Magdalena Adamczuk
Krzysztof Liedel

Doktryna cyberbezpieczeństwa RP

Doktryna cyberbezpieczeństwa RP jest pierwszym w Polsce dokumentem określającym strategiczne kierunki prac oraz stanowiącym wspólną, koncepcyjną podstawę działań w obszarze cyberbezpieczeństwa zarówno podmiotów administracji publicznej, służb bezpieczeństwa i porządku publicznego, sił zbrojnych, jak i sektora prywatnego oraz obywateli. Jest to ważny dokument, z którym powinien zapoznać się i wdrożyć zawarte w nim postulaty każdy z wymienionych podmiotów realizujących zadania w cyberprzestrzeni. Warto w tym miejscu wspomnieć o roli cyberprzestrzeni i znaczeniu, jakie odgrywa w kompleksowym systemie bezpieczeństwa państwa.

We współczesnym świecie bezpieczeństwo państwa (w sferze militarnej i pozamilitarnej, zewnętrznej i wewnętrznej) zyskało dodatkowy wymiar, jakim oprócz lądu, wody, powietrza i przestrzeni kosmicznej jest cyberprzestrzeń. Przyniosło to m.in. nowe koncepcje konfliktów (jak cyberwojna) oraz realne zagrożenia, np. cyberterrorystyczne.

Głównym determinantem postrzegania bezpieczeństwa w cyberprzestrzeni jako jednego z priorytetów działań państw jest to, że większość zagrożeń uznanych za tradycyjne znajdzie swoje odzwierciedlenie w świecie wirtualnym, co będzie wymuszać dostosowywanie procedur reagowania do zmieniających się warunków i doskonalenie systemów tego obszaru bezpieczeństwa w praktycznym wymiarze.

Cyberprzestrzeń rozumiana jako element globalnego bezpieczeństwa stanowi wyzwanie dla całej społeczności międzynarodowej. W związku z tym cyberbezpieczeństwo wymaga ciągłego doskonalenia zdolności reagowania na zaistniałe zagrożenia oraz ochrony zasobów państwa w cyberprzestrzeni w ramach współpracy instytucjonalno-prawnej dotyczącej zarówno sfery militarnej jak też cywilnej.

Potrzeba bezpiecznego i prawidłowego funkcjonowania cyberprzestrzeni sprawia, że dbałość o właściwe funkcjonowanie tego obszaru staje się priorytetem w krajowej polityce bezpieczeństwa, który znajduje swoje odzwierciedlenie w dokumentach strategicznych. Warto zwrócić uwagę na to, że większość krajów europejskich, Stany Zjednoczone czy Rosja już od wielu lat dostrzegają realne zagrożenia, które niesie za sobą coraz powszechniejsze funkcjonowanie każdej sfery życia w cyberprzestrzeni. Podejmowane są próby stworzenia efektywnych systemów przeciwdziałania cyberzagrożeniom na poziomie strategicznym, prawnym i instytucjonalnym.

Konieczność tworzenia przez państwa w swych strukturach instytucji i komórek odpowiedzialnych za przeciwdziałanie zagrożeniom występującym w cyberprzestrzeni i ich zwalczanie wynika przede wszystkim ze zmiany zarówno formy potencjalnych zagrożeń dla bezpieczeństwa państw, jak i uwarunkowań pola walki w przypadku zaistnienia konfliktu.

Należy też wspomnieć, że zapisy *Strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*[1] zobowiązują państwa

[1] Wspólny Komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-społecznego i Komitetu regionów - Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna

członkowskie do przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i informacji[2] określającej cele strategiczne i konkretne środki polityczne i regulacyjne, mające na celu osiągnięcie i utrzymanie wysokiego poziomu bezpieczeństwa sieci i informacji, a także wyznaczenia właściwych krajowych organów w dziedzinie bezpieczeństwa sieci i informacji, dysponujących odpowiednimi środkami finansowymi i zasobami ludzkimi, aby w przypadku wystąpienia incydentów i zagrożeń w dziedzinie bezpieczeństwa sieci i informacji odpowiednio postępować i reagować.

Na tle krajów unijnych Polska jest dopiero na początku budowy zintegrowanego systemu bezpieczeństwa cyberprzestrzeni. Jednym z jego elementów jest przyjęta przez Komitet Stały Rady Ministrów w dniu 25 czerwca 2013 r. *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*[3]. Zawiera ona spójną koncepcję systemu zarządzania cyberprzestrzenią oraz w racjonalny sposób definiuje zależności między poszczególnymi organami i instytucjami państwowymi oraz ich wyspecjalizowanymi komórkami odpowiedzialnymi za zapewnienie odpowiedniego poziomu bezpieczeństwa teleinformatycznego w cyberprzestrzeni. Nie jest to jednak dokument o charakterze transsektorowym, a jedynie rządowy.

Jednym z najważniejszych wyzwań w opracowaniu skutecznych narzędzi do przeciwdziałania zagrożeniom jest efektywne, szczegółowe i logiczne ich opisanie w kontekście rzeczywistości prawnej i administracyjnej. Zasadniczym krokiem w kierunku dokonania takiego opisu w polskim systemie prawnym była przeprowadzona z inicjatywy Prezydenta RP nowelizacja ustaw[4] wprowadzająca do polskiego systemu prawnego definicję cyberprzestrzeni[5], a także prace nad opracowaniem doktryny cyberbezpieczeństwa RP.

O znaczeniu cyberbezpieczeństwa w działaniach na poziomie kraju, dotyczących zwłaszcza Sił Zbrojnych, świadczy m.in. wypowiedź Prezydenta RP, który wskazał na

> (…) konieczność pilnego i mądrze zorganizowanego przygotowania się do podjęcia chyba dziś najbardziej perspektywicznego zadania, jakim jest budowa i rozwijanie zdolności do działania w cyberprzestrzeni. Przewiduję, że w kolejnym cyklu planistycznym uczynimy to najważniejszym priorytetem rozwoju sił zbrojnych. (…) Cyberprzestrzeń to sfera, która dopiero się kształtuje. Powstają nowe cybercentra, cyberdowództwa, cyberstrategie – np. wyprzedzającego ataku. Niektórzy mówią wręcz, iż stajemy się dziś świad-

i chroniona cyberprzestrzeń, 7 lutego 2013 r. [online], https://mac.gov.pl/files/wp-content/uploads/2013/03/JOIN2013-1-2.pdf [dostęp: 10 III 2015].

[2] „Sieci i systemy informatyczne" w myśl *Dyrektywy Parlamentu Europejskiego i Rady w sprawie w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii* oznaczają: sieci łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE, oraz b) wszelkie urządzenia lub grupy połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych komputerowych, jak również c) dane komputerowe przechowywane, przetwarzane, odzyskiwane lub przekazywane w celu ich eksploatacji, użycia, ochrony lub utrzymania.

[3] http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html [dostęp: 10 III 2015].

[4] Ustaw: o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom RP, o stanie wyjątkowym oraz o stanie klęski żywiołowej przez wprowadzenie do ich treści zapisów dotyczących pojęcia cyberprzestrzeni - *Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw* (Dz.U. Nr 222, poz. 1323).

[5] *Przez cyberprzestrzeń, o której mowa w ust. 1, rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*, tamże, art. 1.

kami swoistego cyberwyścigu zbrojeń. Oczywiście jest to wielkie wyzwanie, lecz również szansa dla naszych Sił Zbrojnych. Szansa, której nie można zaprzepaścić[6].

Po roku intensywnych prac prowadzonych w Biurze Bezpieczeństwa Narodowego z udziałem przedstawicieli administracji publicznej, środowiska akademickiego, organizacji pozarządowych oraz sektora prywatnego powstała *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*[7]. Punktem wyjścia do jej opracowania były wytyczne *Strategii Bezpieczeństwa Narodowego RP* dotyczące cyberbezpieczeństwa[8], a także zapisy *Polityki Ochrony Cyberprzestrzeni RP* oraz *Strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*. Uwzględniono również prace nad *Dyrektywą Parlamentu Europejskiego i Rady w sprawie w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii*, która przewiduje pewne wymogi dotyczące przyjęcia i zawartości krajowych strategii dotyczących cyberbezpieczeństwa.

Podkreślenia wymaga rozróżnienie, jakiego dokonano w toku prac nad dokumentem dotyczące pojęć: bezpieczeństwo Polski w cyberprzestrzeni[9] oraz bezpieczeństwo cyberprzestrzeni RP[10], co pozwoliło sprecyzować obszary objęte analizą i wypracowaniem właściwych zapisów *Doktryny w odniesieniu do koncepcji zadań i kompetencji podmiotów zaangażowanych w obronę i ochronę cyberprzestrzeni.*

Doktryna cyberbezpieczeństwa wskazuje strategiczne kierunki działań dla zapewnienia pożądanego poziomu 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, siły zbrojne, służby bezpieczeństwa i porządku publicznego, sektor prywatny oraz obywateli. Dzięki temu *Doktryna cyberbezpieczeństwa* może stanowić punkt wyjścia do dalszych prac na rzecz wzmocnienia bezpieczeństwa Polski i Polaków w cyberprzestrzeni[11].

---

[6] http://www.bbn.gov.pl/pl/wydarzenia/4471,Wystapienie-Prezydenta-RP-podczas-odprawy-rozliczeniowo-koordynacyjnej-kierownic.print [dostęp: 15 II 2015].

[7] Zatwierdzona przez RBN w 12 I 2015 r. i opublikowana przez Biuro Bezpieczeństwa Narodowego 22 I 2015 r.

[8] 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, szczególnie wchodzących w skład sektorów: finansowego, energetycznego i ochrony zdrowia. Zob. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* [online], http://www.bbn.gov.pl/ftp/SBN%20RP.pdf, s. 34 [dostęp: 3 II 2015].

[9] 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, *Doktryna cyberbezpieczeństwa RP* [online], http://www.bbn.gov.pl/pl/wydarzenia/6336,Doktryna-cyberbezpieczenstwa-RP.html?search=88442 [dostęp: 25 I 2015].

[10] 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, *Doktryna cyberbezpieczeństwa RP* [online], http://www.bbn.gov.pl/pl/wydarzenia/6336,Doktryna-cyberbezpieczenstwa-RP.html?search=88442 [dostęp: 25 I 2015].

[11] Przesłanie Prezydenta RP – *Doktryna Cyberbezpieczeństwa RP* [online], http://www.bbn.gov.pl/ftp/

W *Doktrynie* przede wszystkim określono cel strategiczny, który osiąga się przez realizację zadań o charakterze operacyjnym i preparacyjnym (przygotowawczym) w dziedzinie cyberbezpieczeństwa. Zawiera ocenę zagrożeń, ryzyk i szans w dynamicznie rozwijającym się środowisku cyberbezpieczeństwa[12] (w jego wymiarze zewnętrznym i wewnętrznym, krajowym i międzynarodowym), identyfikuje najważniejsze zadania operacyjne dla zapewnienia cyberbezpieczeństwa w sektorze publicznym, prywatnym i obywatelskim oraz rekomenduje zadania preparacyjne mające na celu doskonalenie, rozwój i transformację systemu cyberbezpieczeństwa, z uwzględnieniem podsystemu kierowania oraz publicznych i prywatnych ogniw wykonawczych.

Na szczególną uwagę zasługują pojawiające się w *Doktrynie* **nowe cenne postulaty** i zadania zarówno dla sektora prywatnego, państwowego, jak i dla obywateli, które dotychczas nie były definiowane na poziomie krajowym, a także kierunki współdziałania w tym obszarze.

Po pierwsze można wśród nich wyróżnić **wypracowanie mechanizmów wzajemnego oddziaływania sektorów publicznego i prywatnego** w zakresie dbałości o cyberbezpieczeństwo państwa, a szczególnie:

a) efektywną współpracę i wsparcie państwa w dziedzinie cyberbezpieczeństwa dla prywatnych operatorów elementów infrastruktury krytycznej sterowanych przy użyciu systemów teleinformatycznych oraz operatorów i dostawców usług teleinformatycznych,
b) postulat stworzenia standardów bezpieczeństwa wdrażanych na poziomie państwowym oraz przenoszonych na najważniejsze z punktu widzenia cyberbezpieczeństwa elementy sektora prywatnego,
c) rozszerzenie współpracy w sferze ochrony przed atakami na sektor prywatny, co ma ogromne znaczenie w kontekście elementów infrastruktury krytycznej będących własnością prywatnych kontrahentów, a mających często strategiczne znaczenie dla bezpieczeństwa kraju,
d) publiczno-prywatny dialog przy przygotowaniu projektów legislacyjnych dotyczących sfery cyberbezpieczeństwa, który przyczyni się do wspólnej dbałości o cyberbezpieczeństwo państwa.

Na uwagę zasługuje opracowany przez twórców Doktryny podział na zadania operacyjne i preparacyjne, który pozwala na systemowe uporządkowanie niezbędnych działań. Odnosząc go do postulatu **wypracowania mechanizmów wzajemnego oddziaływania sektorów publicznego i prywatnego** główne działania zdefiniowano jako:

dok/01/DCB.pdf [dostęp: 25 I 2015].

[12] Środowisko 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 cyberbezpieczeństwa) sprzyjające realizacji interesów oraz osiąganiu celów podmiotu w dziedzinie cyberbezpieczeństwa; ryzyka cyberbezpieczeństwa – możliwości negatywnych dla danego podmiotu skutków własnego działania w cyberprzestrzeni; zagrożenia cyberbezpieczeństwa – pośrednie lub bezpośrednie zakłócające lub destrukcyjne oddziaływania na podmiot w cyberprzestrzeni. http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html [dostęp: 3 II 2015].

Zadania operacyjne:

- 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.

Zadania przygotowawcze:

- dialog publiczno-prywatnego 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.

Po drugie w *Doktrynie* dostrzeżono też **dylemat, jakim jest próba zapewnienia równowagi między środkami bezpieczeństwa a swobodami obywatelskimi**. Podkreślono, że 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.

Po trzecie, co szczególnie istotne, po raz pierwszy nastąpiło oficjalne stwierdzenie **konieczności prowadzenia** nie tylko działań defensywnych, lecz także **działań ofensywnych** na poziomie kraju, które, będąc celami operacyjnymi, zostały określone jako zwalczanie (dezorganizowanie, zakłócanie i niszczenie) źródeł zagrożeń (aktywna obrona oraz działania ofensywne). Zadaniem preparacyjnym dla podsystemu operacyjnego i wsparcia jest, według *Doktryny,* nabycie zdolności do samodzielnego prowadzenia defensywnych (ochronnych i obronnych) oraz ofensywnych cyberoperacji, a także udzielania i przyjmowania wsparcia w ramach działań sojuszniczych. Sektor prywatny również powinien posiadać zdolności do prowadzenia aktywnej cyberobrony – w ramach działań ofensywnych w cyberprzestrzeni – oraz utrzymania gotowości do cyberwojny.

O działaniach ofensywnych wspomniano również przy definiowaniu zdolności i zadań Sił Zbrojnych RP (ogniw operacyjnych), które 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 one być zintegrowane z pozostałymi zdolnościami SZ RP, aby zwiększyć narodowy potencjał odstraszania (zniechęcania, powstrzymywania) potencjalnego agresora. Po-

winny być one też gotowe, samodzielnie i we współpracy z sojusznikami, do prowadzenia operacji ochronnych i obronnych na dużą skalę w razie cyberkonfliktu, w tym cyberwojny.

Kolejnym (czwartym) i niezwykle cennym postulatem, który dotychczas nie był realizowany z dostatecznym naciskiem, jest **inwestowanie w narodowe rozwiązania w dziedzinie cyberbezpieczeństwa,** szczególnie w dziedzinie kryptologii. W obecnych realiach jest to konieczne działanie przekładające się na uzyskanie pełnych kompetencji oraz zdolności do wytwarzania polskich rozwiązań technologicznych służących zapewnieniu akceptowalnego poziomu bezpieczeństwa w cyberprzestrzeni oraz sprawowanie suwerennej kontroli nad najważniejszymi systemami komunikacji, dowodzenia i kontroli w państwie, np. wysoce zinformatyzowanymi systemami walki i wsparcia. Biorąc pod uwagę polski potencjał naukowy w dziedzinie nauk informatycznych i matematycznych, stwarza to szansę w sferze cyberbezpieczeństwa.

Słusznie podkreślono, że zadaniem operacyjnym sektora prywatnego są niewątpliwie działania w dziedzinie kryptografii i kryptoanalizy w celu zabezpieczenia własnych zasobów informacyjnych oraz rozpoznania potencjalnych zagrożeń ze strony wrogich państw i podmiotów niepaństwowych.

W kontekście rozwoju systemowego podejścia do cyberbezpieczeństwa w wymiarze prawnym niezbędne jest zapewnienie strukturalnego wsparcia i finansowania prac badawczo-rozwojowych w zakresie tworzenia nowych, narodowych rozwiązań w dziedzinie teleinformatyki i kryptologii.

W ocenie ekspertów z zakresu technologii informacyjnych określone w *Doktrynie* zadanie preparacyjne ogniw wsparcia mówiące o strategicznym znaczeniu uzyskiwania zdolności i kompetencji w zakresie kontroli nad podsystemami informatycznymi sterującymi uzbrojeniem i sprzętem zagranicznej produkcji (dysponowanie kodami źródłowymi), wykorzystywanymi dla celów bezpieczeństwa narodowego, jest pewnego rodzaju przełomem w myśleniu o cyberbezpieczeństwie w kraju.

Piątą, lecz nie mniej istotną propozycją jest **stworzenie krajowego ponadresortowego organu koordynacji działań.** W związku z obserwowanym wzrostem instytucjonalizacji płaszczyzny działań dotyczących cyberprzestrzeni, większość dokumentów strategicznych krajów europejskich (i nie tylko) przewiduje utworzenie wyspecjalizowanych instytucji, które w sposób zintegrowany będą się zajmować cyberzagrożenieniami wpływającymi na właściwe funkcjonowanie kraju. Zawierają one także propozycje stworzenia krajowych ośrodków koordynacji, których zadanie ma polegać na organizowaniu współpracy pomiędzy poszczególnymi podmiotami, ułatwianiu wymiany informacji oraz promowaniu dobrych praktyk w dziedzinie bezpieczeństwa.

W *Doktrynie*, z racji tego, że w myśl zapisów Strategii Bezpieczeństwa Narodowego, Rada Ministrów jest odpowiedzialna za koordynację działań w zakresie cyberbezpieczeństwa na poziomie strategicznym – pojawia się postulat stworzenia lub poszerzenia zadań i kompetencji istniejącego ponadresortowego organu pomocniczego Rady Ministrów. Powinien on posiadać kompetencje doradcze, konsultacyjne i koordynacyjne, w tym dotyczące spraw przygotowywania odpowiednich rozwiązań i standardów (w ramach współpracy podmiotów sektora publicznego i prywatnego oraz przedstawicieli społeczeństwa obywatelskiego), a także kompetencję koordynacji współpracy międzynarodowej w obszarze cyberbezpieczeństwa. Docelowo podmiot taki mógłby stać się częścią szerszego organu ponadresortowego do spraw bezpieczeństwa narodowego[13].

[13] W ramach Strategicznego Przeglądu Bezpieczeństwa Narodowego zaproponowano utworzenie Rządowego Komitetu Bezpieczeństwa Narodowego (z obsługującym go Rządowym Centrum Bezpieczeństwa

Innym (6), wartym wspomnienia postulatem jest konieczność ciągłego **podnoszenia świadomości obywatelskiej w zakresie cyberbezpieczeństwa** oraz **wykorzystanie potencjału obywateli w ramach cyberobrony i cyberochrony kraju**. Niezwykle cenna jest także idea zaangażowania przedstawicieli sektora publicznego, prywatnego oraz obywateli w proces ciągłego kształcenia i podnoszenia świadomości o zagrożeniach w obszarze cyberbezpieczeństwa przez intensyfikację działań edukacyjnych a także określenie wymogów i celów dla programów edukacyjnych, informacyjnych oraz badawczych (w formie szkoleń i kampanii społecznych).

Zupełnie nowym pomysłem jest opracowywanie systemowych podstaw stworzenia swego rodzaju wolontariatu na rzecz cyberobrony państwa.

Ostatnim (7) zagadnieniem jest **budowa systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa** realizowanych we współpracy ze światem nauki oraz z przedsiębiorstwami komercyjnymi. Co ciekawe, za priorytetowe w tym zakresie uznano tworzenie systemu certyfikacji krajowych rozwiązań, który w perspektywie ma sprzyjać uzyskaniu narodowej niezależności w wymiarze technicznym, programistycznym i kryptologicznym.

Doktryna cyberbezpieczeństwa RP nie zawiera planu działań, jakie należy podjąć, aby osiągnąć założenia i zadania z niej wynikające. Nie jest to rolą dokumentu strategicznego. Jako transsektorowy dokument wykonawczy do Strategii Bezpieczeństwa Narodowego RP powinien on być wykorzystywany przez struktury rządowe, samorządowe, podmioty sektora prywatnego, a także obywateli w organizowaniu bezpiecznego funkcjonowania w cyberprzestrzeni.

Zgodnie z zapowiedziami rozwinięcie *Doktryny* ma znajdować się m.in. w Polityczno-Strategicznej Dyrektywie Obronnej, w planach zarządzania kryzysowego oraz operacyjnych planach funkcjonowania struktur państwa w czasie zagrożenia i wojny, a także w programach rozwoju sił zbrojnych i programach pozamilitarnych przygotowań obronnych.

Zaznaczyć też należy, że będzie ona w zależności od sytuacji strategicznej aktualizowana wraz z kolejnymi edycjami Strategicznego Przeglądu Bezpieczeństwa Narodowego oraz nowelizacjami Strategii Bezpieczeństwa Narodowego.

Stworzenie *Doktryny* jest wyjątkowo istotną inicjatywą w budowie zintegrowanego i transsektorowego systemu bezpieczeństwa RP w cyberprzestrzeni. Jej zapisy zwracają uwagę na problemy i zadania konieczne do zrealizowania zarówno w sektorze publicznym, prywatnym, jak i dotyczące optyki organizacji pozarządowych w kontekście obywatelskim.

Pomimo, że *Doktryna* nie ma umocowania prawnego i nie nakłada na służby i instytucje obowiązku wypełnienia jej zapisów, należy mieć nadzieję, że stanie się ona istotnym „drogowskazem" w osiąganiu pożądanego i adekwatnego poziomu bezpieczeństwa kraju w cyberprzestrzeni.

Warto podkreślić aktywność BBN w rozumieniu i dostrzeganiu zagrożeń i zmian zachodzących w środowisku bezpieczeństwa. Poza inicjowaniem prac dotyczących wyzwań i zagrożeń cyberprzestrzeni (które niewątpliwe zmieniają współczesne pole walki i sposób prowadzenia konfliktów zbrojnych), wychodząc naprzeciw współczesnym wyzwaniom, na polecenie Prezydenta RP BBN rozpoczęło prace i analizy dotyczące współczesnych konfliktów hybrydowych, w tym bezpieczeństwa informacyjnego, a zwłaszcza walki informacyjnej.

Narodowego w strukturze Kancelarii Prezesa Rady Ministrów), który mógłby zajmować się ponadresortową koordynacją całości spraw bezpieczeństwa narodowego.