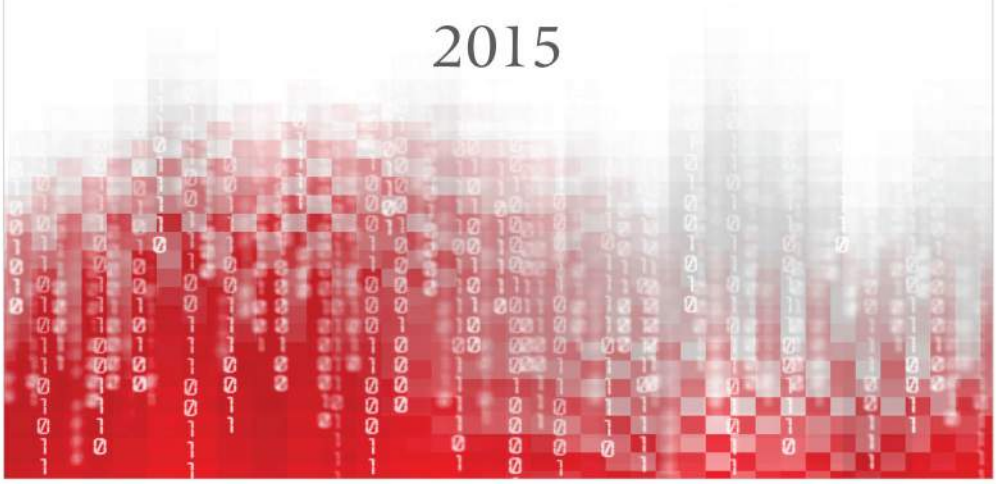
Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej

2015



Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej

Warszawa 2015

SPIS TREŚCI

SŁOWO WSTĘPNE PREZYDENTA RZECZYPOSPOLITEJ POLSKIEJ

Szanowni Państwo,

Jedną z najważniejszych zmian we współczesnym środowisku bezpieczeństwa jest pojawienie się nowego obszaru aktywności państwa, podmiotów prywatnych i obywateli, jakim jest cyberprzestrzeń. Zmiana ta sprawia, że musimy być przygotowani na zagrożenia z jakimi wcześniej nie mieliśmy do czynienia.

Cyberprzestrzeń jest polem konfliktu, na którym przychodzi nam zmierzyć się nie tylko z innymi państwami, ale także z wrogimi organizacjami, jak choćby z grupami ekstremistycznymi, terrorystycznymi, czy zorganizowanymi grupami przestępczymi. Dlatego jednym z istotnych priorytetów polskiej strategii stało się bezpieczeństwo tego nowego środowiska.

Zgodnie z tym priorytetem dokonaliśmy już pewnych zmian w polskim systemie prawnym, wprowadzając do niego w 2011 r. m.in. pojęcie cyberprzestrzeni oraz ustanawiając prawne podstawy nadzwyczajnego reagowania na występujące w niej zagrożenia. W pełni wykorzystujemy dorobek Unii Europejskiej i NATO w tej dziedzinie. Na potrzeby polskiej administracji wprowadzono nowe rozwiązania w toku prac nad Polityką Ochrony Cyberprzestrzeni RP, przyjętą przez Radę Ministrów w 2013 r. Dokument ten dotyczy przede wszystkim ochrony cyberprzestrzeni w wymiarze pozamilitarnym. W Ministerstwie Obrony Narodowej trwają prace nad budową systemu cyberobrony. Prywatne podmioty dbają o swoje bezpieczeństwo w cyberprzestrzeni także we własnym zakresie.

Celem niniejszej doktryny jest stworzenie warunków do połączenia i strategicznego ukierunkowania tych wysiłków na rzecz budowania zintegrowanego systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Dokument przygotowany został w wyniku analiz prowadzonych z udziałem przedstawicieli administracji publicznej, środowiska akademickiego, organizacji pozarządowych oraz sektora prywatnego. Główne założenia doktryny zostały rozpatrzone i zaakceptowane przez Radę Bezpieczeństwa Narodowego.

Doktryna cyberbezpieczeństwa wskazuje strategiczne kierunki działań dla zapewnienia bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni. Jednocześnie powinna być traktowana jako jednolita podstawa koncepcyjna, zapewniająca spójne i kompleksowe podejście do zagadnień cyberochrony i cyberobrony – jako wspólny mianownik dla działań realizowanych przez podmioty administracji publicznej, służby bezpieczeństwa i porządku publicznego, siły zbrojne, sektor prywatny oraz obywateli. Dzięki temu doktryna cyberbezpieczeństwa może stanowić punkt wyjścia do dalszych prac na rzecz wzmocnienia bezpieczeństwa Polski.

Warszawa, 22 stycznia 2015 roku

WPROWADZENIE

1. We współczesnym świecie bezpieczeństwo państwa, w sferze militarnej i pozamilitarnej, zewnętrznej i wewnętrznej, zyskało dodatkowy wymiar, jakim – obok lądu, wody, powietrza i przestrzeni kosmicznej – jest cyberprzestrzeń.

2. Działania na rzecz cyberbezpieczeństwa muszą być podejmowane z uwzględnieniem ochrony praw człowieka i obywatela, a także poszanowaniem prawa do wolności słowa oraz prywatności. Proporcjonalność środków bezpieczeństwa w stosunku do zagrożeń powinna być oparta na efektywnej i wiarygodnej analizie ryzyka.

3. Punktem wyjścia niniejszej Doktryny są kierunkowe postanowienia Strategii Bezpieczeństwa Narodowego RP dotyczące cyberbezpieczeństwa, a także zapisy Polityki Ochrony Cyberprzestrzeni RP oraz Strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń.

4. Główne pojęcia przyjęte w Doktrynie:

- **cyberprzestrzeń –** przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami;
- **cyberprzestrzeń RP** – cyberprzestrzeń w obrębie terytorium państwa polskiego oraz w miejscach, gdzie funkcjonują przedstawicielstwa RP (placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji);
- **cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni)** – proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich

dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni;

- **bezpieczeństwo cyberprzestrzeni RP** – część cyberbezpieczeństwa państwa, obejmująca zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych;
- ś**rodowisko cyberbezpieczeństwa –** ogół warunków funkcjonowania danego podmiotu w cyberprzestrzeni charakteryzowany przez wyzwania (szanse i ryzyka) oraz zagrożenia dla osiągania przyjętych celów;
- **wyzwania cyberbezpieczeństwa –** sytuacje problemowe w dziedzinie cyberbezpieczeństwa, stwarzane zwłaszcza przez szanse i ryzyka oraz generujące dylematy decyzyjne, przed jakimi stoi podmiot w rozstrzyganiu spraw cyberbezpieczeństwa;
- **szanse cyberbezpieczeństwa –** niezależne od woli podmiotu okoliczności (zjawiska i procesy w środowisku bezpieczeństwa) sprzyjające realizacji interesów oraz osiąganiu celów podmiotu w dziedzinie cyberbezpieczeństwa;
- **ryzyka cyberbezpieczeństwa –** możliwości negatywnych dla danego podmiotu skutków własnego działania w sferze cyberbezpieczeństwa;
- **zagrożenia cyberbezpieczeństwa –** pośrednie lub bezpośrednie zakłócające lub destrukcyjne oddziaływania na podmiot w cyberprzestrzeni;
- **Doktryna cyberbezpieczeństwa RP –** oficjalne poglądy i ustalenia dotyczące celów, ocen środowiska oraz koncepcji (zasad i sposobów) działania (w tym tzw. dobrych praktyk) dla zapewnienia bezpiecznego funkcjonowania państwa jako całości, jego struktur, osób fizycznych i osób prawnych – w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej – w cyberprzestrzeni.

1. CELE STRATEGICZNE RP W DZIEDZINIE CYBERBEZPIECZEŃSTWA

5. **Strategicznym celem** w obszarze cyberbezpieczeństwa RP, sformułowanym w Strategii Bezpieczeństwa Narodowego RP, jest **zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni**, w tym adekwatnego poziomu bezpieczeństwa narodowych systemów teleinformatycznych – zwłaszcza teleinformatycznej infrastruktury krytycznej państwa – a także kluczowych dla funkcjonowania społeczeństwa prywatnych podmiotów gospodarczych, w szczególności wchodzących w skład sektorów: finansowego, energetycznego i ochrony zdrowia.

6. Cel strategiczny osiąga się przez realizację zadań prowadzących do osiągania celów o charakterze **operacyjnym i preparacyjnym**. Główne cele operacyjne to:

- ocena warunków cyberbezpieczeństwa, w tym rozpoznawanie zagrożeń, szacowanie ryzyk i identyfikacja szans;
- zapobieganie (przeciwdziałanie) zagrożeniom, redukowanie ryzyk i wykorzystywanie szans;
- obrona i ochrona własnych systemów i zgromadzonych w nich zasobów;
- zwalczanie (dezorganizowanie, zakłócanie i niszczenie) źródeł zagrożeń (aktywna obrona oraz działania ofensywne);
- po ewentualnym ataku – odtwarzanie sprawności i funkcjonalności systemów tworzących cyberprzestrzeń.

7. Do osiągnięcia powyższych celów operacyjnych potrzebne jest, w **wymiarze preparacyjnym,** zbudowanie, utrzymywanie i systematyczne doskonalenie (rozwój) zintegrowanego, zarządzanego (koordynowanego) ponadresortowo, systemu cyberbezpieczeństwa RP obejmującego:

- podsystem kierowania – zdolny do organizowania i koordynowania działań podmiotów rządowych i pozarządowych realizujących zadania w zakresie cyberbezpieczeństwa;
- podsystemy operacyjne i wsparcia – zdolne do samodzielnego prowadzenia defensywnych (ochronnych i obronnych) oraz ofensywnych cyberoperacji, a także udzielania i przyjmowania wsparcia w ramach działań sojuszniczych.

2. ŚRODOWISKO CYBERBEZPIECZEŃSTWA RP

2.1. WYMIAR WEWNĘTRZNY

2.1.1. Zagrożenia

8. Wraz z postępującym rozwojem technologicznym wszystkie tradycyjne wewnętrzne zagrożenia bezpieczeństwa coraz częściej mogą znajdować odpowiedniki (analogie) w cyberprzestrzeni. Mowa o zjawiskach takich, jak cyberprzestępczość, cyberprzemoc, cyberprotesty czy cyberdemonstracje o charakterze destrukcyjnym, zakłócające realizację istotnych zadań administracji publicznej oraz sektora prywatnego.

9. Wśród cyberzagrożeń szczególnie istotne są te dotyczące infrastruktury krytycznej państwa, sterowanej za pomocą systemów informatycznych. W tym zakresie nadzwyczaj niebezpieczne dla państwa mogą być celowe ataki na systemy komunikacji (łączności) zapewniające sprawne funkcjonowanie podsystemu kierowania bezpieczeństwem narodowym, podsystemu obronnego i podsystemów ochronnych, a także podsystemów wsparcia (gospodarczego i społecznego).

10. Z podmiotami publicznymi w cyberprzestrzeni współistnieją i współdziałają podmioty prywatne. Wśród nich szczególnie zagrożone, zwłaszcza kradzieżą danych lub naruszeniem ich integralności, naruszeniem poufności prowadzonych działań czy dostępności usług, są podmioty należące do sektorów: finansowego, wysokich technologii, energetycznego, transportowego oraz zdrowia publicznego.

11. Narażeni na zagrożenia w cyberprzestrzeni są także operatorzy oraz dostawcy usług teleinformatycznych. Zakłócenia ich działalności, zwłaszcza przerwanie ciągłości świadczenia usług, mogą zakłócić funkcjonowanie instytucji państwowych, podmiotów sektora prywatnego i obywateli.

12. Odrębną kategorią zagrożeń są zjawiska, z którymi stykają się obywatele RP. W dobie przenoszenia do cyberprzestrzeni wielu usług świadczonych przez administrację publiczną oraz usług o charakterze finansowym poważnym zagrożeniem stają się kradzieże danych, kradzieże tożsamości i przejmowanie kontroli nad prywatnymi komputerami.

2.1.2. Wyzwania (ryzyka i szanse)

13. Ryzyka w obszarze cyberbezpieczeństwa RP wiążą się z lukami i słabościami istniejącymi w systemie cyberbezpieczeństwa. Ich najpoważniejszymi źródłami są:

- nieuregulowane lub niewłaściwie uregulowane relacje między poszczególnymi podmiotami w tym systemie (przyczyną może być zła komunikacja, brak wymiany informacji, a także nieprecyzyjne określenie odpowiedzialności w zakresie przeciwdziałania cyberzagrożeniom);
- luki prawne (np. co do obowiązku raportowania istotnych incydentów naruszenia bezpieczeństwa teleinformatycznego, a także obowiązku współpracy w ich rozwiązywaniu z powołanymi do tego celu zespołami).

14. Ryzyka w dziedzinie cyberbezpieczeństwa potęgowane są dynamiką wzrostu wykorzystywania przez instytucje publiczne zaawansowanych systemów informatycznych do wykonywania zadań o krytycznym znaczeniu dla funkcjonowania państwa i społeczeństwa.

15. Szczególnie wysokie ryzyka wiążą się z wykorzystaniem dla potrzeb bezpieczeństwa narodowego (militarnego, pozamilitarnego, zewnętrznego i wewnętrznego) wysoce zinformatyzowanych systemów technicznych obcej produkcji, zwłaszcza systemów walki i wsparcia (w tym zautomatyzowanych systemów dowodzenia i kierowania), bez uzyskania dostępu do kodów źródłowych ich oprogramowania, gwarantujących informatyczne panowanie (kontrolę) nad nimi.

16. Istotne źródło ryzyk stanowi wrażliwość systemów teleinformatycznych administracji publicznej na możliwe działania ograniczające dostępność i integralność oraz naruszające poufność przetwarzanych w nich danych. Dotyczy to także braku skutecznych zabezpieczeń teleinformatycznych oraz planów przywracania sprawności tych systemów.

17. Źródłem ryzyk może być nieodpowiednie finansowanie zespołów powołanych do koordynacji reagowania na incydenty komputerowe na poziomie krajowym, a także nieadekwatne finansowanie wdrażania zabezpieczeń eksploatowanych systemów teleinformatycznych.

18. Ryzyka dla cyberbezpieczeństwa RP wiązać mogą się ze strukturą własności prywatnych operatorów i dostawców usług teleinformatycznych (szczególnie w przypadku podmiotów transnarodowych z zagranicznymi ośrodkami decyzyjnymi) ograniczającą wpływ państwa na ich funkcjonowanie.

19. Do działań mogących rodzić ryzyka, zwłaszcza z punktu widzenia podmiotów gospodarczych oraz obywateli, należy zaliczyć ewentualne próby wprowadzania zmian organizacyjnych i regulacji w zakresie cyberbezpieczeństwa bez zapewnienia koniecznego dialogu oraz konsultacji społecznych. Powodować to może sprzeciw społeczny motywowany obawami o naruszenia praw człowieka lub wolności gospodarczej.

20. Coraz szersze zagospodarowanie cyberprzestrzeni może stwarzać ryzyko braku akceptacji społecznej dla racjonalnego określenia granicy między wolnością osobistą i ochroną praw jednostki w świecie wirtualnym a stosowaniem środków służących zapewnieniu akceptowalnego poziomu bezpieczeństwa, co może powodować trudności we wprowadzaniu nowych, efektywnych systemów bezpieczeństwa w cyberprzestrzeni.

21. Szanse w dziedzinie cyberbezpieczeństwa stwarza potencjał naukowy RP w dziedzinie nauk informatycznych i matematycznych, dający możliwość rozwijania narodowych systemów służących cyberbezpieczeństwu oraz kryptologii, w tym kryptografii, zapewniających suwerenne panowanie nad systemami teleinformatycznymi należącymi do państwa.

22. Jako szansę należy wskazać rosnącą świadomość w zakresie cyberbezpieczeństwa, zarówno wśród obywateli, jak i podmiotów prywatnych, które coraz częściej pozytywnie odnoszą się do współpracy ze strukturami państwa w tej dziedzinie.

2.2. WYMIAR ZEWNĘTRZNY

2.2.1. Zagrożenia

23. Rozwój technologii teleinformatycznych oraz internetu prowadzi do powstawania nowych zagrożeń zewnętrznych, takich jak cyberkryzysy i cyberkonflikty z udziałem podmiotów państwowych i niepaństwowych,

w tym także groźbę cyberwojny. Operacje w cyberprzestrzeni stanowią dziś integralną część klasycznych kryzysów i konfliktów polityczno-militarnych (wojen), w ramach ich hybrydowego charakteru.

24. Ważnym zagrożeniem zewnętrznym w cyberprzestrzeni jest cyberszpiegostwo, związane z prowadzeniem przez służby obcych państw i podmioty pozapaństwowe, w tym organizacje terrorystyczne, działań wykorzystujących specjalistyczne narzędzia i mających na celu uzyskanie dostępu do danych newralgicznych z punktu widzenia funkcjonowania struktur państwa.

25. Źródłami zagrożeń w cyberprzestrzeni są także organizacje ekstremistyczne, terrorystyczne oraz zorganizowane transnarodowe grupy przestępcze, których ataki w cyberprzestrzeni mogą mieć podłoże ideologiczne, polityczne, religijne, biznesowe i kryminalne.

2.2.2. Wyzwania (ryzyka i szanse)

26. Ryzyka może generować, szczególnie w ramach współpracy z sojusznikami i partnerami międzynarodowymi, nieodpowiednie określenie lub brak wspólnych definicji prawnych (kategorii pojęciowych) zjawisk i procesów w cyberprzestrzeni, a także zadań i działań w obszarze cyberbezpieczeństwa. Dotyczy to przede wszystkim definicji cyberkonfliktu oraz cyberwojny. Ryzyka mogą wynikać także z braku należytej symetryczności (wzajemności) we współpracy z innymi podmiotami międzynarodowymi.

27. Szansą dla wzmocnienia cyberbezpieczeństwa RP jest wykorzystanie potencjału wynikającego z członkostwa Polski w sojuszniczych strukturach obrony i ochrony cybernetycznej (NATO, UE), ukierunkowane na potrzeby państwa zaangażowanie w prace organizacji międzynarodowych, aktywność na forum gremiów zajmujących się bezpieczeństwem w cyberprzestrzeni, a także bilateralna współpraca z państwami bardziej zaawansowanymi w sprawach cyberbezpieczeństwa.

3. KONCEPCJA ZADAŃ OPERACYJNYCH W DZIEDZINIE CYBERBEZPIECZEŃSTWA

28. Zadania operacyjne ukierunkowane na osiągnięcie strategicznego celu, jakim jest zapewnienie akceptowalnego poziomu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni, powinny być realizowane przez podmioty sektora publicznego (w wymiarze krajowym i międzynarodowym), prywatnego (komercyjnego), obywatelskiego oraz w wymiarze transsektorowym.

29. Do głównych zadań sektora publicznego w wymiarze krajowym należą:

- rozpoznawanie realnych i potencjalnych źródeł zagrożeń, w tym przez międzynarodową wymianę informacji;
- ciągła analiza ryzyka w odniesieniu do ważnych obiektów infrastruktury krytycznej, również tej służącej zadaniom NATO i UE;
- działania w dziedzinie kryptografii i kryptoanalizy w celu zabezpieczenia własnych zasobów informacyjnych oraz rozpoznania potencjalnych zagrożeń ze strony wrogich państw i podmiotów niepaństwowych;
- bieżący monitoring newralgicznych punktów systemu bezpieczeństwa, szczególnie narażonych na ataki cybernetyczne, zwłaszcza poprzez wykorzystanie zespołów reagowania na incydenty bezpieczeństwa teleinformatycznego;
- audyt środków i mechanizmów cyberbezpieczeństwa z uwzględnieniem przyjętych standardów;
- przygotowanie i wdrażanie scenariuszy postępowania w razie cyberataków wymierzonych w cyfryzowane zadania państwa;
- opracowywanie i bieżąca aktualizacja – z punktu widzenia cyberbezpieczeństwa – planów reagowania kryzysowego oraz operacyjnych planów funkcjonowania w czasie zagrożenia i wojny, szczególnie pod kątem wpływu na systemy kierowania w państwie, z uwzględnieniem stosownych planów NATO i UE;
- prowadzenie aktywnej cyberobrony – i w jej ramach działań ofensywnych w cyberprzestrzeni – oraz utrzymanie gotowości do cyberwojny;

- ochrona i obrona własnych systemów teleinformatycznych i zgromadzonych w nich zasobów;
- wspieranie pozostałych kluczowych podmiotów sektora prywatnego w zakresie ich cyberbezpieczeństwa;
- przeciwdziałanie i zwalczanie cyberprzestępczości;
- bieżące działania informacyjne i edukacyjne skierowane do społeczeństwa w zakresie bezpiecznego korzystania z cyberprzestrzeni oraz informowanie o zidentyfikowanych zagrożeniach.

30. Główne zadania sektora publicznego na poziomie międzynarodowym:

- udział w międzynarodowym reagowaniu na zagrożenia w cyberprzestrzeni, przede wszystkim w strukturach NATO i Unii Europejskiej;
- międzynarodowa wymiana doświadczeń i dobrych praktyk w celu podnoszenia skuteczności działań krajowych;
- oddziaływanie na transnarodowe struktury sektora prywatnego za pośrednictwem organizacji międzynarodowych;
- wymiana informacji o podatnościach, zagrożeniach i incydentach.

31. Główne zadania sektora prywatnego:

- współpraca z sektorem publicznym w zakresie przeciwdziałania zagrożeniom cybernetycznym, w tym opracowywanie propozycji regulacji prawnych oraz samoregulacja sektora prywatnego wspierająca bezpieczeństwo w cyberprzestrzeni;
- prowadzenie audytu środków i mechanizmów cyberbezpieczeństwa z uwzględnieniem standardów bezpieczeństwa ustanowionych dla sektora publicznego i promowanych wśród podmiotów sektora prywatnego narażonych w szczególny sposób na cyberataki;
- współpraca z sektorem publicznym w zakresie wymiany informacji dotyczących istniejących oraz nowych zagrożeń dla cyberbezpieczeństwa;
- wymiana informacji o podatnościach, zagrożeniach i incydentach.

32. Główne zadania sektora obywatelskiego:

- pomoc w zapewnieniu bezpieczeństwa państwa poprzez dbałość o użytkowane systemy i urządzenia teleinformatyczne oraz samokształcenie w zakresie cyberbezpieczeństwa;
- monitorowanie propozycji zmian prawnych i organizacyjnych w celu zapewnienia ochrony praw człowieka, w tym prawa do prywatności w internecie;
- udział w społecznych inicjatywach wspierających cyberbezpieczeństwo RP (wolontariat dla cyberbezpieczeństwa, w tym także cyberobrony państwa).

33. Główne zadania transsektorowe:

- koordynacja współpracy podmiotów sektora prywatnego i publicznego oraz tworzenie mechanizmów wymiany informacji (jawnych i niejawnych), a także standardów i dobrych praktyk w obszarze cyberbezpieczeństwa (np. tworzenie przez instytucje państwowe programów certyfikacji bezpiecznego sprzętu i oprogramowania).

4. KONCEPCJA ZADAŃ PREPARACYJNYCH (PRZYGOTOWAWCZYCH) W DZIEDZINIE CYBERBEZPIECZEŃSTWA (UTRZYMANIA I ROZWOJU SYSTEMU CYBERBEZPIECZEŃSTWA RP)

34. Najważniejsze zadania preparacyjne (przygotowawcze) w obszarze cyberbezpieczeństwa to wdrożenie i rozwój systemowego podejścia do cyberbezpieczeństwa w wymiarze prawnym, organizacyjnym i technicznym. Umożliwi to obronę i ochronę systemów teleinformatycznych przy zachowaniu efektywności i elastyczności realizacji procesów oraz zadań wykonywanych z wykorzystywaniem tych systemów.

35. Działania, których celem jest przyjęcie nowych rozwiązań prawnych, dotyczą zwłaszcza:

- tworzenia podstaw ciągłego funkcjonowania systemu teleinformatycznego, zapewniającego akceptowalny poziom bezpieczeństwa, szczególnie na potrzeby podsystemu kierowania bezpieczeństwem narodowym, w tym obronnością państwa;
- zapewnienia strukturalnego wsparcia i finansowania prac badawczo-rozwojowych w zakresie tworzenia nowych, narodowych rozwiązań w dziedzinie teleinformatyki i kryptologii;
- przeglądu i analizy regulacji istniejących w sferze cyberbezpieczeństwa w celu precyzyjnego określenia potrzeby ewentualnych zmian naprawczych i uzupełniających.

36. Polski system cyberbezpieczeństwa powinien być kształtowany w zgodzie z dokumentami UE i NATO oraz innymi inicjatywami międzynarodowymi, aby był wewnętrznie spójny i kompatybilny z systemami państw sojuszniczych i organizacji międzynarodowych, których członkiem jest Polska (NATO, UE).

4.1. PODSYSTEM KIEROWANIA

37. Rada Ministrów jest odpowiedzialna za koordynację działań w zakresie cyberbezpieczeństwa na poziomie strategicznym. Wskazane jest poszerzenie zadań i kompetencji istniejącego ponadresortowego organu pomocniczego Rady Ministrów w sprawach szeroko rozumianego cyberbezpieczeństwa. Powinien on mieć kompetencje doradcze, konsultacyjne i koordynacyjne, w tym dotyczące spraw przygotowywania – w ramach współpracy podmiotów sektora publicznego i prywatnego oraz przedstawicieli społeczeństwa obywatelskiego – odpowiednich rozwiązań i standardów, a także kompetencję koordynacji współpracy międzynarodowej w obszarze cyberbezpieczeństwa. Docelowo podmiot taki mógłby stać się częścią szerszego organu ponadresortowego do spraw bezpieczeństwa narodowego[1].

38. Krokiem w kierunku osiągnięcia wysokiej efektywności systemu kierowania cyberbezpieczeństwem powinno być tworzenie technicznych centrów kompetencyjnych podporządkowanych właściwym ministrom. Ich zadaniem byłoby zapewnienie akceptowalnego poziomu bezpieczeństwa usług teleinformatycznych służących działalności gospodarczej, e-administracji i funkcjonowaniu swobód obywatelskich oraz budowie zdolności obronnych w cyberprzestrzeni.

39. W ramach utrzymania i rozwoju podsystemu kierowania cyberbezpieczeństwem szczególnie istotne jest:

- opracowywanie oraz wdrażanie zasad i procedur (również tzw. dobrych praktyk) kierowania cyberbezpieczeństwem, w tym współpracy między sektorem publicznym a prywatnym;
- ciągłe modernizowanie technicznych elementów podsystemu kierowania, w tym wdrożenie bezpiecznych środków kierowania;
- zbudowanie niezależnej sieci łączności kierowania bezpieczeństwem narodowym (np. w ramach sieci łączności rządowej) oraz zapewnienie narodowej kontroli systemów teleinformatycznych;

[1] W ramach Strategicznego Przeglądu Bezpieczeństwa Narodowego zaproponowany został Rządowy Komitet Bezpieczeństwa Narodowego (z obsługującym go Rządowym Centrum Bezpieczeństwa Narodowego w strukturze Kancelarii Prezesa Rady Ministrów), który mógłby zajmować się ponadresortową koordynacją całości spraw bezpieczeństwa narodowego.

- wypracowywanie minimalnych standardów cyberbezpieczeństwa infrastruktury krytycznej;
- opracowywanie planów ćwiczeń i szkoleń w zakresie cyberbezpieczeństwa; ponadto problematyka cyberbezpieczeństwa powinna być uwzględniana w innych przedsięwzięciach szkoleniowych, np. ćwiczeniach zarządzania kryzysowego i szkoleniach obronnych;
- określenie wymogów i celów dla programów edukacyjnych, informacyjnych oraz badawczych.

4.2. OGNIWA OPERACYJNE

40. Przygotowanie (utrzymanie i rozwój) operacyjnych ogniw systemu cyberbezpieczeństwa powinno mieć na celu zapewnienie środków i kompetencji adekwatnych do dynamicznie zmieniających się potrzeb operacyjnych. Dlatego istotne jest:

- stworzenie mechanizmów ochronnych i obronnych pozwalających na szybką adaptację do zmian środowiska bezpieczeństwa, umożliwiających reagowanie na nieprzewidziane sytuacje kryzysowe;
- uzyskanie zdolności do sprawnego zarządzania środkami cyberbezpieczeństwa;
- zapewnienie bezpiecznego przepływu informacji między operacyjnymi ogniwami systemu cyberbezpieczeństwa;
- budowanie zdolności prowadzenia aktywnych działań w cyberprzestrzeni.

41. Siły Zbrojne RP powinny dysponować zdolnościami obrony i ochrony własnych systemów teleinformatycznych i zgromadzonych w nich zasobów, a także zdolnościami do aktywnej obrony i działań ofensywnych w cyberprzestrzeni. Powinny być zintegrowane z pozostałymi zdolnościami SZ RP, aby zwiększyć narodowy potencjał odstraszania (zniechęcania, powstrzymywania) potencjalnego agresora. Powinny być też gotowe, samodzielnie i we współpracy z sojusznikami, do prowadzenia operacji ochronnych i obronnych na dużą skalę w razie cyberkonfliktu, w tym cyberwojny.

42. Konieczne jest tworzenie i wzmacnianie struktur wojskowych przeznaczonych do realizacji zadań w cyberprzestrzeni, dysponujących zdolnościami w zakresie rozpoznawania, zapobiegania i zwalczania cyberzagrożeń dla Sił Zbrojnych RP.

43. Niezbędna jest implementacja standardów NATO dotyczących cyberobrony, zwłaszcza w kontekście planowania obronnego i operacyjnego. Konieczne jest również uwzględnianie minimalnych standardów wypracowywanych przez NATO w zakresie ochrony zasobów własnych Sojuszu oraz zasobów krajowych infrastruktury krytycznej, niezbędnej do realizacji zadań wynikających z członkostwa w Sojuszu.

44. Należy rozwijać kompetencje i zdolności służb wywiadowczych oraz kontrwywiadowczych do działania w cyberprzestrzeni, umożliwiające skuteczną neutralizację aktywności obcych służb wywiadowczych i przeciwdziałanie szpiegostwu w cyberprzestrzeni.

45. Należy dążyć do uzyskania pełnych kompetencji oraz zdolności do wytwarzania polskich rozwiązań technologicznych służących zapewnieniu akceptowalnego poziomu bezpieczeństwa w cyberprzestrzeni. Strategiczne znaczenie ma uzyskiwanie zdolności i kompetencji w zakresie kontroli nad podsystemami informatycznymi uzbrojenia i innego sprzętu zagranicznej produkcji (dysponowanie kodami źródłowymi), wykorzystywanego do celów bezpieczeństwa narodowego. Istotne są zdolności i kompetencje w dziedzinie kryptologii, również w kontekście rozwoju krajowego systemu cyberbezpieczeństwa, dostosowywanego do dynamicznie zmieniających się potrzeb.

46. Potrzebny jest rozwój w pełni kontrolowanych przez państwo narzędzi teleinformatycznych i technologii, przy zachowaniu zgodności z narzędziami oraz technologiami NATO i sojuszników, na których oparta byłaby obrona i ochrona krytycznych systemów państwa.

4.3. PUBLICZNE I PRYWATNE OGNIWA WSPARCIA

47. Należy stworzyć warunki sprzyjające oddziaływaniu podmiotów prywatnych oraz obywateli na działania publiczne w zakresie cyberbezpieczeństwa. Pozwoli to osiągnąć synergię publiczno-prywatnego partnerstwa na rzecz cyberbezpieczeństwa RP.

48. Istnieje potrzeba zapewnienia odpowiednich mechanizmów współpracy oraz partnerstwa sektorów publicznego i prywatnego w dziedzinie cyberbezpieczeństwa. Wspólnej dbałości o cyberbezpieczeństwo państwa służy:

- dialog publiczno-prywatny w zakresie przygotowywania projektów legislacyjnych sprzyjających tworzeniu efektywnych zasad i procedur działania w sferze cyberbezpieczeństwa;
- budowa porozumienia w obszarze celów i zadań systemu cyberbezpieczeństwa poprzez dialog na poziomie teoretycznym oraz praktycznym;
- promowanie na poziomie krajowym oraz międzynarodowym polskich rozwiązań i produktów w dziedzinie cyberbezpieczeństwa;
- efektywna współpraca i wsparcie państwa w dziedzinie cyberbezpieczeństwa dla prywatnych operatorów elementów infrastruktury krytycznej sterowanych przy użyciu systemów teleinformatycznych oraz operatorów i dostawców usług teleinformatycznych;
- zaangażowanie przedstawicieli sektora publicznego, prywatnego oraz obywateli w proces ciągłego kształcenia i podnoszenia świadomości o zagrożeniach w obszarze cyberbezpieczeństwa.

49. Istotna jest budowa systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa oraz edukacji, w tym projektów realizowanych we współpracy ze światem nauki oraz z przedsiębiorstwami komercyjnymi. Priorytetowe w tym zakresie jest tworzenie systemu certyfikacji krajowych rozwiązań, co może sprzyjać uzyskaniu narodowej niezależności w wymiarze technicznym, programistycznym i kryptologicznym.

50. Dla długoterminowej optymalizacji systemu cyberbezpieczeństwa RP należy stworzyć odpowiednie standardy branżowe i dobre praktyki wspierające organizacje prywatne oraz niepubliczne (NGO, instytucje naukowo-badawcze) w zarządzaniu ryzykiem w obszarze cyberbezpieczeństwa, w tym poprzez dostarczanie narzędzi do identyfikacji luk w ich systemach oraz opracowanie planu ich ciągłego doskonalenia.

51. Należy opracować programy kształcenia kadr na potrzeby systemu cyberbezpieczeństwa (także ścieżki kariery pozwalające przyciągnąć najlepszych specjalistów).

52. Dla przygotowania efektywnego systemu cyberbezpieczeństwa ważne będzie opracowanie systemowych podstaw wykorzystania potencjału obywateli (niebędących członkami Sił Zbrojnych RP ani innych służb czy instytucji państwowych) dzięki współpracy publiczno-prywatnej.

53. Ważne jest prowadzenie działań informacyjnych i edukacyjnych o charakterze profilaktycznym w zakresie przygotowania obywateli do ich ochrony (w tym samoochrony) przed zagrożeniami w cyberprzestrzeni.

54. Należy uznać indywidualnych użytkowników, ich umiejętności i świadomość bezpieczeństwa, za jeden z filarów cyberbezpieczeństwa państwa, a co za tym idzie, kształtować mechanizmy przekazywania wiedzy oraz umiejętności w taki sposób, aby służyły zwiększeniu szans na osiągnięcie pożądanego poziomu cyberbezpieczeństwa.

ZAKOŃCZENIE

55. Doktryna cyberbezpieczeństwa RP – jako transsektorowy dokument wykonawczy do Strategii Bezpieczeństwa Narodowego RP – stanowi podstawę koncepcyjną do przygotowania i realizacji skoordynowanych w skali państwa działań na rzecz cyberbezpieczeństwa RP poszczególnych sektorów publicznych i sektora prywatnego.

56. Rekomendacje niniejszej Doktryny przeznaczone są do odpowiedniego wykorzystania przez wszystkie podmioty publiczne i prywatne odpowiedzialne za planowanie, organizowanie i realizowanie zadań w dziedzinie cyberbezpieczeństwa.

57. Treść doktryny powinna być rozwinięta przede wszystkim w Polityczno-Strategicznej Dyrektywie Obronnej oraz w kolejnej edycji Strategii (Programu) Rozwoju Systemu Bezpieczeństwa Narodowego, a także w planach zarządzania kryzysowego oraz operacyjnych planach funkcjonowania struktur państwa w czasie zagrożenia i wojny, jak również w programach rozwoju sił zbrojnych i programach pozamilitarnych przygotowań obronnych.

Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej
została wydana przez Biuro Bezpieczeństwa Narodowego
22 stycznia 2015 r.

Przygotowanie do druku, druk:
Centrum Poligrafii Sp. z o.o.
www. jakubiccy.com.pl

ISBN: 978-83-60846-25-4