. Zgodnie z § 3 *Rozporządzenia Rady Ministrów z dn. 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych:*

1. Podmiot publiczny opracowuje, modyfikuje w zależności od potrzeb oraz wdraża politykę bezpieczeństwa dla systemów teleinformatycznych używanych przez ten podmiot do realizacji zadań publicznych.
2. Przy opracowywaniu polityki bezpieczeństwa, o której mowa w ust. 1, podmiot publiczny powinien uwzględniać postanowienia Polskich Norm z zakresu bezpieczeństwa informacji.

Aby móc skutecznie koordynować działania dotyczące ochrony cyberprzestrzeni państwa wskazanym jest działanie na rzecz zapewnienia spójności polityk bezpieczeństwa w zakresie ochrony przed atakami z publicznych sieci teleinformatycznych. Zapewnieniu spójności służyć będą przygotowane przez podmiot odpowiedzialny za ochronę cyberprzestrzeni państwa wytyczne lub zalecenia, dotyczące wzorca fragmentu polityki bezpieczeństwa opisującego aspekty przeciwdziałania i reagowania na zagrożenia cyberterrorystyczne.

2.15 Programy badawcze

Ważne z punktu widzenia powodzenia wykonania *Programu* jest przygotowanie i uruchomienie krajowych programów badawczych dotyczących bezpieczeństwa teleinformatycznego o formule, która zachęciłaby do wspólnego prowadzenia badań naukowych nad bezpieczeństwem teleinformatycznym podmioty zajmujące się bezpieczeństwem teleinformatycznym ze sfery administracji publicznej, ośrodki naukowe oraz inne podmioty dysponujące elementami krytycznej infrastruktury teleinformatycznej państwa, na przykład operatorów teleinformatycznych. Podmiotem koordynującym *Program* w tym zakresie zostanie Ministerstwo Nauki i Szkolnictwa Wyższego (MNiSW) jako ustawowo właściwe w sprawach badań naukowych i prac rozwojowych. Wykaz zadań w obszarze koniecznych programów badawczych, uwzględniając dynamikę stanu wiedzy określony zostanie na poziomie projektów wykonawczych *Programu* i może być uzupełniany z inicjatywy właściwych podmiotów odpowiedzialnych za realizację *Programu.*

2.16 Skuteczność działań

Miarą skuteczności podjętych w ramach *Programu* działań, będzie ocena stworzonych regulacji, instytucji i relacji, które umożliwią rzeczywiste zaistnienie skutecznego systemu ochrony krytycznej infrastruktury teleinformatycznej państwa.

Jedną z podstawowych metod wpływania na skuteczność złożonych działań wykonywanych przez wiele instytucji jest precyzyjne ustalenie zakresu zadań każdego z podmiotów oraz, co powinno być z tym tożsame, precyzyjne ustalenie odpowiedzialności za wykonanie - ale i za niewykonanie - poszczególnych zadań.

Jak uczy doświadczenie, projekty które angażowały dużą liczbę podmiotów, a w których niedostatecznie doprecyzowano kwestię odpowiedzialności za poszczególne działania, z góry skazane były na niepowodzenie. Dlatego też przy tworzeniu regulacji stanowiących działania organizacyjno-prawne niniejszego programu szczególny nacisk należy położyć na jednoznaczne przypisanie odpowiedzialności za poszczególne działania konkretnym podmiotom.

3. Działania techniczne

Działania techniczne powinny obejmować między innymi:

a) *rozbudowę zespołu reagowania na incydenty komputerowe,*

b) *rozbudowę systemu wczesnego ostrzegania przez atakami sieciowymi,*

c) *wdrażanie dodatkowych rozwiązań prewencyjnych,*

d) *zarządzanie ćwiczeń obejmujących badanie odporności krytycznej infrastruktury teleinformatycznej na kontrolowane cyberataki,*

e) *szczególną ochronę kluczowych systemów informatycznych,*

f) *wdrażanie rozwiązań zapasowych, które mogą przejąć realizację procesu w sytuacji uszkodzenia, zniszczenia lub niedostępności systemów i sieci zaliczonych do krytycznej infrastruktury teleinformatycznej,*

g) *rozwój witryny www.cert.gov.pl jako podstawowego źródła informacji o metodach przeciwdziałania, podatnościach i atakach z cyberprzestrzeni,*

h) *konsolidację dostępu do usług publicznych.*

3.1 Rozbudowa zespołu reagowania

Aby możliwe było skuteczne prowadzenie działań związanych z ochroną cyberprzestrzeni, w tym reagowania na incydenty bezpieczeństwa teleinformatycznego, konieczne jest zapewnienie odpowiedniego zaplecza technicznego, nie tylko umożliwiającego realizację bieżących zadań, ale również uwzględniającego wzrastające zapotrzebowanie na specjalizowane systemy teleinformatyczne w przyszłości. W ramach dotychczasowych prac Departamentu Bezpieczeństwa Teleinformatycznego ABW podjęto działania zmierzające do stworzenia zaplecza technicznego na potrzeby Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL. Do 30 czerwca 2009 uruchomione zostaną pomieszczenia zobrazowania dla funkcjonariuszy CERT.GOV.PL. Planowane jest również uruchomienie serwerowni umożliwiającej wieloletni rozwój bazy technicznej zespołu reagowania na incydenty komputerowe.

W związku z rosnącym zagrożeniem dla bezpieczeństwa cyberprzestrzeni należy również dostosować strukturę pionu informatycznego ABW do potrzeb organizacji komórki odpowiedzialnej za reagowanie na incydenty bezpieczeństwa teleinformatycznego w sieciach wchodzących w skład krytycznej infrastruktury teleinformatycznej państwa. W ramach reorganizacji struktury organizacyjnej ABW opracowany zostanie nowy plan etatowy oraz stworzona zostanie polityka rekrutacji dodatkowych funkcjonariuszy mających pracować w CERT.GOV.PL uwzględniająca siatkę płac oraz formę zatrudnienia gwarantującą zatrudnienie ekspertów z danej dziedziny. Reorganizacja spowoduje zwiększenie zasobów DBTI o specjalistów IT z dziedziny bezpieczeństwa sieciowego, analityków bezpieczeństwa oraz inne osoby zdolne do wykonywania działań o wysokim charakterze specjalistycznym.

Analogicznie, w sferze wojskowej właściwy kierownik komórki organizacyjnej przedstawi Ministrowi Obrony Narodowej dostosowaną do zadań wynikających z Programu strukturę organów bezpieczeństwa teleinformatycznego.

3.2 Rozbudowa systemu wczesnego ostrzegania

W ramach *Programu* kontynuowane będą inicjatywy realizowane na podstawie wniosków zawartych w „*Sprawozdaniu z prac Zespołu ds. Krytycznej Infrastruktury Teleinformatycznej"*, zatwierdzonym w maju 2005 r. przez Kolegium ds. Służb Specjalnych. Departament Bezpieczeństwa Teleinformatycznego ABW wraz z zespołem CERT Polska działającym w ramach Naukowej i Akademickiej Sieci Komputerowej (NASK) dokonał wdrożenia systemu wczesnego ostrzegania przed zagrożeniami z sieci Internet – ARAKIS-GOV, w 50 jednostkach organizacyjnych administracji publicznej. Architektura systemu oparta jest na rozproszonym zestawie sensorów instalowanych w chronionych instytucjach na styku sieci produkcyjnej z Internetem. Centralną część systemu stanowią serwery dokonujące m. in. korelacji zdarzeń otrzymanych z poszczególnych źródeł oraz prezentujące wyniki analizy w witrynie WWW. Podstawowym zadaniem systemu jest wykrywanie oraz opisywanie nowych zagrożeń pojawiających się w Internecie. Wartym podkreślenia jest fakt, iż w przeciwieństwie do powszechnie stosowanych rozwiązań, ARAKIS-GOV nie bazuje przede wszystkim na istniejących sygnaturach zagrożeń, lecz dzięki zaawansowanym mechanizmom analizy pakietów sieciowych i korelacji zdarzeń (w tym pochodzących ze źródeł zewnętrznych) sam tworzy sygnatury wykrywanych niezidentyfikowanych zagrożeń, które mogą być następnie stosowane w produktach komercyjnych. ARAKIS-GOV nie jest zatem typowym systemem zabezpieczającym i w żadnym wypadku nie zastępuje funkcjonalności standardowych systemów ochrony sieci takich jak firewall, antywirus czy system IDS/IPS. Ze względu jednak na swoją specyfikę może być z powodzeniem

stosowany jako uzupełnienie wyżej wspomnianych systemów, dostarczające informacji na temat:

a) nowych zagrożeń pojawiających się w sieci Internet – wspólnych dla wszystkich uczestników systemu, w tym m. in.:
   - nowowykrytych samopropagujących się zagrożeń typu *worm*,
   - nowych typów ataków, obserwowanych z poziomu dużej liczby lokalizacji,
   - trendów aktywności ruchu sieciowego na poszczególnych portach,
   - trendów aktywności wirusów rozsyłanych pocztą elektroniczną,
b) zagrożeń lokalnych związanych z konkretną, chronioną lokalizacją:
   - braku aktualnych szczepionek antywirusowych,
   - zainfekowanych komputerów w sieci wewnętrznej,
   - nieszczelnej konfiguracji brzegowych systemów zaporowych,
   - prób skanowania publicznej przestrzeni adresowej zarówno z Internetu jak i z sieci wewnętrznej.

Kontynuując proces wdrażania kolejnych sond sytemu ARAKIS-GOV, a także rozwoju i zwiększania funkcjonalności tego systemu, w celu jak najszerszego wykorzystania potencjału systemu ARAKIS-GOV, w latach 2009-2011 programem objęte zostaną wszystkie elementy krytycznej infrastruktury teleinformatycznej w administracji publicznej i sieci wchodzące w skład krytycznej infrastruktury teleinformatycznej państwa poza administracją publiczną. Osiągnięte to będzie poprzez:

a) instalację kolejnych sensorów systemu na stykach sieci Internet wyznaczonych instytucji administracji publicznej,
b) umożliwienie podmiotom komercyjnym, których sieci należą do krytycznej infrastruktury teleinformatycznej państwa, przystąpienia do projektu ARAKIS-GOV,
c) zapewnienie jak najszerszego dostępu do wyników działania systemu poprzez informowanie o zaletach ARAKIS-GOV oraz promowanie idei wczesnego ostrzegania przed zagrożeniami.

3.3 Wdrażanie dodatkowych rozwiązań prewencyjnych

Mając na uwadze postęp zachodzący w technologiach teleinformatycznych i związaną z nim tendencję pojawiania się coraz bardziej wyrafinowanych zagrożeń dla bezpieczeństwa teleinformatycznego, podczas wdrażania *Programu* podjęte zostaną inicjatywy promujące tworzenie coraz nowocześniejszych rozwiązań wspierających bezpieczeństwo teleinformatyczne.

Projektami o szczególnym znaczeniu są systemy o charakterze prewencyjnym, umożliwiające wykrywanie nowego rodzaju zagrożeń poprzez ich aktywne wyszukiwanie w sieci. Przykładem może być będący obecnie w fazie implementacji system HoneySpiderNetwork służący do zautomatyzowanego wyszukiwania złośliwych stron WWW, będących aktualnie jednym z głównych sposobów przeprowadzania ataków sieciowych. Należy dążyć do stosowania jak najszerszego spektrum różnych rodzajów systemów zabezpieczeń w celu zapewnienia bezpieczeństwa krytycznych zasobów

teleinformatycznych.

3.4 Testowanie poziomu zabezpieczeń

Planowane jest cykliczne organizowanie ćwiczeń polegających na przeprowadzaniu kontrolowanych ataków symulujących działania cyberterrorystyczne. Ćwiczenia mają obejmować swoim zakresem wiele jednostek, posiadających zasoby stanowiące krytyczną infrastrukturę teleinformatyczną państwa. Testy mają służyć ocenie bieżącej odporności krytycznej infrastruktury teleinformatycznej na cyberataki, wskazaniu najsłabszych punktów zabezpieczeń i przygotowaniu zaleceń do dalszych działań prewencyjnych. Ćwiczenia będą organizowane i koordynowane przez zespół CERT.GOV.PL.

3.5 Ochrona kluczowych systemów informatycznych

Zgodnie z „Planem informatyzacji Państwa na lata 2007-2010" stanowiącym załącznik do *Rozporządzenia Rady Ministrów z dn. 28 marca 2005 r. w sprawie Planu Informatyzacji Państwa na lata 2007-2010* budowane przez Departament Bezpieczeństwa Teleinformatycznego ABW: Techniczne Centrum Koordynacji Krajowego Systemu Ochrony Krytycznej Infrastruktury Teleinformatycznej oraz system ARAKIS-GOV wspomagający zarządzanie bezpieczeństwem teleinformatycznym w celu wczesnego ostrzegania administracji publicznej przed zagrożeniami wykrytymi w sieci Internet, mają stanowić podstawę utworzenia warstw bezpieczeństwa sieciowego organizowanej przez MSWiA Elektronicznej Platformy Usług Administracji Publicznej (E-PUAP), a także wydzielonej sieci rządowej. W związku z tym, realizacja Programu docelowo zmierzała będzie do objęcia wszystkich kluczowych rządowych rozwiązań informatycznych polityką bezpieczeństwa opracowaną w ramach *Programu*.

3.6 Rozwój witryny www.cert.gov.pl

Jednym z zadań Rządowego Zespołu Reagowania na Incydenty Komputerowe jest utrzymywanie witryny internetowej dostępnej pod adresem www.cert.gov.pl. Obecna witryna ma charakter tymczasowy i zawiera jedynie podstawowe informacje dotyczące funkcjonowania zespołu oraz niezbędne dane kontaktowe. Docelowo witryna ta powinna stać się głównym źródłem wszelkiego rodzaju informacji związanych z bezpieczeństwem teleinformatycznym dla osób zajmujących się bezpieczeństwem teleinformatycznych w instytucjach administracji publicznej, a także innych osób zainteresowanych tą tematyką.

W szczególności witryna będzie miejscem publikacji następujących informacji:

a) aktualności związanych z bezpieczeństwem teleinformatycznym,

b) informacji o podatnościach i zagrożeniach,

c) biuletynów bezpieczeństwa,

d) różnego rodzaju poradników, dobrych praktyk, itp.,

e) raportów, informacji na temat trendów i statystyk,

f) forum wymiany informacji oraz doświadczeń osób zaangażowanych w działania związane z bezpieczeństwem teleinformatycznym w administracji publicznej i krytycznej infrastrukturze teleinformatycznej.

Ponadto witryna pełnić będzie rolę jednego z dostępnych interfejsów zgłaszania

incydentów bezpieczeństwa teleinformatycznego.

3.7 Konsolidacja dostępu do usług publicznych

Bezpieczeństwo usług świadczonych drogą elektroniczną bardzo silnie zależy od poziomu zabezpieczeń infrastruktury teleinformatycznej operatora sieci teleinformatycznej oraz zarządcy serwerów, z których świadczona jest usługa. W przypadku administracji publicznej duża część usług jest świadczona poprzez tzw. outsourcing (podzlecenie usługi zewnętrznej instytucji), czyli z wykorzystaniem zasobów teleinformatycznych prywatnych operatorów sieci. Należy dążyć do takich rozwiązań systemowych, które zwiększą pozytywne konsekwencje outsourcingu jednocześnie minimalizując potencjalne konsekwencje negatywne. Dla usług krytycznych dla funkcjonowania państwa świadczonych drogą elektroniczną przez administrację publiczną zostanie opracowany katalog wymagań dotyczący poziomu zabezpieczeń, które powinny spełniać systemy teleinformatyczne firm, którym można przekazać usługę w outsourcing.

Konsolidacja usług może również korzystnie odbić się na budżecie tych jednostek administracji państwowej, które aktualnie nie zarządzają kompleksowo umowami outsourcingowymi, co powoduje zupełne rozdrobnienie zleconych usług (przykładowo: każdy portal u innego dostawcy usług albo każda delegatura regionalna podłączana przez innego operatora sieci). Działania konsolidacyjne sprzyjają optymalizacji kosztów, poprzez optymalizację listy kontrahentów i łączenie ofert.

3.8 Zarządzanie Ciągłością Działania krytycznej infrastruktury teleinformatycznej RP (Business Continutiy Management)

W celu zapewnienia nieprzerwanego funkcjonowania infrastruktury teleinformatycznej RP konieczne jest opracowanie Planów ciągłości działania na wypadek zaistnienia sytuacji krytycznej spowodowanej cyberteroryzmem.

Plany ciągłości działania powinny uwzględniać potrzebę posiadania rozwiązań zapasowych w przypadku wystąpienia sytuacji krytycznych powodujących uszkodzenie, zniszczenie lub niedostępność rozwiązań podstawowych. Plany powinny zawierać strukturę zarządzania kryzysowego, listę osób kontaktowych, dokładny opis sposobu postępowania i eskalacji działań oraz sposób powrotu do normalnej działalności sprzed wystąpienia sytuacji kryzysowej. Plany powinny być na bieżąco aktualizowane. W celu weryfikacji skuteczności Planów ciągłości działania powinny być one okresowo testowane.

W opracowywanie oraz testowanie Planów ciągłości działania zaangażowane powinny być wszystkie podmioty, zarówno zarządzające jak i wykorzystujące krytyczną infrastrukturę teleinformatyczną, które realizują ważne z punktu widzenia funkcjonowania RP usługi.

Przy opracowaniu i testowaniu Planów ciągłości działania szczególną uwagę zwrócić należy na zabezpieczenie się przed skutkami cyberataków typu odmowa usługi (Denial of Service - Dos i Distributed Denial of Service - DDos).

Za koordynację całego procesu weryfikacji i testowania Planów ciągłości działania odpowiedzialne jest Ministerstwo Spraw Wewnętrznych i Administracji (MSWiA) jako podmiot odpowiedzialny za krytyczną infrastrukturę teleinformatyczną RP.

3.9 System komunikacji powszechnej

System komunikacji powszechnej powinien obejmować i nadzorować działania związane z komunikacją społeczną w zakresie ochrony cyberprzestrzeni RP, a w szczególności powinien określać zakres informacji oraz kanały jej dystrybucji w przypadkach cyberataków i cyberterroryzmu. Dlatego niezbędne jest powołanie w ramach tego systemu biura prasowego oraz określenie zasad kontaktowania się z mediami w przypadku potrzeby poinformowania społeczeństwa o incydentach w cyberprzestrzeni oraz o ich skali i skutkach (komunikaty w TV, radiu, prasie internecie - poprzez oficjalną stronę Programu). Wydaje się, że w celu niemnożenia bytów, oficjalną stroną internetową Systemu mogłaby być strona www.cert.gov.pl. Ponadto istotnym elementem tego systemu jest stworzenie Contact Center, które stanowiłoby źródło informacji telefonicznej dla obywateli.

Poprzez zintegrowane działania w Systemie społeczeństwo dowiadywałoby się jakie działania w obszarze cyberprzestrzeni są dozwolone, a jakie należy, dla ich bezpieczeństwa, zaniechać.

Brak Systemu może spowodować niekontrolowane (nieświadome) działania obywateli, których skutki mogą być znacznie większe od pierwotnych, powstałych w wyniku ataku na cyberprzestrzeń.

4. Edukacja społeczna i specjalistyczna

Działania w ramach edukacji społecznej i specjalistycznej będą obejmować w szczególności:

a) *racjonalizację programów kształcenia informatycznego na wyższych uczelniach,*
b) *ustawiczne kształcenie specjalistów z dziedziny bezpieczeństwa teleinformatycznego zatrudnionych w jednostkach administracji publicznej,*
c) *współpracę z producentami sprzętowych i programowych zabezpieczeń,*
d) *działalność CERT.GOV.PL jako ośrodka konsultacyjnego i doradczego w zakresie ochrony cyberprzestrzeni i bezpieczeństwa teleinformatycznego,*
e) *realizację kampanii społecznej o charakterze edukacyjno-prewencyjnym.*

4.1 Racjonalizacja programów kształcenia na uczelniach wyższych

Jednym z podstawowych aspektów zapewnienia bezpieczeństwa cyberprzestrzeni jest posiadanie wysoko wykwalifikowanych kadr w sektorze publicznym i prywatnym odpowiadających za utrzymanie systemów i sieci teleinformatycznych ze szczególnym uwzględnieniem zasobów kluczowych dla bezpieczeństwa państwa. Aby zapewnić ciągły dopływ odpowiednio wyszkolonych specjalistów z dziedziny bezpieczeństwa teleinformatycznego konieczne jest zaangażowanie w program ochrony cyberprzestrzeni wyższych uczelni. Zagadnienia związane z bezpieczeństwem powinny stać się stałym elementem każdego programu nauczania. W szczególności dotyczy to uczelni technicznych kształcących informatyków - bez względu na końcową specjalizację informatyczną. Nie można dopuszczać do sytuacji, w której projektanci i programiści aplikacji skupiają się wyłącznie na funkcjonalności zapominając o zasadach bezpiecznego tworzenia kodu, a administratorzy sieci i systemów za priorytet stawiają dostępność zasobów dla swych użytkowników zapominając o konieczności ochrony

przetwarzanych informacji przed intruzami. W tym celu konieczne jest między innymi objęcie bezpieczeństwa teleinformatycznego długofalowym programem kierunków zamawianych, a także ustanowienie adekwatnego programu rozwoju kadry naukowej.

Zadanie propagowania zmian w obszarze programów nauczania należeć będzie do Ministra Nauki i Szkolnictwa Wyższego.

4.2 Kształcenie ustawiczne specjalistów

Równolegle z kształceniem nowych kadr konieczne jest zapewnienie specjalistycznych szkoleń dla osób obecnie odpowiedzialnych za bezpieczeństwo i administrujących zasobami teleinformatycznymi administracji publicznej. Należy jednocześnie dążyć do podnoszenia poziomu merytorycznego ośrodków szkoleniowych, między innymi poprzez ich audytowanie i uznawanie przez organy odpowiedzialne za bezpieczeństwo teleinformatyczne. W ramach działań zmierzających do zwiększenia kompetencji osób odpowiedzialnych za nadzór nad rządowymi sieciami teleinformatycznymi na bazie inicjatywy współpracy Departamentu Bezpieczeństwa Teleinformatycznego ABW z podmiotami komercyjnymi stworzony zostanie program organizacji szkoleń dla administracji publicznej.

4.3 Kształcenie kadry urzędniczej oraz ustanowienie dodatkowych kryteriów obsady stanowisk w administracji publicznej

Analogicznie do szkoleń dla osób odpowiedzialnych za zasobami teleinformatyczne administracji publicznej, konieczna jest edukacja kadry urzędniczej, mającej dostęp oraz korzystającej z infrastruktury teleinformatycznej państwa, w zakresie zagadnień dotyczących bezpieczeństwa sieci – odpowiednio do zajmowanego stanowiska i ryzyka z nim związanego. Szkolenia powinny dotyczyć w szczególności zastosowania procedur ochrony informacji w instytucji, znajomości technik wyłudzania informacji stosowanych w cyberprzestępczości, konsekwencji złamania zabezpieczeń przez cyberprzestępców, procedur obowiązujących w przypadku udanego ataku cyberterrorystów. Wraz z rozwojem infrastruktury teleinformatycznej państwa, procedury bezpieczeństwa powinny być modyfikowane a szkolenia ponawiane – odpowiednio do zakresu wprowadzonych zmian. Szkolenia powinny zawsze kończyć się weryfikacją nabytych informacji – czy to w formie egzaminu, czy też w ramach ćwiczeń przeprowadzanych zgodnie z punktem 3.4. Odrębnym zagadnieniem jest weryfikacja wiadomości w zakresie bezpieczeństwa oraz ryzyka związanego z korzystaniem z sieci, dla osób ubiegających się o stanowiska w administracji publicznej. Konieczne jest, aby takie osoby posiadały wiedzę w tym zakresie – przynajmniej na poziomie minimalnych standardów. W trakcie procedury rekrutacyjnej sprawdzenia kompetencji mogą dokonać osoby administrujące zasobami teleinformatycznymi.

4.4 Współpraca z producentami systemów teleinformatycznych

Ważnymi partnerami dla instytucji rządowych i innych podmiotów odpowiedzialnych za bezpieczeństwo teleinformatyczne w działaniach zmierzających do zwiększenia bezpieczeństwa w cyberprzestrzeni są producenci sprzętu i oprogramowania. Rozwój współpracy z tymi partnerami, w tym wymiana doświadczeń i oczekiwań, stanowić będzie jeden z ważniejszych czynników mających duży wpływ zarówno na system edukacji społecznej i specjalistycznej, jak i na jakość tworzonych systemów. Szczególne znaczenie dla rozszerzenia spektrum dostępnych narzędzi ma współpraca podmiotów odpowiedzialnych za bezpieczeństwo teleinformatyczne z producentami systemów

zabezpieczeń. Należy dążyć do udostępniania pojedynczym jak i instytucjonalnym użytkownikom jak największego wachlarza rozwiązań służących ochronie informacji. Zadaniem służb takich jak ABW i SKW, posiadających zgodnie z ustawą o ochronie informacji niejawnych kompetencje w zakresie certyfikacji środków ochrony kryptograficznej, będzie inicjowanie współpracy i zachęcanie firm do tworzenia nowych rozwiązań oraz branie czynnego udziału w ich tworzeniu i popularyzacji.

4.5 Działania konsultacyjne i doradcze

Wskazanym jest skuteczne rozpropagowanie informacji o konsultacyjnej i doradczej roli podmiotu odpowiedzialnego za ochronę cyberprzestrzeni państwa, czyli ABW, a konkretnie zespołu CERT.GOV.PL, wobec wszystkich podmiotów administracji publicznej oraz podmiotów prywatnych posiadających zasoby stanowiące krytyczną infrastrukturę teleinformatyczną państwa.

ABW powinno być postrzegane nie tylko jako instytucja pełniąca ustawowe obowiązki służby ochrony państwa, tu w kontekście zagrożeń z cyberprzestrzeni, ale również - analogicznie jak w przypadku zagadnień objętych ustawą o ochronie informacji niejawnej – jako centrum kompetencyjne służące pomocą merytoryczną zarówno na etapie tworzenia właściwych struktur i procedur jak i problemów w trakcie ich eksploatacji w poszczególnych jednostkach administracji czy też podmiotów zarządzających fragmentami krytycznej infrastruktury teleinformatycznej.

4.6 Kampania społeczna o charakterze edukacyjno-prewencyjnym

Powszechność korzystania przez obywateli z systemów informatycznych podłączonych do Internetu oraz zwiększające się znaczenie dostępności usług oferowanych przez sieć implikują konieczność uwrażliwienia obywateli na problem bezpieczeństwa informatycznego, podnoszenia ich świadomości odnośnie bezpiecznych metod korzystania z systemów informatycznych. Każdy użytkownik komputera powinien pamiętać o tym, że korzystanie z Internetu oprócz niekwestionowanych korzyści niesie za sobą także szereg zagrożeń. Każdy użytkownik komputera wcześniej czy później zetknie się z nimi, nawet, jeśli będą one dla niego niezauważalne. Dlatego tak ważne jest szerzenie wśród całego społeczeństwa świadomości istnienia niebezpieczeństw w globalnej sieci oraz konieczności przeciwdziałania cyberzagrożeniom. Świadomość i wiedza na temat sposobów przeciwdziałania i zwalczania zagrożeń stanowią kluczowe elementy walki z tymi zagrożeniami. Jedynie odpowiedzialne zachowanie odpowiednio wyedukowanego użytkownika może skutecznie zminimalizować ryzyko wynikające z istniejących zagrożeń. Należy podkreślić, iż we współczesnym świecie zapewnienie bezpieczeństwa teleinformatycznego nie zależy jedynie od działalności wyspecjalizowanych instytucji rządowych, specjalistów do spraw bezpieczeństwa teleinformatycznego, zespołów reagowania na incydenty, ani nawet administratorów sieci. Wraz z upowszechnieniem się dostępu do Internetu w domach, szkołach i miejscach pracy oraz zmianą sposobu przeprowadzania ataków komputerowych, gdzie do skutecznej infekcji wykorzystywana jest nie tylko podatność oprogramowania, lecz coraz częściej niewiedza lub niefrasobliwość użytkowników, odpowiedzialność za bezpieczeństwo spoczywa na każdym użytkowniku komputera.

Kampania społeczna o charakterze edukacyjno-prewencyjnym stanowi wyzwanie i jest istotnym elementem *Programu*. Ze względu na fakt, że przestępczością komputerową zagrożeni są zarówno użytkownicy indywidualni, jak również instytucje publiczne, podmioty gospodarcze, organizacje społeczne, kampania będzie miała charakter wielowymiarowy i uwzględniać będzie konieczne zróżnicowanie form i treści przekazu w

zależności od potrzeb jej adresatów. Zawierać się ona będzie w powszechnym oraz instytucjonalnie różnorodnym oddziaływaniu na postawy wszystkich użytkowników komputerów podłączonych do Internetu. Zakłada się długofalowy i globalny charakter kampanii społecznej.

Ze względu na bezpieczeństwo teleinformatyczne warunkujące realizację zadań publicznych, adresatami akcji informacyjnych będą w szczególności pracownicy administracji publicznej oraz podmioty, których zasoby należą do infrastruktury krytycznej.

Kampania *edukacyjno-prewencyjna* skierowana zostanie także do:

a) dzieci i młodzieży – jako grupy najbardziej podatnej na wpływy. Edukacja powinna rozpocząć się już od najmłodszych lat, w celu wytworzenia pewnych nawyków, które uchronią najmłodszych przed zagrożeniami czyhającymi na nich w sieci (np. przed zjawiskiem *cyberbullingu* - przemocy w sieci, zawieraniem niebezpiecznych znajomości, niecenzuralnymi treściami, piractwem, uzależnieniem od Internetu). Dziecko wiedzę na temat cyberzagrożeń powinno uzyskiwać zarówno w szkole jak i w domu.

b) rodziców – jako najważniejszych nauczycieli i osoby odpowiedzialne za wychowanie kolejnych pokoleń. To na rodzicach spoczywa odpowiedzialność za przygotowanie dzieci do funkcjonowania w społeczeństwie, również w społeczeństwie informacyjnym. Statystyki wskazują, iż komputer przestaje być w Polsce traktowany jako dobro luksusowe, a staje się sprzętem codziennego użytku znajdującym się na wyposażeniu większości polskich rodzin. Stopniowo rośnie również liczba domowych szerokopasmowych przyłączy do Internetu. Aby móc zapewnić skuteczny nadzór nad działalnością dziecka w Internecie rodzice sami powinni posiąść odpowiednią wiedzę na temat zagrożeń oraz metod ich unikania.

c) nauczycieli – w związku z pełnioną przez tę grupę zawodową misją edukacyjną oraz olbrzymią rolą szkoły w procesie kształcenia i wychowywania. W społeczeństwie informacyjnym komunikacja obywatel-państwo i przedsiębiorca-państwo w coraz większym stopniu będzie wykorzystywać drogę elektroniczną, zatem aspekt świadomego i bezpiecznego korzystania z systemów informatycznych powinien stać się elementem nowoczesnej edukacji z zakresu wychowania obywatelskiego.

Kampanii społeczna adresowana do dzieci, młodzieży i ich rodziców w dużej mierze powinna być realizowana w placówkach oświatowych wszystkich szczebli.

Kampania społeczna edukacyjno – prewencyjna realizowana będzie także za pośrednictwem środków masowego przekazu. Media – jako istotny partner w promowaniu zagadnień ochrony cyberprzestrzeni RP oraz popularyzacji przedsięwzięć zawartych w *Programie* zwiększą skuteczność realizacji założonych celów. Dzięki ich pomocy w trakcie realizacji *Programu* możliwe będzie również przeprowadzenie rozmaitych akcji informacyjnych i kampanii edukacyjnych. W tym celu zaangażowane zostaną media ogólnopolskie, regionalne i lokalne.

W ramach kampanii społecznej informacje dotyczące bezpieczeństwa teleinformatycznego oraz przedsięwzięć edukacyjnych i organizacyjno-prawnych podejmowanych w ramach Programu prezentowane będą na stronach internetowych: MSWiA, ABW oraz na stronie zespołu CERT.GOV.PL, gdzie będą dostępne także interaktywne kursy dotyczące zagadnień bezpieczeństwa.

Podmiotami odpowiedzialnymi za realizację *Programu* w tym zakresie będą zgodnie

z właściwością MSWiA, MON, MNiSW, MEN oraz ABW.

5. Podsumowanie

Program ochrony cyberprzestrzeni RP na lata 2009-2011 jest programem o szerokim spektrum działań.

Program jest pierwszym rządowym dokumentem całościowo obejmującym kwestie bezpieczeństwa przestrzeni cybernetycznej państwa. Główną zaletą Programu jest jednoznaczne określenie celów i kierunków działań stanowiących ramy realizacji *Programu* oraz podmiotów odpowiedzialnych za koordynację i realizację Programu.

Istotne z punktu widzenia interesu państwa jest, iż *Program* powstaje w czasie, kiedy w Polsce nie odnotowany został żaden incydent teleinformatyczny na miarę ataku, który miał miejsce w Estonii. W tym sensie przyjęcie *Programu* stanowić będzie jeden z elementów prewencyjnej polityki państwa, dzięki któremu uruchomione zostaną procesy mogące w dużej mierze przyczynić się do zapobiegnięcia naruszeniu w przyszłości bezpieczeństwa cyberprzestrzeni państwa.

Wdrożenie niniejszego *Programu* w latach 2009-2011, zgodnie z założeniami Rządu ma stać się kamieniem milowym w realizacji polityki państwa w obszarze bezpieczeństwa jego cyberprzestrzeni.

Osiągnięcie celu *Programu,* jakim jest podniesienie bezpieczeństwa krytycznej dla państwa infrastruktury teleinformatycznej powinno przyczynić się do nadania temu celowi stałego miejsca w rozważaniach na temat bieżącej polityki, jak i w formułowaniu długookresowych idei i planów kolejnych rządów RP.

Program w przedłożonej postaci, z uwagi na merytorycznie rozległy charakter, nie jest dokumentem *stricte* programowym i stanowi podstawę do wypracowania Portfela projektów wykonawczych. W projektach wykonawczych określone zostaną w szczególności role podmiotów wdrażających i współpracujących przy realizacji poszczególnych części *Programu;* szczegółowy harmonogram działań, uwzględniający rodzaje, kolejność i terminy realizacji zadań, oznaczenie skutków finansowych wprowadzanych rozwiązań, itd. Ponadto w projektach wykonawczych ujęte zostaną rodzaje działań o charakterze legislacyjnym – np. prawne uregulowanie organizacji ochrony krytycznej infrastruktury teleinformatycznej państwa, jak i rodzaje działań o charakterze technicznym takie jak rozbudowa i wdrożenie narzędzi, aplikacji i procedur dla zwiększenia zdolności państwa do reagowania na ataki cyberterrorystyczne. Portfel projektów wykonawczych do *Programu* będą uzupełniać również projekty zakrojonych na szeroką skalę działań o charakterze edukacyjnym uświadamiających adresatom Programu potrzebę ochrony cyberprzestrzeni państwa.

5.1 Przewidywane efekty programu

Przewiduje się następujące długofalowe efekty skutecznego wdrożenia niniejszego programu:

a) większy poziom bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa oraz większy poziom odporności państwa na ataki cyberterrorystyczne,

b) spójną dla wszystkich zaangażowanych podmiotów administracji publicznej i innych współstanowiących krytyczną infrastrukturę teleinformatyczną państwa politykę dotycząca bezpieczeństwa cyberprzestrzeni,

c) mniejszą skuteczność ataków cyberterrorystycznych i mniejsze koszty usuwania

następstw ataków cyberterrorystycznych,

d) funkcjonujący skuteczny system koordynacji i wymiany informacji pomiędzy publicznymi i prywatnymi podmiotami odpowiedzialnymi za zapewnianie bezpieczeństwa cyberprzestrzeni oraz władającymi zasobami stanowiącymi krytyczną infrastrukturę teleinformatyczną państwa,

e) większą kompetencję odnośnie bezpieczeństwa cyberprzestrzeni podmiotów zaangażowanych w ochronę krytycznej infrastruktury teleinformatycznej państwa,

f) większe zaufanie obywateli do właściwego zabezpieczenia usług państwa świadczonych drogą elektroniczną, upowszechnienie elektronicznej drogi korzystania z tych usług,

g) większą świadomość obywateli co do metod bezpiecznego użytkowania systemów dostępnych elektronicznie i sieci teleinformatycznych.

5.2 Skutki finansowe

Ponieważ częściowo *Program* zakłada kontynuację i koordynację już realizowanych bądź zaplanowanych działań, część zadań przypisanych w programie poszczególnym instytucjom będzie finansowana ze środków budżetowych pozostających w ich dyspozycji.

Budżet działań wymagających odrębnego dodatkowego finansowania zostanie oszacowany w Portfelu projektów wykonawczych.

5.3 Metoda oceny skuteczności programu

Za miarę oceny skuteczności programu przyjmuje się stopień osiągnięcia podanych powyżej przewidywanych efektów programu. Natomiast jako miarę oceny skuteczności wdrażania programu przyjmuje się stopień podjęcia i zrealizowania działań wymienionych wśród działań organizacyjno-prawnych, technicznych oraz szkoleniowych i edukacyjnych.