Zeszyty Naukowe AON nr 2 (103) 2016
ISSN 0867–2245

INSTYTUCJONALNE PODMIOTY OCHRONY MILITARNEJ CYBERPRZESTRZENI PAŃSTWA

dr Andrzej NOWAK
Akademia Obrony Narodowej

Streszczenie

Artykuł został poświęcony problematyce ochrony cyberprzestrzeni realizowanej na potrzeby militarne. Zidentyfikowano w nim główne podmioty działające w tym obszarze, omawiając zadania każdego z nich, jak również zasady działania i podejmowanej współpracy. Uwaga została skupiona na pięciu zasadniczych podmiotach, tj. Pełnomocniku Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni, Narodowym Centrum Kryptografii, Inspektoracie Systemów Informacyjnych, Resortowym Centrum Zarządzania Sieciami i Usługami Teleinformatycznymi oraz Systemie Reagowania na Incydenty Komputerowe. W załączniku do artykułu przedstawiono w formie tabelarycznej przebieg budowy instytucjonalnej ochrony cyberprzestrzeni militarnej państwa.

Słowa kluczowe: cyberbezpieczeństwo, bezpieczeństwo informacyjne, ochrona militarna cyberprzestrzeni

Wprowadzenie

Współcześnie trudno nie zgodzić się z tezą, że bezpieczeństwo informacyjne jest jednym z wielu komponentów potencjału obronnego państwa, a co za tym idzie, jednym z podsystemów operacyjnych wsparcia bezpieczeństwa narodowego. Jeśli główny element tego systemu stanowią Siły Zbrojne RP[1], to komponent bezpieczeństwa informacyjnego jest jednym z najważniejszych czynników kształtowania tego systemu.

Zauważyć należy, że bezpieczeństwo informacyjne (cyberbezpieczeństwo) nie ma wymiaru przestrzennego – podporządkowuje się ono nieco innym regułom oraz czynnikom, które powstały dopiero w krótkim okresie końca XX wieku. Ponadto nie ulega dziś wątpliwości, że sieć internetowa jest ukształtowana w złożony sposób,

1 Strategia Obronności Rzeczypospolitej Polskiej, Strategia sektorowa do Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2009, s. 9.

gdyż jest podobna do globalnego państwa i globalnego społeczeństwa, które jest sterowane i kontrolowane.

Z uwagi na uzależnienie wielu dziedzin funkcjonowania państwa, w tym także obszaru militarnego, od systemów informatycznych, istotne staje się objęcie badaniami obszaru cyberbezpieczeństwa oraz ochrony cyberprzestrzeni państwa. Najwyższa Izba Kontroli negatywnie ocenia działania podejmowane przez państwo na rzecz ochrony cyberprzestrzeni. Taka ocena nie powinna budzić wątpliwości, gdyż od dawna dostrzec można brak organu koordynującego zagadnienia szeroko rozumianego cyberbezpieczeństwa oraz kunktatorskie podejście do tej kwestii. Analizując działania prowadzone w ramach ochrony cyberprzestrzeni, inspektorzy NIK stwierdzili, że „działania podmiotów państwowych związane z ochroną cyberprzestrzeni były prowadzone w sposób rozproszony i bez spójnej wizji systemowej. Sprowadzały się one do doraźnego, ograniczonego reagowania na bieżące wydarzenia oraz biernego oczekiwania na regulacje unijne”[2].

Co więcej, w ocenie NIK znalazł się zarzut, iż „Podmioty państwowe nie prowadzą spójnych i systemowych działań związanych z ochroną cyberprzestrzeni RP. Jako działania pozytywne i wzory dobrych praktyk można wskazać jedynie «fragmentaryczne» działania poszczególnych instytucji, np. powołanie i utrzymywanie na wysokim poziomie Zespołów CERT przez ABW, MON oraz NASK”[3].

Z przeprowadzonej analizy wynika, że w Ministerstwie Obrony Narodowej można zidentyfikować następujące podmioty zaangażowane na rzecz ochrony cyberprzestrzeni:

1. Pełnomocnik MON ds. Bezpieczeństwa Cyberprzestrzeni,
2. Narodowe Centrum Kryptologii,
3. Inspektorat Systemów Informacyjnych Dowództwa Operacyjnego,
4. Resortowe Centrum Zarządzania Sieciami i Usługami Teleinformatycznymi.

Celem artykułu jest zaprezentowanie wyników badań z zakresu identyfikacji krajowych podmiotów zaangażowanych na rzecz ochrony cyberprzestrzeni wykorzystywanej na potrzeby militarne oraz rozwiązanie problemu badawczego, który zawiera się w pytaniu: jakie są instytucjonalne podmioty ochrony cyberprzestrzeni wykorzystywane przez MON?

Dla właściwego rozwiązania określonego problemu badawczego konieczne jest wyjaśnienie zasadniczych zagadnień, stanowiących o istocie przedmiotu badań. W tym kontekście do rozstrzygnięcia pojawiają się kolejne pytania problemowe:

1. Jakie działania na rzecz ochrony cyberprzestrzeni realizuje Pełnomocnik MON ds. Bezpieczeństwa Cyberprzestrzeni?

2. Jakie działania na rzecz ochrony cyberprzestrzeni realizuje Narodowe Centrum Kryptografii?

2 Zob. *NIK o bezpieczeństwie w cyberprzestrzeni*, dostępne na stronie: https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html [dostęp: 30.06.2015].

3 Zob.: http://www.gazetaprawna.pl/artykuly/838061,ochrona-cyberprzestrzeni-w-polsce-jest-w-fatalnym-stanie.html [dostęp: 16.05.2015].

3. Jakie działania na rzecz ochrony cyberprzestrzeni realizuje Inspektorat Systemów Informacyjnych Dowództwa Operacyjnego?

4. Jakie działania na rzecz ochrony cyberprzestrzeni realizuje Resortowe Centrum Zarządzania Sieciami i Usługami Teleinformatycznymi?

5. Jakie działania na rzecz ochrony cyberprzestrzeni realizuje System Reagowania na Incydenty Komputerowe?

6. Jakie inne podmioty realizują zadania na rzecz ochrony cyberprzestrzeni wykorzystywanej na potrzeby militarne?

Rozwiązania powyższych zagadnień szczegółowych zawarte są w treści niniejszego opracowania.

Pełnomocnik MON do spraw Bezpieczeństwa Cyberprzestrzeni[4]

Głównym organem działającym na rzecz ochrony cyberprzestrzeni wykorzystywanej na potrzeby militarne jest Pełnomocnik Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni[5], który jest mianowany przez Ministra Obrony Narodowej. W strukturze instytucjonalnej funkcjonuje on od 2012 roku, kiedy to został powołany decyzją MON określającą zakres przysługujących mu uprawnień.

Zgodnie z właściwym aktem prawnym pełnomocnik jest organem koordynującym przedsięwzięcia przewidziane dla MON w sprawach bezpieczeństwa w cyberprzestrzeni, w odniesieniu do wszystkich komórek organizacyjnych MON i jednostek organizacyjnych resortu obrony narodowej, z wyłączeniem zadań zastrzeżonych dla pełnomocników ds. ochrony informacji niejawnych określonych odrębnymi przepisami. W kompetencjach pełnomocnika spoczywa również inicjowanie oraz wspieranie działań komórek organizacyjnych Ministerstwa i jednostek organizacyjnych resortu w obszarze osiągania zdolności do zapewnienia bezpieczeństwa cyberprzestrzeni całego resortu obrony narodowej. Pełnomocnik jest ponadto upoważniony do sprawowania nadzoru nad realizacją zadań wynikających z aktów prawnych, polityk i programów rządowych dotyczących zapewnienia bezpieczeństwa cyberprzestrzeni.

W gestii pełnomocnika spoczywa również obowiązek ustanowienia spójnego, współdzielonego systemu informacyjnego o bieżącym stanie oraz zagrożeniach w cyberprzestrzeni. Współpraca takiego systemu musi odbywać się z zachowaniem warunków bezpieczeństwa informacji oraz kompetencji komórek i jednostek organizacyjnych ministerstwa, jak i całego resortu.

Omawiany podmiot jest także organem reprezentującym resort obrony narodowej w zakresie bezpieczeństwa w cyberprzestrzeni poza granicami kraju, w szczególności w pracach kierowniczych gremiów Organizacji Traktatu Północnoatlantyc-

4 Decyzja nr 38/MON Ministra Obrony Narodowej z dnia 16 lutego 2012 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni.

5 Dalej „pełnomocnik" [przyp. red.].

kiego i Unii Europejskiej. W celu realizacji powierzonych zamiarów pełnomocnik ma możliwość współpracy ze Służbą Kontrwywiadu Wojskowego w zakresie kreowania spójnego, jednolitego i efektywnego systemu zarządzania bezpieczeństwem cyberprzestrzeni dla resortu obrony narodowej.

Nie bez znaczenia jest także fakt, że pełnomocnik jest odpowiedzialny za przygotowanie dla MON corocznego raportu o stanie bezpieczeństwa w cyberprzestrzeni. W celu opracowania takiej diagnozy konieczna jest współpraca pomiędzy pełnomocnikiem a innymi podmiotami działającymi w sferze militarnej, tj. szefem Sztabu Generalnego Wojska Polskiego, szefem Służby Kontrwywiadu Wojskowego i Pełnomocnikiem Ministra Obrony Narodowej do spraw Ochrony Informacji Niejawnych. Jednocześnie pełnomocnik wykonuje zadania we współdziałaniu z właściwymi komórkami organizacyjnymi Ministerstwa Obrony Narodowej, ze szczególnym uwzględnieniem Zarządu Kierowania i Dowodzenia – P6 Sztabu Generalnego Wojska Polskiego. Wszystkie współpracujące podmioty zgodnie z właściwością rzeczową zobowiązane są do udzielenia wszelkiej niezbędnej pomocy, w szczególności przez udostępnianie informacji niezbędnych do realizacji jego zadań.

W sytuacjach wymagających szerszych konsultacji pełnomocnik ma możliwość występowania do komórek organizacyjnych MON i jednostek organizacyjnych resortu obrony narodowej z wnioskami dotyczącymi cyberprzestrzeni, czyli o rozpatrzenie oraz zajęcie stanowiska w sprawie pozostającej w ich właściwości.

Nie bez znaczenia jest także fakt, że w sprawach wymagających współpracy ze środowiskiem niemilitarnym, omawiany organ ma prawo do podjęcia współpracy z innymi podmiotami, np. organami administracji publicznej, organizacjami pozarządowymi oraz podmiotami krajowymi realizującymi zadania dotyczące bezpieczeństwa cyberprzestrzeni.

Od 12 stycznia 2015 roku, decyzją Ministra Obrony Narodowej, funkcja pełnomocnika powierzona została podsekretarzowi stanu w MON – Bartłomiejowi Grabskiemu[6]. Obsługa merytoryczna i administracyjna dla omawianego organu zapewniana jest przez Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych.

Narodowe Centrum Kryptografii

W strukturze instytucjonalnej działającej na rzecz ochrony cyberprzestrzeni wykorzystywanej na potrzeby militarne odpowiednie zadania realizuje także Narodowe Centrum Kryptografii (NCK). Organ ten został utworzony na mocy zarządzenia MON z 29 kwietnia 2013 roku. Zgodnie z zapisami zawartymi w przedmiotowym

6 Decyzja nr 490/MON Ministra Obrony Narodowej z dnia 16 grudnia 2015 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni.

dokumencie do zadań NCK należy konsolidacja kompetencji i zasobów resortu obrony narodowej w obszarze kryptologii.

Działania te w praktyce sprowadzają się do kwestii takich jak realizacja zadań związanych z prowadzeniem badań, projektowaniem, budową, wdrażaniem, użytkowaniem oraz ochroną narodowych technologii kryptologicznych, jak również wytwarzaniem nowych produktów dla państwa przez zespolenie potencjału naukowego i przemysłowego w obszarze zaawansowanych technologii informatycznych i kryptograficznych. Co więcej, omawiany organ odpowiada za realizację zadań w zakresie kryptologii zleconych, za pośrednictwem Ministra Obrony Narodowej, przez inne organy państwa lub administracji publicznej oraz innych zadań zleconych przez ministra właściwego w sprawach obrony narodowej.

W obszarze odpowiedzialności NCK znajduje się ponadto osiągnięcie oraz utrzymanie potencjału i kompetencji w zakresie:

- budowy urządzeń i narzędzi kryptograficznych służących do przetwarzania informacji niejawnych oraz innych – posiadających zdolności kryptograficzne;
- wytworzenia rozwiązań do pełnej ochrony i zabezpieczenia informacji i przekazu wraz z możliwością przygotowania zasad wdrożenia i produkcji;
- wypracowania metodologii i rozwiązań naukowo-technicznych w obszarze badania odporności rozwiązań kryptograficznych na kompromitację;
- zapewnienia warunków do prowadzenia badań, także we współpracy z jednostkami organizacyjnymi posiadającymi uprawnienia do nadawania stopnia naukowego doktora w dziedzinach nauki związanych w sposób bezpośredni lub pośredni z kryptologią;
- organizacji biblioteki i zbioru opracowań, w tym zawierających informacje niejawne, dotyczących zaawansowanej kryptologii[7].

Powierzone zadania realizowane są w czterech obszarach działalności, a mianowicie: naukowo-edukacyjnym, badawczo-rozwojowym, wdrożeniowym i opiniodawczym. W tym celu Centrum może korzystać z pomocy, jak i współpracy z jednostkami organizacyjnymi resortu obrony narodowej oraz ze Służbą Kontrwywiadu Wojskowego i Służbą Wywiadu Wojskowego.

Zaplecze naukowe dla NCK oparte jest na Wojskowej Akademii Technicznej, która jako jedyna w Polsce, i jedna z dwóch europejskich uczelni, od roku 1997 kształci kryptologów w Instytucie Matematyki i Kryptologii Wydziału Cybernetyki. Od 2011 roku prowadzi także prace nad projektem pt. „Ochrona informacji istotnych dla bezpieczeństwa i funkcjonowania państwa, w tym o klauzuli ściśle tajne – budowa narodowego centrum kryptografii i dekryptażu". Celem realizowanego

7 http://www.infor.pl/dzienniki-urzedowe/ministra-obrony-narodowej,rok,2013,nr,30/poz,-21,zarzadzenie-nr-10-mon-ministra-obrony-narodowej-w-sprawie-utworzenia-i-nadania html# [dostęp: 2.02.2015].

projektu jest utworzenie narodowych algorytmów, urządzeń kryptograficznych oraz specjalistycznego oprogramowania[8].

Nie jest to jedyne przedsięwzięcie badawczo-rozwojowe, w którym bierze udział NCK. Od pewnego czasu we współpracy z Narodowym Centrum Badań i Rozwoju realizuje ono projekt ROTOR, mający na celu „zagwarantowanie najwyższego poziomu ochrony kryptograficznej krajowych informacji niejawnych". Nie bez znaczenia jest także fakt, że na wniosek NCK rozpoczęto pracę nad wojskowymi normami kryptograficznymi[9].

W skład zespołu NCK wchodzi szereg specjalistów wojskowych z zakresu kryptografii, matematyki, informatyki, elektroniki, jak również eksperci ABW. Zajmują się oni budową algorytmów kryptologicznych, testowaniem urządzeń kryptograficznych, a także kryptoanalizą, czyli łamaniem szyfrów. Centrum traktowane jest jako jednostka wojskowa, a co za tym idzie, podlega ministrowi kierującemu resortem obrony narodowej.

Z dostępnych materiałów wnioskować można o wzrastającej roli NCK w przypadku zagrożenia cyberterrorystycznego w resorcie obrony narodowej. W takiej sytuacji Centrum stanowić będzie ogniwo koordynujące podjęte działania. Decyzja zwiększająca znaczenie i uprawnienia NCK w obliczu cyberataku podjęta została przez ministra Tomasza Siemoniaka, który formalnoprawnie poszerzył kompetencje Centrum o „realizację zadań związanych z pełnieniem funkcji Centrum Koordynacyjnego Systemu Reagowania na Incydenty Komputerowe resortu obrony narodowej".

Inspektorat Systemów Informacyjnych Dowództwa Operacyjnego

Kolejnym organem działającym na rzecz ochrony cyberprzestrzeni wykorzystywanej na potrzeby militarne jest funkcjonujący od 1 października 2013 roku Inspektorat Systemów Informacyjnych (ISI). Jednostka ta powstała w miejsce funkcjonującego Departamentu Informatyki i Telekomunikacji MON. Decyzja o jej powołaniu została podpisana 24 lipca 2013 roku przez ówczesnego ministra obrony narodowej Tomasza Siemoniaka. Była ona konsekwencją strukturalnego racjonalizowania systemu dowodzenia i kierowania Siłami Zbrojnymi RP.

Wdrażanie nowego systemu dowodzenia i kierowania SZ RP spowodowało szereg zmian strukturalnych, które nie ominęły również obszaru teleinformatyki wojskowej. Reforma ta wiązała się z rozpoczęciem procesu transformacji i konsolidacji struktur wsparcia działających na rzecz bezpieczeństwa teleinformatycznego w wojsku.

Konsekwencją podjętych działań było przejęcie przez ISI w podporządkowanie, jak również zintegrowanie, wszystkich elementów wsparcia teleinformatycznego

8 Zob. więcej: *Warszawska twierdza szyfrów*, dostępne na stronie internetowej: http://www.polskazbrojna.pl/home/articleinrnagazineshow/10926?t=WARSZAWSKA-TWIERDZA-SZYFROW [dostęp: 5.02.2015].

9 http://www.rp.pl/artykul/1128596.html?print=tak&p=0 [dostęp: 23.03.2014].

podległych pod poszczególne Dowództwa Rodzajów Sił Zbrojnych. W związku z tym Inspektorat stał się odpowiedzialny za całokształt spraw związanych z informatyzacją resortu, w tym za wsparcie procesów kierowania i dowodzenia oraz bezpieczeństwo cyberprzestrzeni Sił Zbrojnych RP.

Integracja struktur teleinformatyki wojskowej poprzez uformowanie jednej instytucji, której podlegają wszystkie wojskowe jednostki teleinformatyczne, pozwoliła na kompleksowe świadczenie usług teleinformatycznych i właściwe zabezpieczenie w tym zakresie wszystkich jednostek wojskowych.

Zmieniła się także podległość samego Inspektoratu, który przed reformą Sił Zbrojnych, tj. do 31 grudnia 2013 roku, bezpośrednio podlegał Dyrektorowi Generalnemu MON, na którym spoczywał obowiązek przeformowania Departamentu Informatyki i Telekomunikacji. Z kolei z dniem 1 stycznia 2014 roku, czyli po utworzeniu Dowództwa Generalnego Rodzajów SZ, Inspektorat stał się jednostką podporządkowaną Dowódcy Generalnemu Rodzajów Sił Zbrojnych.

Na strukturę wewnętrzną ISI składa się szereg wyspecjalizowanych komórek organizacyjnych. Należą do nich:

- Kierownictwo,
- Szefostwo Sieci Teleinformatycznych: Oddział Sieci Telekomunikacyjnych, Oddział Sieci Informatycznych,
- Szefostwo Informatycznych Systemów Zarządzania: Oddział Informatycznych Systemów Zarządzania Zasobami Logistycznymi i Kadrowymi, Oddział Informatycznych Systemów Wsparcia Bieżącego, Oddział Informatycznych Systemów Zarządzania Zasobami Finansowymi,
- Szefostwo Informatycznych Systemów Wsparcia Dowodzenia Sił Zbrojnych: Oddział Informatycznych Systemów Rodzajów Wojsk, Oddział Informatycznych Systemów Rodzajów Sił Zbrojnych,
- Oddział Bezpieczeństwa Cyberprzestrzeni i Ochrony Informacji Niejawnych.

Ponadto omawianemu Instytutowi podlega kilka jednostek właściwych w zakresie bezpieczeństwa teleinformatycznego. Można zaliczyć do nich:

- Centrum Wsparcia Teleinformatycznego Sił Powietrznych,
- Centrum Wsparcia Teleinformatycznego Sił Zbrojnych,
- Resortowe Centrum Zarządzania Sieciami i Usługami Teleinformatycznymi,
- Resortowe Centrum Zarządzania Projektami Informatycznymi,
- Wojskowe Biuro Zarządzania Częstotliwościami,
- Zespół Zarządzania Wsparciem Teleinformatycznym w Bydgoszczy,
- Zespół Zarządzania Wsparciem Teleinformatycznym we Wrocławiu,
- Zespół Zarządzania Wsparciem Teleinformatycznym w Warszawie,
- Zespół Zarządzania Wsparciem Teleinformatycznym w Krakowie,
- Zespół Zarządzania Wsparciem Teleinformatycznym w Gdyni.

Wyniki badań dowodzą, że ISI jest właściwy w zakresie informatyzacji resortu obrony narodowej. Jest on odpowiedzialny za organizowanie i kierowanie procesami planowania, dostarczania, wsparcia, eksploatacji oraz użytkowania systemów teleinformatycznych stosownie do wypracowanych kierunków rozwoju. Zadania te realizowane są przez organizatorów systemów funkcjonalnych, w szczególności

wsparcia dowodzenia oraz zgodnie z potrzebami zgłaszanymi przez inne komórki i jednostki organizacyjne.

Instytut odpowiada za system zarządzania bezpieczeństwem teleinformatycznym w cyberprzestrzeni pozostającej w kompetencji Ministra Obrony Narodowej, wykonując zadania obejmujące planowanie i organizację systemu dowodzenia we wszystkich stanach funkcjonowania państwa, tj. w czasie pokoju, kryzysu i wojny[10].

Resortowe Centrum Zarządzania Sieciami i Usługami Teleinformatycznymi

Resortowe Centrum Zarządzania Sieciami i Usługami Teleinformatycznymi (RCZSiUT) stanowi kolejne ogniwo w strukturze militarnej działającej na rzecz ochrony cyberprzestrzeni. Na podstawie dostępnych materiałów wywnioskować można, że jest ono jednostką organizacyjną podległą ministrowi obrony narodowej, natomiast bezpośrednio podporządkowaną szefowi Inspektoratu Systemów Informacyjnych MON.

Działalność RCZSiUT jest regulowana szeregiem dokumentów określających zasady jego funkcjonowania. Podstawę w tym zakresie stanowią:

- wytyczne specjalistyczne Dyrektora Generalnego MON ukierunkowujące funkcjonowanie resortu ON w zakresie systemów informatycznych i telekomunikacyjnych,
- dyrektywa Szefa Sztabu Generalnego WP do działalności Sił Zbrojnych RP,
- Strategia Informatyzacji Resortu ON,
- zadania wynikające z planów:
  - Centralnego Planu Inwestycji Budowlanych Resortu ON,
  - Centralnego Planu Remontów Nieruchomości Resortu ON,
  - Planu Budownictwa Specjalnego ISI,
- zadania bieżące określane przez szefa ISI.

Dostępne materiały identyfikują główne zadania realizowane przez RCZSiUT. Należy do nich przede wszystkim zarządzanie systemami transmisyjnymi, komutacyjnymi, sieciami transmisji danych z uwzględnieniem optymalizacji jakości usług, struktury oraz kosztów utrzymania. Omawiany organ jest odpowiedzialny także za monitorowanie oraz analizowanie w trybie ciągłym stanu pracy i poziomu usług wojskowego systemu telekomunikacyjnego oraz koordynację procesów usuwania powstałych awarii. Po trzecie, Centrum pełni funkcję inwestora bezpośredniego inwestycji realizowanych dla instytucji i jednostek wojskowych w zakresie infrastruktury teleinformatycznej.

W odpowiedzialności RCZSiUT znajduje się również realizacja procesu modernizacji i remontów wojskowej infrastruktury telekomunikacyjnej. Co więcej,

10 http://www.isi.wp.mil.pl/pl/3.html [dostęp: 23.05.2014].

Centrum monitoruje w trybie ciągłym zagrożenia w obszarze teleinformatycznym, a w przypadku ich wystąpienia jest odpowiedzialne za reagowanie na zaistniałe incydenty komputerowe, a także sprawowanie funkcji Centrum Wsparcia Technicznego dla Centrum Koordynacji Systemu Reagowania na Incydenty Komputerowe.

Z uwagi na podległość merytoryczną RCZSiUT realizuje zadania na potrzeby szefa ISI związane ze sprawowaną przez niego funkcją gestora sprzętu informatyki oraz organizatora wojskowego systemu teleinformatycznego. Ponadto Centrum realizuje funkcję Oddziału Gospodarczego w zakresie usług telekomunikacyjnych dla 1258 instytucji wojskowych w wybranych działach zaopatrzenia. W tym zakresie obsługuje pododdziały własne oraz instytucje i jednostki wojskowe resortu obrony narodowej zgodnie z nadanym Planem Przydziałów Gospodarczych.

Z publikacji wynika, że główne cele RCZSiUT realizuje poprzez istniejące komórki wewnętrzne, do których należą:

- Oddział Zarządzania Sieciami Teleinformatycznymi,
- Oddział Zarządzania Usługami Teleinformatycznymi,
- Wydział Zarządzania Systemami Teleinformatycznymi,
- Wydział Bieżącego Zarządzania Systemami Teleinformatycznymi,
- Oddział Modernizacji i Remontów[11].

W celu wypełniania swoich obowiązków RCZSiUT współpracuje z organami administracji państwowej oraz operatorami telekomunikacyjnymi w zakresie realizacji przedsięwzięć dotyczących eksploatacji infrastruktury telekomunikacyjnej oraz monitoruje funkcjonowanie systemów teleinformatycznych NATO na obszarze Polski.

System Reagowania na Incydenty Komputerowe

Prace mające na celu ochronę krytycznej infrastruktury teleinformatycznej w Polsce rozpoczęły się właściwie w 1996 roku, tj. w momencie powstania CERT Polska (z ang. Computer Emergency Response Team). Jest to zespół powołany w celu reagowania na zdarzenia, które naruszają bezpieczeństwo w sieci Internet. Od roku 1997 zespół jest członkiem FIRST (Forum of Incidents Response and Security Teams)[12] oraz działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej)[13].

11 http://www.rczsiut.wp.mil.pl/pl/6.html [dostęp: 14.02.2014].

12 Organizacja o charakterze międzynarodowym, powstała w roku 1989, która skupia zespoły z całego świata zajmujące się reagowaniem na incydenty komputerowe dotyczące sieci Internet. Zob. więcej: http://www.first.org/about [dostęp: 14.02.2014].

13 NASK – Naukowa i Akademicka Sieć Komputerowa. Wiodący polski operator sieci transmisji danych, oferujący nowoczesne rozwiązania teleinformatyczne dla klientów biznesowych, administracji i nauki. Od roku 2010 funkcjonuje jako instytut badawczy. Zob. więcej: http://www.nask.pl/run/n/Dzialalnosc/ [dostęp: 11.03.2014].

Główne zadania CERT Polska skupiają się na rejestracji i obsłudze zdarzeń naruszających bezpieczeństwo sieci, alarmowaniu użytkowników o niebezpieczeństwie, działalności szkoleniowej oraz prowadzeniu badań i przygotowywaniu corocznych raportów dotyczących bezpieczeństwa polskich zasobów sieci Internet[14]. Zespół zajmuje się także publikowaniem opracowań o tematyce dotyczącej zagadnień związanych z szeroko pojętym bezpieczeństwem w sieci.

W roku 2008 został powołany Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL[15]. Nadmienić należy, że „zgodnie z przyjętą Polityką Ochrony Cyberprzestrzeni RP[16] w zakresie realizacji zadań związanych z bezpieczeństwem cyberprzestrzeni RP, […] pełni [on] rolę głównego zespołu CERT w obszarze administracji rządowej i obszarze cywilnym. Podstawowym jego zadaniem jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami. Realizuje on jednocześnie zadania głównego narodowego zespołu odpowiadającego za koordynację procesu obsługi incydentów komputerowych w obszarze CRP. Stanowi poziom drugi Krajowego Systemu Reagowania na Incydenty Komputerowe w CRP"[17].

Warto także dodać, że zespół CERT.GOV.PL zajmuje się prowadzeniem działalności szkoleniowej z zakresu reagowania na incydenty naruszające bezpieczeństwo teleinformatyczne. Ponadto w witrynie internetowej umieszcza aktualne informacje z zakresu cyberbezpieczeństwa.

Zespół CERT Polska, działający w ramach NASK, a także przy współpracy z Agencją Bezpieczeństwa Wewnętrznego, przyczynił się do stworzenia systemu wczesnego ostrzegania o zagrożeniach występujących w Internecie – ARAKIS-GOV, którego podstawowym zadaniem jest wsparcie ochrony zasobów informatycznych administracji państwowej.

Z kolei w obszarze militarnym stworzono System Reagowania na Incydenty Komputerowe (SRnIK) resortu obrony narodowej[18], który zajmuje się realizowaniem zadań w zakresie koordynacji procesów zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach i sieciach teleinformatycznych użytkowanych przez resort. W tym celu współpracuje zarówno z jednostkami i komórkami organi-

14 http://www.cert.pl/o-nas [dostęp: 14.02.2014].

15 Usytuowany jest w strukturze Agencji Bezpieczeństwa Wewnętrznego i działa w ramach departamentu bezpieczeństwa teleinformatycznego.

16 Zob. więcej: http://www.cert-gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony Cyberprzestrzeni-Rzeczy-pospolitej-Polskiej.html [dostęp: 14.03.2015].

17 Tamże, s. 8 i 18.

18 Decyzja nr 357/MON Ministra Obrony Narodowej z dnia 29 lipca 2008 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej, http://www.srnik.wp.mil.p1/pl/2.html [dostęp: 11.07.2014].

zacyjnymi resortu obrony, jak również z organizacjami zewnętrznymi. Działania te dotyczącą współpracy na poziomie krajowym, jak i międzynarodowym[19].

Z dostępnych materiałów wynika, że SRnIK został zorganizowany w trzypoziomową strukturę, w skład której wchodzą:

- Centrum Koordynacyjne SRnIK, którego funkcję spełnia właściwa komórka wewnętrzna Narodowego Centrum Kryptologii;
- Centrum Techniczne SRnIK, którego funkcję spełnia właściwa komórka wewnętrzna Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych;
- administratorzy systemów teleinformatycznych w jednostkach i komórkach organizacyjnych.

Dostępne materiały pozwalają stwierdzić, że SRnIK został zorganizowany w celu zapewnienia koordynacji i realizacji procesów zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach teleinformatycznych oraz autonomicznych stanowiskach komputerowych resortu obrony narodowej. Zamiar ten jest realizowany z wyłączeniem systemów teleinformatycznych i narodowych segmentów międzynarodowych systemów teleinformatycznych Służby Wywiadu Wojskowego oraz Służby Kontrwywiadu Wojskowego, a także systemów Żandarmerii Wojskowej wykorzystywanych bezpośrednio do prowadzenia działalności dochodzeniowo-śledczej oraz operacyjno-rozpoznawczej.

Istotny dla rozważanej tematyki jest fakt, że zgodnie z decyzją Ministra Obrony Narodowej nr 2/MON z 12 stycznia 2015 roku, nadzór nad funkcjonowaniem SRnIK sprawuje Pełnomocnik Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni, aktualnie podsekretarz stanu w MON Bartłomiej Grabski.

Każdy z poziomów SRnIK, tj. zarówno Centrum Koordynacyjne SRnIK, jak również Centrum Techniczne, realizują odrębne zadania wynikające z decyzji ministra w sprawie organizacji i funkcjonowania SRnIK. Centrum Koordynacyjne określa ogólne zasady funkcjonowania SRnIK, a także współpracuje z różnymi podmiotami w zakresie ustalania formalnoprawnych zasad funkcjonowania SRnIK oraz planów jego rozwoju w wymiarze krajowym i międzynarodowym. Ogniwami współpracującymi w tym obszarze są:

- Służba Kontrwywiadu Wojskowego,
- Żandarmeria Wojskowa,
- Departament Ochrony Informacji Niejawnych,
- Organizator Systemu Funkcjonalnego Wsparcia Dowodzenia,
- Centrum Techniczne SRnIK w zakresie ustalania ogólnych zasad funkcjonowania SRnIK,
- Centrum Koordynacyjne systemu reagowania na incydenty komputerowe Organizacji Traktatu Północnoatlantyckiego,

19 Decyzja nr 243/MON Ministra Obrony Narodowej z dnia 18 lipca 2014 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej, http://www.srnik.wp.mil.p1/pl/2.html [dostęp: 11.07.2014].

• krajowe i międzynarodowe organy koordynujące systemy reagowania na incydenty komputerowe.

Kompetencje Centrum Koordynacyjnego obejmują również realizację zadań wynikających z Planu Zarządzania Kryzysowego MON, Wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego oraz Planu Operacyjnego Funkcjonowania Działu Administracji Rządowej Obrona Narodowa w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny.

Nie bez znaczenia jest także fakt, że omawiany poziom SRnIK bierze udział w pracach grup roboczych w ramach Organizacji Traktatu Północnoatlantyckiego oraz reprezentuje resort obrony narodowej w kontaktach z organizacjami spoza resortu, w zakresie reagowania na incydenty komputerowe w systemach teleinformatycznych. Ponadto do zadań Centrum Koordynacyjnego należy prowadzenie ewidencji systemów teleinformatycznych objętych SRnIK na podstawie danych otrzymanych od organizatorów systemów teleinformatycznych.

Centrum Koordynacyjne w zakresie ustalenia ogólnych zasad funkcjonowania SRnIK współpracuje z Centrum Technicznym, które z kolei odpowiada za przygotowanie i realizację szeregu działań analitycznych i diagnostycznych. Do głównych zadań Centrum Technicznego należy wydawanie biuletynów informacyjnych, analiza infrastruktury teleinformatycznej, opracowywanie zaleceń i wytycznych zapobiegających wystąpieniu incydentów komputerowych. Ponadto współpracuje ono z wieloma podmiotami w zakresie reagowania na incydenty komputerowe i incydenty bezpieczeństwa teleinformatycznego. Należą do nich:

• Rządowy Zespół Reagowania na Incydenty Komputerowe,
• Służba Kontrwywiadu Wojskowego,
• właściwe piony ochrony informacji niejawnych, Żandarmeria Wojskowa i inne organy uprawnione do ścigania przestępstw komputerowych – w zakresie bezpieczeństwa systemów teleinformatycznych w resorcie obrony narodowej oraz reagowania na podejrzenie popełnienia przestępstwa przeciwko ochronie informacji,
• Rządowe Centrum Bezpieczeństwa,
• Dowództwo Operacyjne Rodzajów Sił Zbrojnych,
• Centrum Techniczne systemu reagowania na incydenty komputerowe Organizacji Traktatu Północnoatlantyckiego,
• krajowe i międzynarodowe zespoły systemu reagowania na incydenty komputerowe,
• organizatorzy systemów teleinformatycznych,
• kierownicy jednostek organizacyjnych i komórek organizacyjnych poprzez administratorów systemów teleinformatycznych.

Do obowiązków Centrum Technicznego należy ponadto monitorowanie stanu bezpieczeństwa nadzorowanych systemów teleinformatycznych, prowadzenie wykazu osób funkcyjnych odpowiedzialnych za SRnIK, w tym danych teleadresowych. Omawiany poziom jest również odpowiedzialny za realizację zadań związanych z bezpośrednią obsługą incydentów komputerowych w systemach teleinformatycznych według odpowiednich procedur. Co więcej, Centrum zbiera i analizuje informacje o zdarzeniach oraz tworzy na ich bazie okresowe raporty o stanie bezpieczeństwa

w systemach teleinformatycznych dla potrzeb organizatorów systemów, Centrum Koordynacyjnego SRnIK oraz Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni. Jest ono również odpowiedzialne za organizowanie dla personelu komórek i jednostek organizacyjnych szkolenia z zakresów reagowania na incydenty komputerowe oraz bezpieczeństwa teleinformatycznego.

W uzgodnieniu z organizatorem systemu oraz Pełnomocnikiem Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni Centrum może stosować środki techniczne i organizacyjne oraz narzędzia do zdalnego zarządzania i kontroli konfiguracji systemów teleinformatycznych, służące do zapobiegania, wykrywania i usuwania skutków incydentów komputerowych. W przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych zastosowanie wyżej wymienionych rozwiązań uwzględnia się w szacowaniu ryzyka oraz dokumentacji bezpieczeństwa systemu teleinformatycznego. W powyższym zakresie organizator systemu uzgadnia dokumentację bezpieczeństwa z Centrum Technicznym SRnIK.

Nie bez znaczenia jest również fakt, że omawiany poziom na polecenie Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni realizuje wniosek organizatora systemu lub organu akredytującego, w porozumieniu z organizatorem systemu, a w przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych również z właściwym pionem ochrony, za wiedzą organizatora i organu akredytującego, testy bezpieczeństwa i testy podatnościowe, mające na celu weryfikację poprawności funkcjonowania zabezpieczeń, ustalenie ich aktualnego stanu oraz rekomendowanie skutecznych rozwiązań.

Centrum Techniczne odpowiada także za prowadzenie portali informacyjnych w sieci INTER-MON i MIL-WAN na potrzeby obsługi incydentów komputerowych i prowadzonych działań informacyjnych. W przypadku wystąpienia takiego zdarzenia, wnioskuje ono do organizatora systemu o czasowe wyłączenie lub zaniechanie przetwarzania informacji w systemie lub części systemu teleinformatycznego przetwarzającego informacje niejawne. Omawiany poziom podejmuje również decyzje o czasowym odłączeniu systemu teleinformatycznego posiadającego połączenie z siecią Internet, w którym stwierdzono wystąpienie incydentu komputerowego – o podjętej decyzji Centrum Techniczne SRnIK powiadamia organizatora systemu.

Do zadań Centrum należy również udział w pracach grup roboczych w zakresie reagowania na incydenty komputerowe w systemach teleinformatycznych przeznaczonych do przetwarzania informacji jawnych lub narodowych informacji niejawnych. Odpowiada ono za informowanie organizatora systemu o zdarzeniach, incydentach komputerowych, zagrożeniach związanych z monitorowanym systemem teleinformatycznym oraz o wydanych zaleceniach i podjętych decyzjach.

W razie konieczności dany poziom udziela niezbędnej pomocy pełnomocnikom do spraw ochrony informacji niejawnych oraz administratorom systemów teleinformatycznych w przypadku prowadzenia postępowania wyjaśniającego wystąpienie incydentu komputerowego oraz przywracania funkcjonowania systemu po zaistniałym incydencie.

Utrzymywanie laboratorium technicznego na potrzeby analizy kodów złośliwych oraz prowadzenia testów bezpieczeństwa i podatności to kolejne z zadań, za które odpowiedzialny jest omawiany podmiot. Ponadto nie bez znaczenia jest także fakt, że prowadzi on ewidencję administratorów systemów teleinformatycznych, zawierającą stopień wojskowy, imię i nazwisko oraz numer telefonu, nazwę komórki albo jednostki organizacyjnej osoby wyznaczonej do pełnienia funkcji administratora systemu teleinformatycznego.

Centrum Techniczne odpowiada również za opracowanie i stałą aktualizację wielu opracowań i podręczników dotyczących bezpieczeństwa teleinformatycznego. Wśród nich wymienić należy publikacje takie jak:

- *Podręcznik reagowania na incydenty komputerowe w resorcie obrony narodowej*,
- *Standardowe Procedury Operacyjne SRnIK w resorcie obrony narodowej*,
- *Wytyczne do opracowania Lokalnych Procedur Operacyjnych SRnlK w jednostce organizacyjnej*.

Wszystkie wskazane wyżej dokumenty są zatwierdzane przez Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni. Zanim to jednak nastąpi, Centrum Techniczne ma obowiązek uzgodnienia występujących tam treści z wieloma komórkami organizacyjnymi współpracującymi w zakresie bezpieczeństwa w sieci. Należą do nich:

- Departament Ochrony Informacji Niejawnych,
- Żandarmeria Wojskowa,
- Centrum Koordynacyjne SRnIK,
- Organizator Systemu Funkcjonalnego Wsparcia Dowodzenia,
- organizator systemu, w części dotyczącej jego systemu,
- Departament Strategii i Planowania Obronnego w zakresie zachowania spójności dokumentów z Planem Zarządzania Kryzysowego MON, Wykazem przedsięwzięć i procedur systemu zarządzania kryzysowego oraz Planem Operacyjnym Funkcjonowania Działu Administracji Rządowej Obrona Narodowa w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny,
- Służba Kontrwywiadu Wojskowego.

Należy podkreślić fakt, iż w wykonywaniu swoich zadań Centrum Techniczne SRnIK ściśle współpracuje z administratorami systemów teleinformatycznych w komórkach i jednostkach organizacyjnych. Są oni zobowiązani do wykonywania zaleceń Centrum w zakresie przeciwdziałania naruszeniom polityk bezpieczeństwa i obsługi incydentów komputerowych zgodnie z procedurami SRnIK. Administratorzy systemów teleinformatycznych są odpowiedzialni za wdrożenie w uzgodnieniu z kierownikiem jednostki organizacyjnej „Lokalnych Procedur Operacyjnych SRnIK w jednostce organizacyjnej" ujętych w dokumentacji bezpieczeństwa. Ich zadaniem jest także nadzorowanie użytkowników administrowanych przez nich jawnych systemów teleinformatycznych oraz wspomagania inspektorów bezpieczeństwa teleinformatycznego w nadzorowaniu użytkowników administrowanych przez nich niejawnych systemów teleinformatycznych w zakresie przestrzegania ustalonych procedur bezpieczeństwa.

W celu realizacji powierzonych zadań konieczna jest współpraca administratorów systemów teleinformatycznych z odpowiednimi podmiotami zewnętrznymi, do których należą instytucje takie jak:

- Służba Kontrwywiadu Wojskowego,
- właściwe piony ochrony informacji niejawnych, Żandarmeria Wojskowa i inne organy uprawnione do ścigania przestępstw komputerowych – w zakresie bezpieczeństwa systemów teleinformatycznych w resorcie obrony narodowej oraz reagowania na podejrzenie popełnienia przestępstwa przeciwko ochronie informacji,
- Rządowe Centrum Bezpieczeństwa w zakresie zabezpieczenia śladów i ustalenia przyczyn wystąpienia incydentu komputerowego, zgodnie z procedurami SRnIK.

W sytuacji wykrycia incydentu komputerowego lub innego zdarzenia mogącego wpłynąć na naruszenie polityki bezpieczeństwa w administrowanych przez nich systemach teleinformatycznych administratorzy zobowiązani są do zgłaszania zdarzeń do Centrum Technicznego SRnIK, a w przypadku systemów teleinformatycznych przetwarzających informacje niejawne dodatkowo do inspektora bezpieczeństwa teleinformatycznego.

Mają oni także obowiązek niezwłocznego przesyłania do Centrum Technicznego wskazanych przez nie próbek kodu lub materiałów umożliwiających prowadzenie analiz technicznych, zgodnie z procedurami SRnIK, a w przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych – na zasadach opisanych w dokumentacji bezpieczeństwa teleinformatycznego; informowania Centrum Technicznego SRnIK przez kierownika jednostki organizacyjnej o zmianach personalnych administratorów systemów teleinformatycznych.

Realizacja zadań z zakresu bezpieczeństwa teleinformatycznego spoczywa również w gestii kierowników komórek i jednostek organizacyjnych, którzy mają zapewnić możliwość wykonywania działań przez pełnomocników ochrony, inspektorów bezpieczeństwa teleinformatycznego i administratorów systemów teleinformatycznych zgodnie z określonymi procedurami. Stoją oni także na straży przestrzegania obowiązujących dokumentów normatywnych i zaleceń w zakresie reagowania na incydenty komputerowe. Ponadto kierownicy odpowiadają za realizowanie Lokalnych Procedur Operacyjnych SRnIK oraz uwzględnienie obowiązków przewidzianych w dokumentacji bezpieczeństwa teleinformatycznego oraz dokumentacji eksploatacyjnej i procedurach dla systemów teleinformatycznych.

Inne podmioty zaangażowane w ochronę cyberprzestrzeni w MON

W realizację zadań z zakresu ochrony cyberprzestrzeni zaangażowane są także inne podmioty. Jednym z nich jest powstałe w 2010 roku Centrum Bezpieczeństwa Cybernetycznego (CBC) w Białobrzegach, gdzie rozlokowany jest 9. batalion łączności. Informacje na temat tej jednostki z oczywistych względów nie są powszechne i łatwo dostępne – jej działalność jest objęta tajemnicą i chroniona przed środkami

masowego przekazu, w związku z tym niewiele się mówi o czynnościach podjętych w zakresie incydentów komputerowych czy szeroko pojmowanego cyberbezpieczeństwa. Informacje na ten temat przekazywane są lakonicznie, czego potwierdzenie stanowi odpowiedź podsekretarza stanu w Ministerstwie Obrony Narodowej Marcina Idzika z 21 stycznia 2011 roku na zapytanie nr 8332 w sprawie wirusa komputerowego, który paraliżował pracę MON przez dwa dni. W omawianej kwestii pojawiła się informacja dotycząca CBC w Białobrzegach o następującej treści: „Centrum Bezpieczeństwa Cybernetycznego w Białobrzegach posiada inny charakter, zadania i nie jest organizacją dedykowaną do prowadzenia aktywnych, bezpośrednich działań obronnych w sieciach komputerowych resortu obrony narodowej. Jest ono uczestnikiem realizowanego przez Sztab Generalny Wojska Polskiego procesu osiągania zdolności w zakresie dowodzenia i kierowania w cyberprzestrzeni, zgodnie z przyjętymi celami sił zbrojnych NATO".

Należy zwrócić uwagę także na Laboratorium Analiz Ataków Cybernetycznych w Wojskowym Instytucie Łączności (WIŁ) w Zegrzu Południowym. Jego powstanie, jak i cała działalność również jest chroniona tajemnicą. Głównym zadaniem Laboratorium będzie pomoc w walce z cyberprzestępczością. Przy wsparciu Narodowego Centrum Badań i Rozwoju stanie tam m.in. superkomputer, który będzie śledził hakerów w sieci i walczył z nimi.

W Wojskowym Instytucie Łączności w Zegrzu Południowym jest budowane prawie 40-kilometrowe przyłącze światłowodowe prowadzące do centrum Warszawy. Dzięki niemu WIŁ będzie miał własne przyłącze do Polskiego Internetu Optycznego sieci PIONIER. Jest to sieć skupiająca główne centra naukowo-badawcze oraz placówki naukowo-dydaktyczne. Natomiast w Laboratorium Analiz Ataków Cybernetycznych będzie część serwerowa, a w sześciu szafach, na ok. 30 metrach kwadratowych, zostanie umieszczony superkomputer. Dzięki opracowaniom będzie można analizować online w czasie zbliżonym do rzeczywistego strumienie ruchu i badać anomalie w ruchu sieciowym, czyli innymi słowy ustalić, czy nie nastąpił już atak. Laboratorium będzie w stanie zaobserwować symptomy ataku. Jest to podstawowa platforma badawcza, która rozwija kompetencje w zakresie możliwości tworzenia metod ochrony przed atakami cybernetycznymi. Uzyskane zwiększone możliwości obliczeniowe pozwolą na opracowywanie zaawansowanych mechanizmów detekcji. Szybkie łącze internetowe z kolei pozwoli na dostęp do danych składowanych w innych centrach komputerowych oraz na wspólną pracę różnych ośrodków.

W Laboratorium będzie istniała możliwość przeprowadzania symulacji różnego rodzaju zmasowanych ataków, a także testowania sposobów reagowania na takie incydenty i przeciwdziałania im. W celu optymalizacji swojego działania Laboratorium podejmie współpracę z Centrum Bezpieczeństwa Cybernetycznego Ministerstwa Obrony Narodowej i z Komendą Główną Policji[20].

20 Więcej zob.: http://www.polskieradio.pl/7/3172/Artykul/1398880,Superkomputer-chrooni-cyberprzestrzen, [dostęp: 23.02.2015].

Wnioski

Każdy użytkownik sieci i każde państwo może być narażone na atak cybernetyczny. Oczywiście skala ataku na pojedynczego internautę jest niewspółmierna do ataku na państwo, a także jego elementy działające w obszarze bezpieczeństwa. Kraje o wyższym stopniu usieciowienia swoich struktur muszą zwracać szczególną uwagę na działania profilaktyczne i zaradcze w zakresie ochrony cyberprzestrzeni. Z drugiej strony należy także mieć na uwadze, że każde państwo może się stać również sprawcą ataku cybernetycznego, jeżeli znajdzie ku temu odpowiednie przesłanki oraz posiada profesjonalistów zdolnych do jego przeprowadzenia.

Współcześnie nie stanowi żadnego novum przypuszczenie, że każda jednostka, zarówno w wymiarze jednostkowym, jak i instytucjonalnym, może znaleźć się w stanie zagrożenia cybernetycznego. Siły Zbrojne RP oraz inne podmioty wchodzące w skład resortu obrony narodowej nie są wyjątkiem w tym zakresie. To z kolei pozwala sądzić, że poruszany problem jest dość istotny, zwłaszcza obecnie, kiedy większość działających systemów militarnych jest w dużym stopniu zinformatyzowana. Z uwagi na rozwój technologii komputerowych przypuszczać można, że ta zależność będzie coraz silniejsza.

Oczywistym faktem jest, że ataki w cyberprzestrzeni stanowią permanentnie rosnące zagrożenie dla bezpieczeństwa państw, zarówno w wymiarze militarnym, jak i niemilitarnym. Należy pamiętać, że tego typu incydenty, choć przeprowadzane w świecie wirtualnym, mogą wywierać jak najbardziej rzeczywiste skutki. Na gruncie krajowym niewiele państw formalnie określiło sposoby prewencji lub chociażby reakcji na najpoważniejsze zagrożenia pojawiające się w cyberprzestrzeni. Stany Zjednoczone jako pierwsze wprowadziły prawo do militarnej reakcji w przypadku wielkoskalowego ataku na cyberprzestrzeń. Warte uwagi są również działania praktyczne, jakie podjęła Estonia, powołując do życia Ligę Obrony Cybernetycznej (LOC). W jej skład wchodzą: inżynierowie, pracownicy banków, korporacji i ministerstw. W momencie, w którym doszłoby do cyberwojny, LOC podlegać ma wojskowemu dowództwu.

Z przeprowadzonych badań wynika zasadniczy wniosek, że słabym elementem cyberbezpieczeństwa Polski wydaje się brak organu, który posiadałby w swoich uprawnieniach kompetencje koordynacyjne, doradcze oraz konsultacyjne w dziedzinie cyberbezpieczeństwa.

Na poziomie SZ RP zauważa się również rozproszenie działań. Przykładem może być dotychczasowa odpowiedzialność za zdolności operacyjne dwóch organizatorów systemów funkcjonalnych: Organizatora Systemu Funkcjonalnego MON oraz Organizatora Systemu Funkcjonalnego Wsparcia Dowodzenia. Dlatego też proponuje się utworzenie programu operacyjnego pn. „Bezpieczeństwo cyberprzestrzeni i wsparcie kryptologiczne", który skonsoliduje i usystematyzuje realizację wszystkich potrzeb związanych z pozyskiwaniem, utrzymywaniem i rozwojem zdolności operacyjnych w obszarze cyberobrony i narodowej kryptologii. Ponadto zapewni gwarancję kompleksowej budowy systemu obrony cyberprzestrzeni.

Celem artykułu było zaprezentowanie wyników badań z zakresu identyfikacji krajowych podmiotów zaangażowanych na rzecz ochrony cyberprzestrzeni wykorzystywanej na potrzeby militarne. Realizacja podjętego zamiaru wiązała się z rozwiązaniem problemu badawczego oraz problematyki szczegółowej.

W odniesieniu do pierwszego problemu szczegółowego dotyczącego działań podejmowanych przez Pełnomocnika MON ds. Bezpieczeństwa Cyberprzestrzeni ustalono, że jest on organem koordynującym przedsięwzięcia przewidziane dla MON w sprawach bezpieczeństwa cyberprzestrzeni, w odniesieniu do wszystkich komórek organizacyjnych ministerstwa i jednostek organizacyjnych resortu obrony narodowej.

Udzielając odpowiedzi na drugi problem szczegółowy, obejmujący działania podejmowane przez Narodowe Centrum Kryptografii w zakresie ochrony cyberprzestrzeni, dowiedziono, że realizuje ono zadania w czterech obszarach, tj. naukowo-edukacyjnym, badawczo-rozwojowym, wdrożeniowym i opiniodawczym. Zajmuje się w dużej mierze aktywnością związaną z prowadzeniem badań, projektowaniem, budową, wdrażaniem, użytkowaniem oraz ochroną narodowych technologii kryptologicznych, jak również wytwarzaniem nowych produktów dla państwa przez zespolenie potencjału naukowego i przemysłowego w obszarze zaawansowanych technologii informatycznych i kryptograficznych.

Przechodząc do trzeciego zagadnienia szczegółowego, związanego z działaniami podejmowanymi przez Inspektorat Systemów Informacyjnych Dowództwa Operacyjnego, ustalono, iż to ogniwo odpowiada za zintegrowanie wszystkich elementów wsparcia teleinformatycznego podległych pod poszczególne Dowództwa Rodzajów Sił Zbrojnych. W związku z tym Inspektorat jest odpowiedzialny za całokształt spraw związanych z informatyzacją resortu obrony narodowej, w tym za wsparcie procesów kierowania i dowodzenia.

W nawiązaniu do czwartego problemu szczegółowego, obejmującego zakres działań podejmowanych przez Resortowe Centrum Zarządzania Sieciami i Usługami Teleinformatycznymi, jako główny rejon odpowiedzialności zidentyfikowano zarządzanie systemami transmisyjnymi, komutacyjnymi, sieciami transmisji danych z uwzględnieniem optymalizacji jakości usług, struktury oraz kosztów utrzymania. Omawiany organ jest odpowiedzialny także za monitorowanie oraz analizowanie w trybie ciągłym stanu pracy i poziomu usług wojskowego systemu telekomunikacyjnego oraz koordynację procesów usuwania powstałych awarii.

W kwestii kolejnego zagadnienia szczegółowego, dotyczącego Systemu Reagowania na Incydenty Komputerowe, ustalono, że dany podmiot jest podzielony w zakresie zadań i odpowiedzialności na trzy podsystemy, tj. Centrum Koordynacyjne, Centrum Techniczne oraz administratorów systemów teleinformatycznych w jednostkach i komórkach organizacyjnych. Wszystkie z tych elementów realizują powierzone działania w ścisłej współpracy i zgodnie z ustaloną procedurą.

Nawiązując do ostatniego problemu badawczego, który obejmował inne podmioty działające w obszarze ochrony cyberprzestrzeni, zidentyfikowano dwa kluczowe elementy. Pierwszym z nich jest Centrum Bezpieczeństwa Cybernetycznego w Białobrzegach, gdzie rozlokowany jest 9. batalion łączności, natomiast drugim Wojskowy Instytut Łączności w Zegrzu Południowym prowadzący Laboratorium Analiz Ataków Cybernetycznych.

Podsumowując, warto zauważyć, że współczesny system instytucjonalnej ochrony cyberprzestrzeni militarnej zaczął być organizowany dopiero w 2008 roku, czyli prawie 20 lat po tym, jak uruchomiono w Polsce pierwsze łącze internetowe. Przez kilka lat rozwijano poszczególne komponenty tego systemu, podejmując próbę określenia zasad działania oraz zbioru realizowanych zadań, jak również zasad współpracy poszczególnych podmiotów, zarówno w resorcie obrony, jak i poza nim. Organizacja omawianego systemu została przedstawiona w formie tabelarycznej w załączniku nr 1.

Na zakończenie należy zaakcentować, że większość opracowań dotyczących ochrony cyberprzestrzeni oznaczona jest wysoką klauzula tajności. W opracowaniu wykorzystano tylko informacje z otwartych źródeł informacji.

Literatura

Decyzja nr 243/MON Ministra Obrony Narodowej z dnia 18 lipca 2014 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej.

Decyzja nr 357/MON Ministra Obrony Narodowej z dnia 29 lipca 2008 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej.

Decyzja nr 38/MON Ministra Obrony Narodowej z dnia 16 lutego 2012 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni.

Decyzja nr 490/MON Ministra Obrony Narodowej z dnia 16 grudnia 2015 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni.

Strategia Obronności Rzeczypospolitej Polskiej, Strategia sektorowa do Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2009.

http://www.cert.pl/o-nas [dostęp: 14.02.2014].

http://www.cert-gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony Cyberprzestrzeni-Rzeczy-pospolitej-Polskiej.html [dostęp: 14.03.2015].

http://www.first.org/about [dostęp: 14.02.2014].

http://www.gazetaprawna.pl/artykuly/838061,ochrona-cyberprzestrzeni-w-polsce-jest-w-fatalnym-stanie.html [dostęp: 16.05.2015].

http://www.infor.pl/dzienniki-urzedowe/ministra-obrony-narodowej,rok,2013,nr,30/poz,-21,zarzadzenie-nr-10-mon-ministra-obrony-narodowej-w-sprawie-utworzenia-i-nadania html# [dostęp: 2.02.2015].

http://www.isi.wp.mil.pl/pl/3.html [dostęp: 23.05.2014].

http://www.nask.pl/run/n/Działalnosc/ [dostęp: 11.03.2014].

http://www.polskieradio.pl/7/3172/Artykul/1398880,Superkomputer-chrooni-cyberprzestrzen, [dostęp: 23.02.2015].

http://www.rczsiut.wp.mil.pl/pl/6.html [dostęp: 14.02.2014].

http://www.rp.pl/artykul/1128596.html?print=tak&p=0 [dostęp: 23.03.2014].

https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html [dostęp: 30.06.2015].

http://www-Polska-zbrojna.pl/home/articleinrnagazineshow/10926?t=WARSZAWSKA-TWIERDZA-SZYFROW [dostęp: 5.02.2015].

INSTITUTIONAL ACTORS IN STATE'S MILITARY CYBERSECURITY

The article focuses on the security of cyberspace issues for military needs. The author identified the main subjects operating in this field with special focus on their tasks, as well as the rules governing their functioning and cooperation. Special attention was given to five main subjects: Plenipotent of the Ministry of Defence for cyberspace security, National Cryptographic Centre, Inspectorate of IT Systems, Departmental Centre of Networks and ICT Services Management, Computer Incident Response System of the Ministry of National Defence. The attachment includes a table showing the construction of institutional defence of the country's military cyberspace.

Key words: cybersecurity, information security, military defence of cyberspace

Załącznik 1

Regulacja	Dec. 357/MON z 2008 r.	Dec Nr. Pf-29/Org/ SSG/ZOiU-P1	Dec. Nr. 101/ORG/ P1 z 2010	Dec. 38/MON z 2012	Dec. 81/MON z 2013	Zarz 10/MON z 2013	Dec. 196/MON z 2013	2013.08.01	Dec. 212/MON (ISI) Dec. 262/ MON z 2013	2013-2014	Dec. 212/MON z 2013	Dec. 243/MON z 2014	Dec. 2/MON z 2015	Dec. 276/MON z 2015	Dec 490/MON z 2015
Data	2008.08.26	2010.04.26	2011.04.01	2012.02.24	2013.04.09	2013.06.01	2013.07.05		2013.10.01		2014.01.01	2014.06.23	2015.01.13	2015.07.14	2015.12.17
Funkcja/podmiot															
Inspektorat Systemów Informacyjnych	Departament Informatyki i Telekomunikacji								Inspektorat Systemów Informacyjnych		ISI (podl Dcy GRSZ, poza dowództw) Podlega pod Podsekretarza Stanu				
Centrum bezpieczeństwa Cybernetycznego SZ (CBC SZ)		Centrum Bezpieczeństwa Cybernetycznego SZ (podlega Szefowi Zarządu Planowania Systemów Dowodzenia i Łączności – P6 Sztabu Generalnego WP.								CBC SZ (podl. NCK)					
RCZBSIUT			RCZBSiUT (podlega Dyr. DIiT MON)							ISI	RCZBSiUT (podlega NCK)				
Centrum Koordynacyjne	WBBŁiI		RCZBSiUT (następca prawny WBBiŁ)									NCK			
Centrum Wsparcia Technicznego	CZST		RCZSiUT następca prawny CZST)									RCZBSiUT (podległe NCK)			
Administratorzy systemów	Administratorzy systemów i sieci teleinformatycznych w jednostkach i komórkach														
Nadzór nad SRnIK	Dyrektor DIiT MON								ISI następca prawny DIiT MON			Pełnomocnik MON ds. Bezpieczeństwa Cyber.			

Regulacja	Dec. 357/MON z 2008 r.	Dec Nr. PF-29/Org/ SSG/ZOiU-P1	Dec. Nr. 101/ORG/ P1 z 2010	Dec. 38/MON z 2012	Dec. 81/MON z 2013	Zarz 10/MON z 2013	Dec. 196/MON z 2013	2013.08.01	Dec. 212/MON (ISI) Dec. 262/ MON z 2013	2013-2014	Dec. 212/MON z 2013	Dec. 243/MON z 2014	Dec. 2/MON z 2015	Dec. 276/MON z 2015	Dec 490/MON z 2015
Data	2008.08.26	2010.04.26	2011.04.01	2012.02.24	2013.04.09	2013.06.01	2013.07.05	2013.08.01	2013.10.01	2013-2014	2014.01.01	2014.06.23	2015.01.13	2015.07.14	2015.12.17
Pełnomocnik MON ds. Bezp. Cyber.				Dyr. DIiT MON					Radca MON ds. Bezp. Cyber. gen. bryg. rez. K. Bondaryk				Podsekretarz Stanu w MON M. Jankowski		Pod. Stan MON B Grabski
Obsługa merytoryczna Pełnomocnika				RCZBSiUT (podległe dyr. DIiT)					ISI (podl. Dyr. Gen MON)		ISI (podl Dcy GRSZ, Poza Dowództ.			CKSRnIK	
NCK	Narodowe Centrum kryptologii														