WICEPREZES
NAJWYŻSZEJ IZBY KONTROLI
WOJCIECH KUTYŁA

KON – 4101-005-01/2014
P/14/043

WYSTĄPIENIE POKONTROLNE

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/14/043 – Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Departament Obrony Narodowej

Kontroler

Andrzej Dominikowski, specjalista kontroli państwowej, upoważnienie do kontroli nr 89155 z dnia 02.06.2014 r.

(Tom 1 dowód: akta kontroli str. 1-2)

Jednostka kontrolowana

Ministerstwo Obrony Narodowej (MON), Al. Niepodległości 218, 00-911 Warszawa

Kierownik jednostki kontrolowanej

Tomasz Siemoniak, Minister Obrony Narodowej od 2 sierpnia 2011 r.
Bogdan Klich, Minister Obrony Narodowej od 16 listopada 2007 r. do 2 sierpnia 2011 r.

Okres objęty kontrolą

Badaniem objęto okres od początku 2008 r. do dnia 29 października 2014 r.

Wykaz niektórych użytych skrótów

CBC SZ	Centrum Bezpieczeństwa Cybernetycznego Sił Zbrojnych
COC	Centrum Operacji Cybernetycznych
CZK MON	Centrum Zarządzania Kryzysowego MON
CZST	Centrum Zarządzania Systemami Teleinformatycznymi
D-ca GRSZ	Dowódca Generalny Rodzajów Sił Zbrojnych
DIiT	Departament Informatyki i Telekomunikacji
ISI	Inspektorat Systemów Informacyjnych
KPZK	Krajowy Plan Zarządzania Kryzysowego
KRMC	Komitet Rady Ministrów ds. Cyfryzacji
MAiC	Ministerstwo Administracji i Cyfryzacji
NCBR	Narodowe Centrum Badań i Rozwoju
NCK	Narodowe Centrum Kryptologii
RCB	Rządowe Centrum Bezpieczeństwa
RCZBSiUT	Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych
RCZSiUT	Resortowego Centrum Zarządzania Sieciami i Usługami Teleinformatycznymi
RON	Resort Obrony Narodowej
SRnIK	Systemu Reagowania na Incydenty Komputerowe
WAT	Wojskowa Akademia Techniczna
WBBŁiI	Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki

II. Ocena kontrolowanej działalności

Ocena ogólna

Kontrola wykazała, że w resorcie obrony narodowej (resorcie ON) podejmowane były działania w zakresie budowania systemu instytucjonalnego ochrony cyberprzestrzeni i ram dla jego funkcjonowania ukierunkowane na rozbudowę bezpieczeństwa cyberprzestrzeni, które w wielu aspektach były zbieżne z założeniami rządowej *„Polityki ochrony cyberprzestrzeni Rzeczypospolitej Polskiej"*.

W szczególności utworzono i rozwijano system reagowania na incydenty komputerowe, opracowano katalog (klasyfikację) incydentów i przyporządkowany do nich zbiór procedur działania, prowadzono wymianę informacji z innymi podmiotami państwowymi realizującymi zadania w zakresie ochrony cyberprzestrzeni RP, określono wskaźniki (mierniki realizacji zadań) w powiązaniu z szacowaniem ryzyka, przyjęto *„Politykę resortu obrony narodowej w zakresie bezpieczeństwa cyberprzestrzeni"* oraz opracowano *„Projekt Założeń do Planu Obrony Cyberprzestrzeni"*.

Resort ON zrealizował zadanie dotyczące szacowania ryzyka związanego z zagrożeniami występującymi w cyberprzestrzeni zgodnie z metodyką otrzymaną z MAiC oraz podejmowane były działania w ramach planowania zarządzania kryzysowego w zakresie określenia zagrożeń i szacowania ryzyka ich wystąpienia.

W resorcie ON podejmowano działania w zakresie wzmacniania zdolności w ramach ochrony cyberprzestrzeni, w tym ustanowiono wymogi w zakresie bezpieczeństwa teleinformatycznego.

Przedstawiciele resortu ON brali udział w ćwiczeniach systemu bezpieczeństwa cyberprzestrzeni, przeprowadzano testy systemów i sieci teleinformatycznych.

Ustanowiono i rozwijano zespół MIL-CERT.PL, który funkcjonował w ramach infrastruktury teleinformatycznej systemu wczesnego ostrzegania przed zagrożeniami.

Realizowano działania w zakresie szkoleń i działania edukacyjne, a także wspierano działalność badawczą i rozwojową.

W działalności kontrolowanej jednostki stwierdzono występowanie następujących problemów o charakterze systemowym:

- dokonywanie *ad hoc* zmian w systemie instytucjonalnym i w strukturach organizacyjnych, tj. przy braku zatwierdzonego i normatywnie opisanego całościowego, docelowego modelu organizacji systemu ochrony cyberprzestrzeni z określonym harmonogramem realizacji,
- brak oszacowania zasobów i kosztów dotyczących ochrony cyberprzestrzeni,
- brak umiejscowienia działalności w zakresie ochrony cyberprzestrzeni w strukturze budżetu zadaniowego i w procesie planowania wydatków resortu ON.

W wyniku kontroli zidentyfikowano obszary ryzyka mogące mieć wpływ na utrzymanie odpowiednio wysokiego poziomu kompetencji oraz na jakość realizacji zadań w resorcie ON:

- duża liczba zmian w ramach systemu instytucjonalnego,
- brak określania z wyprzedzeniem potrzebnych środków finansowych,
- oparcie systemu na nowej, formułującej się jednostce o profilu działalności wyspecjalizowanej tylko w jednym elemencie z zakresu bezpieczeństwa teleinformatycznego (kryptologii), prowadzonej głównie w ramach działalności naukowo-edukacyjnej i badawczo-rozwojowej (NCK),
- oparcie systemu na jednej osobie kierującej, której odejście mogłoby zagrozić ciągłości funkcjonowania organizacji w danej dziedzinie,

– nieskorelowanie zmian faktycznych ze zmianami uregulowań wewnętrznych.

Ponadto NIK zwraca uwagę na konieczność wzmocnienia współpracy resortu ON i MAiC, w tym na potrzebę wypracowania sposobu przekazywania informacji, w tym niejawnych, do MAiC.

III. Opis ustalonego stanu faktycznego

1. Struktura organizacyjna i uwarunkowania prawne systemu ochrony cyberprzestrzeni w resorcie obrony narodowej

1.1. Ramy prawne systemu ochrony cyberprzestrzeni RP w resorcie obrony narodowej. Działania legislacyjne

Opis stanu faktycznego

W dniu 25 czerwca 2013 r. Rada Ministrów przyjęła *„Politykę ochrony cyberprzestrzeni Rzeczypospolitej Polskiej"*[1] – dokument obowiązujący dla administracji rządowej, w którym określono założenia dotyczące kierunków działań, które należy podjąć w celu osiągnięcia akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Państwa[2]. Osiągnięcie tego celu strategicznego ma być realizowane m.in. poprzez stworzenie ram organizacyjno-prawnych. Jako podstawowy element realizacji *„Polityki..."*, przewidziany niezwłocznie do wykonania, wskazano działania legislacyjne - zwłaszcza zainicjowanie przez ministra właściwego ds. informatyzacji mające na celu opracowanie regulacji prawnych, dające podstawy do podejmowania dalszych działań w ramach wdrożenia zapisów *„Polityki..."*.

W resorcie ON, w tym w Ministerstwie Obrony Narodowej, nie opracowano katalogu (wykazu) konkretnych propozycji legislacyjnych koniecznych do wprowadzenia w celu wdrożenia systemu ochrony cyberprzestrzeni RP. W *„Polityce resortu obrony narodowej w zakresie bezpieczeństwa cyberprzestrzeni"* z czerwca 2014 r.[3] wskazano jedynie, że oprócz Ministra ON, który wydaje decyzje i zarządzenia dotyczące bezpieczeństwa cyberprzestrzeni resortu ON, także Pełnomocnik Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni, za pomocą wytycznych oraz zaleceń, w zakresie posiadanych uprawnień, określa kierunki działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni resortu ON.

Dokumenty normatywne wydane w resorcie ON w latach 2008-2014

W badanym okresie (w latach 2008–2014) w celu unormowania zadań związanych z ochroną cyberprzestrzeni RP zostały wydane m.in.:

– 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[4],

---

[1] Zgodnie z pkt. 1.1. „Polityki..." cyberprzestrzeń RP to cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe).

[2] Zgodnie z pkt. 1 ww. dokumentu: „Polityka" nie obejmuje swoim obszarem zadaniowym niejawnych systemów teleinformatycznych - obszar ochrony informacji niejawnych posiada własne regulacje prawne i stosowne mechanizmy ochronne. Posiada struktury organizacyjne dedykowane do ochrony informacji niejawnych wytwarzanych, przetwarzanych oraz przechowywanych w wydzielonych systemach teleinformatycznych. Podstawowym aktem prawnym jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).

[3] Dokument zaakceptowany przez Ministra Obrony Narodowej 13 czerwca 2014 r.

[4] Dz. Urz. MON Nr 16, poz. 205; ww. decyzję Nr 357/MON uchyliła z dniem 23 czerwca 2014 r. aktualnie obowiązująca decyzja w przedmiotowej sprawie Nr 243/MON z dnia 18 czerwca 2014 r. (Dz. Urz. MON z 2104 r. poz. 203)

- decyzja Nr Pf-29/Org./SSG/ZOiU-P1 Ministra Obrony Narodowej z dnia 26 kwietnia 2010 r. w sprawie sformowania Centrum Bezpieczeństwa Cybernetycznego Sił Zbrojnych (dokument niejawny),
- decyzja Nr 101/Org./P1 Ministra Obrony Narodowej z dnia 26 listopada 2010 r. w sprawie zmian organizacyjnych w jednostkach łączności i informatyki (dokument niepublikowany),
- decyzja Nr 7/MON Ministra Obrony Narodowej z dnia 20 stycznia 2012 r. w sprawie organizacji ochrony systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych w resorcie obrony narodowej[5],
- decyzja Nr 38/MON Ministra Obrony Narodowej z dnia 16 lutego 2012 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni[6],
- decyzja Nr 81/MON Ministra Obrony Narodowej z dnia 9 kwietnia 2013 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do Spraw Utworzenia Narodowego Centrum Kryptologii[7],
- zarządzenie Nr 10/MON Ministra Obrony Narodowej z dnia 23 kwietnia 2013 r. w sprawie utworzenia i nadania statutu państwowej jednostce budżetowej – Narodowe Centrum Kryptologii[8],
- decyzja Nr 196/MON Ministra Obrony Narodowej z dnia 5 lipca 2013 r. w sprawie powołania Zespołu do Spraw Opracowania Założeń do Planu Obrony Cyberprzestrzeni Rzeczypospolitej Polskiej (dokument niepublikowany),
- decyzja Nr 212/MON Ministra Obrony Narodowej z dnia 24 lipca 2013 r. w sprawie sformowania Inspektoratu Systemów Informacyjnych oraz rozformowania Departamentu Informatyki i Telekomunikacji[9],
- „*Program naprawczy w zakresie bezpieczeństwa teleinformatycznego w resorcie obrony narodowej*" – dokument zaakceptowany przez Ministra Obrony Narodowej 18 września 2013 r.[10],
- decyzja Nr 261/MON Ministra Obrony Narodowej z dnia 19 września 2013 r. w sprawie usprawnienia systemów komunikacji elektronicznej w resorcie obrony narodowej[11],
- decyzja Nr 262/MON Ministra Obrony Narodowej z dnia 19 września 2013 r. zmieniająca decyzję w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni[12],
- decyzja Nr Z-45/Org./P1 Ministra Obrony Narodowej z dnia 13 listopada 2013 r. w sprawie zmiany bezpośredniego podporządkowania Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych oraz Centrum Bezpieczeństwa Cybernetycznego Sił Zbrojnych Rzeczypospolitej Polskiej (dokument niejawny),

---

[5] Dz.Urz. MON z 2012 r. poz. 8.

[6] Dz.Urz. MON z 2012 r. poz. 52 ze zm.

[7] Dz.Urz. MON z 2013 r. poz. 88.

[8] Dz.Urz. MON z 2013 r. poz. 121 ze zm.

[9] Dz.Urz. MON z 2013 r. poz. 194.

[10] Dokument (niejawny) wydany w związku z wystąpieniem incydentu komputerowego o szczególnym znaczeniu.

[11] Dz.Urz. MON z 2013 r. poz. 227.

[12] Dz.Urz. MON z 2013 r. poz. 228.

- wytyczne Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni w sprawie szczegółowych zasad i zadań w zakresie kontroli dostępu do systemu, poufności informacji oraz rozliczalności funkcjonowania systemu INTER-MON z dnia 30 grudnia 2013 r. (dokument niejawny),
- *„Projekt Założeń do Planu Obrony Cyberprzestrzeni RP"* zaakceptowany przez Ministra Obrony Narodowej w dniu 21 maja 2014 r. (dokument niejawny),
- *„Polityka resortu obrony narodowej w zakresie bezpieczeństwa cyberprzestrzeni"* – dokument zaakceptowany przez Ministra Obrony Narodowej w dniu 13 czerwca 2014 r. (dokument niepublikowany),
- decyzja Nr 243/MON Ministra Obrony Narodowej z dnia 18 czerwca 2014 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej[13],
- zarządzenie Nr 14/MON Ministra Obrony Narodowej z dnia 18 czerwca 2014 r. zmieniające zarządzenie w sprawie utworzenia i nadania statutu państwowej jednostce budżetowej - Narodowe Centrum Kryptologii[14].

(dowód: akta kontroli Tom 1 str. 11-12, 15-24, 29-32, 45-47, 469-474, Tom 2 str. 109-349)

Zgłoszone i procedowane propozycje zmian regulacji

Zgłoszone zostały także propozycje zmian regulacji w zakresie dotyczącym:

- obsługi merytorycznej Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni

  Pełnomocnik Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni (gen. bryg. rez. K. Bondaryk) dwukrotnie (9 stycznia 2014 r. i 8 sierpnia 2014 r.) przedkładał projekt decyzji zmieniającej ww. decyzję Nr 38/MON z 2012 r. proponując, aby zamiast Inspektoratu Systemów Informacyjnych, obsługę merytoryczną ww. Pełnomocnika zapewniało Narodowe Centrum Kryptologii. W uzasadnieniu do ww. projektu ze stycznia 2014 r. wskazał, że *„potrzeba zmiany wynika z dokonanych zmian organizacyjnych w resorcie ON, polegających na zwiększeniu zdolności NCK wraz z jednostkami podporządkowanymi (RCZBSiUT, CBC SZ), do wykonywania zadań"* m.in. z zakresu bezpieczeństwa cyberprzestrzeni. W ww. projekcie z sierpnia 2014 r. zaproponowano ponadto m.in. zmiany dotyczące kompetencji Pełnomocnika w zakresie udostępniania mu dokumentów i informacji.

  Dyrektor NCK (gen. bryg. rez. K. Bondaryk) wyjaśnił, że *„ISI w momencie zmiany w 2013 r. decyzji Nr 38/MON z 2012 r. był jednostką organizacyjną podporządkowaną Dyrektorowi Generalnemu MON. Od dnia 1 stycznia 2014 r.[15] ISI przeszedł w podporządkowanie Dowódcy Generalnego Rodzajów Sił Zbrojnych, co spowodowało podjęcie działań przez Pełnomocnika Ministra ON ds. Bezpieczeństwa Cyberprzestrzeni* [gen. bryg. rez. K. Bondaryka], *których celem była zmiana na drodze legislacyjnej komórki organizacyjnej odpowiedzialnej obsługę merytoryczną z ISI na NCK."*

  (dowód: akta kontroli Tom 1 str. 36-44, 50-51)

[13] Dz.Urz. MON z 2014 r. poz. 203.

[14] Dz.Urz. MON z 2014 r. poz. 205.

[15] Zgodnie z pkt. 12 ww. decyzji Nr 212/MON z dnia 24 lipca 2013 r. (sformowanie Inspektoratu Systemów Informacyjnych oraz rozformowanie Departamentu Informatyki i Telekomunikacji).

– specjalności wojskowych

W resorcie ON opracowano[16] projekt rozporządzenia Ministra Obrony Narodowej zmieniającego rozporządzenie w sprawie korpusów osobowych, grup osobowych i specjalności wojskowych, w którym zaproponowano m.in. wprowadzenie nowego korpusu osobowego, tj. korpusu osobowego kryptologii i cyberbezpieczeństwa, składającego się z dwóch grup osobowych („A - grupa osobowa kryptologii" i „B - grupa osobowa cyberbezpieczeństwa") oraz zmiany zapisów dotyczących korpusu osobowego łączności i informatyki.

(dowód: akta kontroli Tom 1 str. 84, 92, 103-119)

Identyfikowane przez resort ON niezbędne kierunki zmian legislacyjnych

Kierunki zmian w obszarze prawnym wskazano w kwietniu 2014 r. w niejawnym dokumencie *„Projekt Założeń do Planu Obrony Cyberprzestrzeni Rzeczypospolitej Polskiej"*. W dokumencie tym stwierdzono[17] m.in., że:

– w przepisach krajowych brak jest regulacji uprawniających określone podmioty czy jednostki organizacyjne do przygotowywania i (w razie konieczności) przeprowadzania działań obronnych w cyberprzestrzeni (dotyczy to również trybu i procedur podejmowania decyzji o ich zastosowaniu). W sensie prawnym, zastosowanie środków obronnych w cyberprzestrzeni musi być rozpatrywane według tych samych przepisów, które dotyczą klasycznego konfliktu zbrojnego. Nadal, mimo wprowadzenia do systemu prawnego definicji cyberprzestrzeni, nie wprowadzono możliwości przeprowadzania działań i wprowadzania ograniczeń charakterystycznych dla konfliktu lub kryzysu w cyberprzestrzeni (zawieszenie części lub wyłączenie całości usług internetowych);

– międzynarodowe prawo konfliktów zbrojnych nie wyczerpuje złożoności problematyki konfliktu w cyberprzestrzeni. Problematyka prowadzenia działań w cyberprzestrzeni przez NATO, jak i poszczególne kraje członkowskie sojuszu, nie została dotychczas szczegółowo uregulowana;

– implementacja przez Polskę dyrektywy 2013/40 UE[18] (w dorobku prawnym UE głównej regulacji dotyczącej ataków na systemy informatyczne) będzie wymagała zmiany szeregu aktów prawnych, co może wpłynąć na uwarunkowania działań w cyberprzestrzeni prowadzonych przez Siły Zbrojne RP.

W dokumencie tym wskazano, że należy dokonać zmian legislacyjnych pozwalających na zabezpieczenie potrzeb obrony cybernetycznej, a w szczególności w:

– ustawie z dnia 18 lipca 2002 r. o świadczeniu usług droga elektroniczną[19] - wprowadzić zmiany dotyczące świadczenia usług na rzecz obronności państwa,

– ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[20] oraz w ustawie z dnia 21 czerwca 2002 r. o stanie wyjątkowym[21] i ustawie z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej[22]

---

[16] Według stanu na 29 sierpnia 2014 r. projekt był w fazie uzgodnień.

[17] W części jawnej.

[18] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz. Urz. UE L 218 z 14.08.2013 r., str. 8).

[19] Dz.U. z 2013 r. poz. 1422.

[20] Dz.U. Nr 156 poz. 1301, ze zm.

[21] Dz.U. z 2014 r. poz. 1191.

[22] Dz.U. z 2014 r. poz. 333, ze zm.

- nadając Siłom Zbrojnym uprawnienia w odniesieniu do realizacji zadań związanych z ochroną cyberprzestrzeni RP,

– ustawie z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej[23] – dokonać zmian zgodnie z nowym systemem dowodzenia oraz w zakresie administracji rezerwami osobowymi, w odniesieniu do specjalistów z zakresu bezpieczeństwa teleinformatycznego,

– ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne[24] – wprowadzić zmiany w zakresie obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w szczególności obowiązków w zakresie ochrony i obrony zasobów informacyjnych i uzgadniania planów z Pełnomocnikiem Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni oraz w obszarze bezpieczeństwa i integralności sieci oraz usług telekomunikacyjnych, uwzględniając rolę zespołów CERT.GOV.PL oraz MIL-CERT-PL.

(dowód: akta kontroli Tom 1 str. 469-478, Tom 2 str. 120-143)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

1.2. System ochrony cyberprzestrzeni w RON - struktura, podział zadań i podmioty odpowiedzialne

Opis stanu faktycznego

Zgodnie z pkt. 3.4. 3. rząd owej *„Polityki..."*, - rola pełnomocnika ds. bezpieczeństwa cyberprzestrzeni powinna zostać przypisana osobie odpowiedzialnej za realizację procesu bezpieczeństwa teleinformatycznego. *„Polityka..."* nie wskazuje miejsca usytuowania pełnomocnika ds. bezpieczeństwa cyberprzestrzeni w strukturze jednostki organizacyjnej.

Obecny system instytucjonalny w zakresie ochrony cyberprzestrzeni w resorcie ON

W resorcie ON osobami odpowiedzialnymi i podmiotami mającymi zapewniać realizację zadań w ramach bezpieczeństwa cyberprzestrzeni RP są[25]:

a) Minister Obrony Narodowej,

b) Pełnomocnik Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni[26] – poprzez którego Minister pełni nadzór (od 23.06.2014 r.)[27]

---

[23] Dz.U. z 2012 r., poz. 461, ze zm.

[24] Dz.U. z 2014 r., poz. 243.

[25] Stan na dzień 31 sierpnia 2014 r. Odpowiedzialność podmiotów w resorcie ON określona jest w ww. dokumentach i regulacjach: *„Polityka resortu ON..."*, ww. decyzje Ministra Obrony Narodowej (Nr 38/MON z 16.02.2012 r., Nr 262/MON z 19.09.2012 r., Nr 243/MON z 18.06.2014 r.), ww. Wytyczne Pełnomocnika z 30 grudnia 2013 r.

[26] Zgodnie z pkt. 3 ppkt 1, 2, 3 ww. decyzji Nr 38/MON z 16.02.2012 r. Pełnomocnik jest upoważniony m.in. do:

1) koordynowania przedsięwzięć przewidzianych dla Ministra Obrony Narodowej w sprawach bezpieczeństwa cyberprzestrzeni, w odniesieniu do wszystkich komórek organizacyjnych MON i jednostek organizacyjnych podległego resortu, z wyłączeniem zadań zastrzeżonych dla pełnomocników do spraw ochrony informacji niejawnych określonych odrębnymi przepisami;

2) inicjowania oraz wspierania działań komórek organizacyjnych MON i jednostek resortu w obszarze osiągania zdolności do zapewnienia bezpieczeństwa cyberprzestrzeni resortu ON;

3) sprawowania nadzoru nad realizacją zadań dotyczących zapewnienia bezpieczeństwa cyberprzestrzeni.

[27] Zgodnie z pkt. 3 ww. decyzji Nr 243/MON z dnia 18 czerwca 2014 r. Wcześniej: nadzór nad funkcjonowaniem SRnIK sprawował Dyrektor DIiT MON (od 26.08.2008 r. do 30.09.2013 r.) i jego następca prawny Szef ISI (od 01.10.2013 r. do 22.06.2014 r.).

nad działaniem Systemu Reagowania na Incydenty Komputerowe resortu ON (SRnIK),

c) SRnIK[28] - zorganizowany w trzypoziomową strukturę, w skład której wchodzą:

- Centrum Koordynacyjne SRnIK, którego funkcję spełnia właściwa komórka wewnętrzna Narodowego Centrum Kryptologii[29],
- Centrum Techniczne SRnIK, którego funkcję pełni komórka wewnętrzna RCZBSiUT, tj. Oddział Bieżącego Zarządzania Bezpieczeństwem Teleinformatycznym (MIL-CERT.PL),
- administratorzy systemów teleinformatycznych w jednostkach resortu ON i komórkach organizacyjnych MON,
- Inspektorat Systemów Informacyjnych – wypełniający zadania: administratora sieci i kluczowych usług teleinformatycznych, organizatora systemów teleinformatycznych, gestora korpusu osobowego łączności i informatyki oraz gestora sprzętu i oprogramowania informatycznego,
- inne komórki i jednostki organizacyjne, w tym: Zarząd Planowania Systemów Dowodzenia i Łączności (P-6) Sztabu Generalnego Wojska Polskiego – jako organizator systemu funkcjonalnego[30], RCZBSiUT, Narodowe Centrum Kryptologii oraz Centrum Bezpieczeństwa Cybernetycznego SZ[31].

Zmiany w systemie instytucjonalnym w zakresie ochrony cyberprzestrzeni w resorcie ON w latach 2008 – 2014

Istotny wpływ na kształtowanie systemu instytucjonalnego w zakresie ochrony cyberprzestrzeni w resorcie ON miały incydenty komputerowe (zwłaszcza *„o szczególnym znaczeniu"*) i działania podejmowane w ramach resortu ON w reakcji na ich wystąpienie[32]. Do głównych incydentów komputerowych i ww. działań należały:

- incydent w sieciach teleinformatycznych administracji rządowej (głównie KPRM i MSZ) – początek 2013 r. – w odpowiedzi: propozycja[33] utworzenia - w ramach wspólnego działania instytucji rządowych (MON we współpracy z MSW, ABW i MAiC) - Narodowego Centrum Kryptologii (NCK), tj. centralnego ośrodka, który na potrzeby państwa prowadziłby m.in. badania, projektowanie, użytkowanie oraz ochronę narodowych technologii kryptograficznych;

---

[28] Struktura powstała w efekcie zmian w SRnIK po przyjęciu decyzji MON Nr 243/MON i zarządzenia MON Nr 14/MON (oba akty z dnia 18.06.2014 r.).

[29] Wg stanu na 31.08.2014 r.): Nieetatowy Zespół ds. Obrony Cybernetycznej w NCK (decyzje Dyrektora NCK: 10/Org./2014 z dnia 25 kwietnia 2014 r. i 24/Org./2014 z dnia 29 lipca 2014 r.).

[30] Decyzja Nr 56/Org./P5 Ministra Obrony Narodowej z dnia 24 grudnia 2013 r. w sprawie Organizatorów Systemów Funkcjonalnych Sił Zbrojnych Rzeczypospolitej Polskiej (dokument niepublikowany).

[31] Jednostka utworzona w 2010 r. (na podstawie ww. decyzji Nr Pf-29/Org/SSG/ZOiU-P1 Ministra Obrony Narodowej z dnia 26 kwietnia 2010 r.) jako wyspecjalizowana jednostka wojskowej, której głównym zadaniem jest obrona cyberprzestrzeni poprzez prowadzenie działań w cyberprzestrzeni.

[32] Szczegółowe informacje stanowią informacje niejawne.

[33] Propozycja Radcy Ministra Obrony Narodowej gen. bryg. rez. K. Bondaryka w ramach rekomendacji (od 24 września 2014 r. – jawnych) skierowanych w dniu 2 kwietnia 2013 r. do Ministra Obrony Narodowej w odniesieniu do *„Raportu ABW dotyczącego incydentów teleinformatycznych w sieciach administracji rządowej – stan na dzień 13.03.2013 r."*. Wcześniej idea utworzenia centralnego ośrodka w podobnym obszarze dziedzinowym pojawiła się w projekcie pn. *„Ochrona informacji istotnych dla bezpieczeństwa i funkcjonowania państwa, w tym o klauzuli „Ściśle Tajne" - Budowy narodowego centrum kryptografii i dekryptażu"* (zgłoszonym przez ABW do Narodowego Centrum Badań i Rozwoju – do konkursu projektów badawczych 2011 r.).

- incydent w resortowej sieci (jawnej) INTER-MON (atak na konta poczty elektronicznej) – połowa 2013 r. i ostatni kwartał 2013 r. – w odpowiedzi m.in.: zmiana Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cybernetycznego, przyjęcie *„Programu naprawczego..."*, wydanie „Wytycznych *Pełnomocnika..."* i decyzji Nr 261/MON, zmiana podporządkowania RCZBSiUT;
- incydent w resortowej sieci (jawnej) INTER-MON (atak na konta poczty elektronicznej) – luty 2014 r. – w odpowiedzi: przyjęcie resortowej *„Polityki..."*, zmiany w zakresie organizacji i funkcjonowania SRnIK.

(dowód: akta kontroli Tom 1 str. 453-463, 494-497, 531-535, Tom 2 str. 109-324)

Zmiany systemu instytucjonalnego w resorcie ON w zakresie ochrony cyberprzestrzeni przedstawia Diagram nr 1.

Do 30 września 2013 r. Pełnomocnikiem Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni był Dyrektor Departamentu Informatyki i Telekomunikacji MON. Od 1 października 2013 r. funkcję Pełnomocnika pełni Radca Ministra Obrony Narodowej ds. Bezpieczeństwa Cybernetycznego gen. bryg. rez. Krzysztof Bondaryk.

Zgodnie z zatwierdzonymi w dniu 28 czerwca 2013 r. przez Ministra Obrony Narodowej dokumentami: *„MODEL 2013 – Zmiany podporządkowania jednostek MON i SZ RP"* oraz *„Sposób transformacji organów kierowania i dowodzenia SZ RP"*, od 1 października 2013 r. został sformowany Inspektorat Systemów Informacyjnych (jako następca prawny DIiT MON), pod który zaplanowano podporządkowanie jednostek związanych z zapewnieniem zabezpieczenia teleinformatycznego, w tym RCZBSiUT oraz CBC SZ. W celu umożliwienia realizacji zadań nałożonych na nowego Pełnomocnika Ministra Obrony Narodowej, uwzględniając fakt, że Inspektoratowi Systemów Informacyjnych miały być podporządkowane jednostki wykonawcze w obszarze bezpieczeństwa cyberprzestrzeni (RCZBSiUT oraz CBC SZ), obsługę merytoryczną[34] powierzono ISI.

Dyrektor Departamentu Prawnego MON wyjaśnił, że *„sytuacja, w której obsługę merytoryczną zapewnia podmiot bez relacji bezpośredniej podległości lub podporządkowania, jest modelem stosowanym w resorcie ON (...)."*

Tworzenie SRnIK rozpoczęto w 2008 r. decyzją Nr 357/MON z dnia 29 lipca 2008 r. Obecny kształt organizacyjny Systemu Reagowania na Incydenty Komputerowe (SRnIK) jest efektem kolejnych zmian organizacyjnych w resorcie ON.

Pierwotnie funkcję Centrum Koordynacyjnego SRnIK pełniło Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki. Natomiast rolę Centrum Wsparcia Technicznego powierzono Centrum Zarządzania Systemami Teleinformatycznymi, a sprawowanie nadzoru nad SRnIK Dyrektorowi DIiT MON.

Następnie, z dniem 1 kwietnia 2011 r.[35], Minister Obrony Narodowej postanowił o utworzeniu:

- Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych – RCZBSiUT, które przejęło (po WBBŁiI jako jego następca prawny) funkcję Centrum Koordynacyjnego SRnIK;
- Resortowego Centrum Zarządzania Sieciami i Usługami Teleinformatycznymi – RCZSiUT, które przejęło (po CZST jako jego następca prawny) funkcję Centrum Wsparcia Technicznego.

---

[34] Tzn. zapewnienie wsparcia przez dostarczanie informacji i wykonywanie działań przez komórkę organizacyjną, w której właściwości znajdują się zagadnienia będące przedmiotem działania.

[35] Ww. decyzja Nr 101/Org./P1 Ministra Obrony Narodowej z dnia 26 listopada 2010 r. w sprawie zmian organizacyjnych w jednostkach łączności i informatyki (dokument niepublikowany).

Pełnomocnik Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni wyjaśnił, że *„Minister ON zdecydował o utworzeniu w 2011 r. ww. jednostek (RCZBSiUT i RCZSiUT) w celu podniesienia jakości funkcjonowania SRnIK i w związku z rosnącymi zagrożeniami."*

1 czerwca 2013 r. Minister Obrony Narodowej utworzył Narodowe Centrum Kryptologii[36], do którego zadań należy konsolidacja kompetencji i zasobów resortu ON w obszarze kryptologii, w szczególności prowadzenie badań, projektowanie oraz wytwarzanie nowych produktów w ramach działalności m.in. badawczo-rozwojowej i wdrożeniowej w zakresie związanym z kryptologią.

Pełnomocnik Ministra ON ds. Bezpieczeństwa Cyberprzestrzeni wyjaśnił, że *„Minister ON zdecydował o sformowaniu z dniem 1 czerwca 2013 r. kolejnej* [m.in. po RCZBSiUT i CBC SZ] *wyspecjalizowanej jednostki wojskowej - NCK, w celu podniesienia poziomu bezpieczeństwa informacji przetwarzanych w cyberprzestrzeni resortu ON. Zadaniem tej jednostki jest zabezpieczanie pod względem kryptograficznym informacji przetwarzanych w systemach teleinformatycznych eksploatowanych w MON i SZ RP. Pełni ono rolę centrum kompetencji kryptologicznych RON."*

(dowód: akta kontroli Tom 1 str. 13-16, 24-28, 38, 44-51, 198-210, Tom 2 str. 109-349)

Współpraca komórek i jednostek organizacyjnych resortu ON na szczeblu resortowym, krajowym i międzynarodowym

Regulacje powołujące ww. Pełnomocnika Ministra Obrony Narodowej i SRnIK określiły także obowiązek współpracy na szczeblu resortowym i krajowym komórek i jednostek organizacyjnych resortu ON oraz współpracy na szczeblu międzynarodowym podmiotów z resortu ON w zakresie obrony cyberprzestrzeni.

Podmioty z resortu ON na forum międzynarodowym podjęły współpracę m.in. z:

- Departamentem Obrony USA – porozumienie z dnia 21 czerwca 2010 r.,
- NATO Cyber Defence Management Authority – porozumienie z dnia 12 kwietnia 2011 r.,
- Czeską Republiką – powołano grupę roboczą ds. bezpieczeństwa cyberprzestrzeni.

(dowód: akta kontroli Tom 1 str. 13-16, 279-307)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

1.3. Zasoby i wydatki

Opis stanu faktycznego

Planowanie i finansowanie

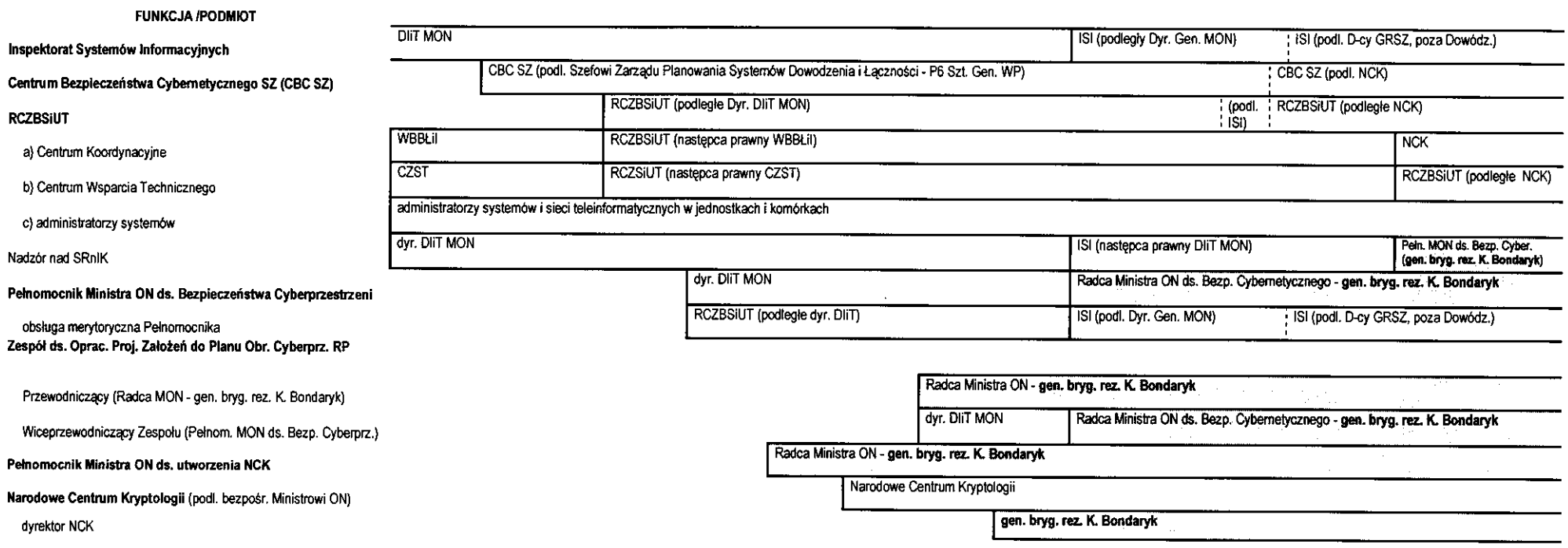
Resort ON, w tym MON, nie przekazywał Ministerstwu Administracji i Cyfryzacji, po zatwierdzeniu rządowej *„Polityki..."* - mimo zapisów w pkt. 5 *„Polityki..."* – informacji na temat zrealizowanych dotychczas zadań oraz wydatków poniesionych w związku z ochroną cyberprzestrzeni RP oraz informacji na temat wydatków (oraz innych przypisanych zasobów) zaplanowanych na lata 2014 i 2015 w związku z realizacją zadań dotyczących ochrony cyberprzestrzeni RP.

W obowiązującej w resorcie ON klasyfikacji budżetowej nie ma bezpośredniego wydzielenia wydatków z przeznaczeniem na rzecz ochrony cyberprzestrzeni.

[36] § 1 ww. zarządzenia Nr 10/MON z dnia 29 kwietnia 2013 r.

Diagram nr 1. Zmiany w systemie instytucjonalnym w zakresie ochrony cyberprzestrzeni w resorcie ON w latach 2008–2014

Regulacja	dec. 357/MON z 2008 r.	dec. Nr Pf - 29/Org./SSG/ZOiU-P1	dec. Nr 101/Org./P1 z 2010 r.	dec. 38/MON z 2012 r.	dec. 81/MON z 2013 r.	dec. 10/MON z 2013 r.	dec. 196/MON z 2013 r.	2013.08.01	dec. 212/MON (ISI); dec. 262/MON (Pełn.) z 2013 r.	2013-2014	dec. 212/MON z 2013 r.	dec. 243/MON z 2014 r.
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



Źródło: Opracowanie kontrolera NIK.

Z wyjaśnień członków Kierownictwa MON[37] wynika, że *„MON nie przekazywał do MAiC tych danych ze względu na ich wstępny, poglądowy charakter. (...) Problem odseparowania tematyki obrony cyberprzestrzeni jako odrębnej zdolności jest przedmiotem prac koncepcyjnych, pozwalających w przyszłości wydzielać dedykowane dla cyberbezpieczeństwa zasoby osobowe, rzeczowe i finansowe. (...) Prowadzony obecnie Przegląd Potrzeb Sił Zbrojnych RP (jeden z elementów programowania SZ RP), pozwoli zdefiniować potrzeby i wymagania operacyjne ochrony cyberprzestrzeni oraz sposób i warunki ich realizacji w perspektywie średnioterminowej (10 lat)."*

Zastępca dyrektora NCK na posiedzeniu sejmowej Komisji Obrony Narodowej w dniu 7 maja 2014 r.[38] poinformował, że *„NCK uważa za niezbędne utworzenie w ramach programu rozwoju Sił Zbrojnych w latach 2013-2022 nowego programu operacyjnego wsparcia kryptograficznego i obrony cyberprzestrzeni. (...) umożliwi to zabezpieczenie wyłącznej jurysdykcji państwa nad wojskowymi systemami kierowania, dowodzenia i łączności w obszarze technologicznym, uzyskanie przez Siły Zbrojne RP gotowości do prowadzenia operacji w cyberprzestrzeni poprzez polskie narzędzia informatyczne i oprogramowanie, odbudowę kryptografii i kryptoanalizy wojskowej, uzyskanie przez Polskę wiodącej roli w wielonarodowych inicjatywach rozwoju sojuszniczych zdolności obronnych, zgodnie z aktualnymi strategiami NATO, Unii Europejskiej, czy grupy wyszehradzkiej, podniesienie znaczenia wiarygodności państwa na arenie międzynarodowej (...)."*

(dowód: akta kontroli Tom 1 str. 97-103, 118-119, 444, 460-461, 512-530)

Zasoby osobowe

W ocenie wyrażonej przez Ministra Obrony Narodowej resort ON nie dysponuje odpowiednią liczbą specjalistów posiadających wystarczające kwalifikacje w obszarze obrony cyberprzestrzeni.

(dowód: akta kontroli Tom 1 str. 77, 84)

Minister Obrony Narodowej wyjaśnił, że *„w resorcie ON funkcjonuje zunifikowany system wynagrodzeń żołnierzy i pracowników wojska dotyczący również specjalistów cyberbezpieczeństwa. Nie stosuje się systemu zachęt mających na celu pozyskanie i utrzymanie pracowników o niezbędnych kwalifikacjach w obszarze ochrony cyberprzestrzeni. O wprowadzenie takiego systemu wnioskował Pełnomocnik Ministra ON ds. Bezpieczeństwa Cyberprzestrzeni."*

(dowód: akta kontroli Tom 1 str. 77, 84)

Z otrzymanych z resortu ON informacji[39] wynika, że według stanu na dzień 9 października 2014 r. stan ukompletowania żołnierzami zawodowymi (żz) oraz pracownikami wojska (pw) w NCK i jednostkach bezpośrednio podporządkowanych kształtował się na poziomie 40% stanu docelowego, w tym: NCK 36% obsady etatowej (41% żz i 34% pw); CBC SZ 34% (27% żz i 83% pw) oraz RCZBSiUT 94%, w (88% żz i 100% pw).

Zastępca Dyrektora NCK[40] wyjaśnił, że *„NCK od momentu utworzenia w dniu 1 czerwca 2013 r. podejmowało szereg działań zmierzających do wyznaczenia żołnierzy w ww.*

---

[37] W zastępstwie Ministra Obrony Narodowej Sekretarz Stanu w MON Czesław Mroczek oraz Radca Ministra Obrony Narodowej – Pełnomocnik Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni gen. bryg. rez. K. Bondaryk.

[38] Według publikowanego na stronie www.sejm.gov.pl zapisu przebiegu posiedzenia sejmowej Komisji Obrony Narodowej nr 80 w dniu 7 maja 2014 r.

[39] Informacje udzielone przez Zastępcę dyrektora NCK (z upoważnienia Dyrektora NCK).

[40] Z upoważnienia Dyrektora NCK.

jednostkach organizacyjnych na stanowiska służbowe. Dotychczas [według stanu na dzień 9 października 2014 r.] *na wysłanych 26 wniosków o pozyskanie specjalistów z zakresu kryptologii i bezpieczeństwa cyberprzestrzeni pozytywnie rozpatrzono wyłącznie 2. Obecnie stosowana w Siłach Zbrojnych procedura wyznaczania żołnierzy zawodowych na stanowiska służbowe nie traktuje priorytetowo wyznaczania specjalistów z dziedziny kryptologii i obrony cybernetycznej do dedykowanych w tym celu jednostek. W dłuższej perspektywie czasu może to doprowadzić do poważnych braków kadrowych jak i spowolnić budowę kompetencji w zakresie kryptologii i obrony cybernetycznej."*

(dowód: akta kontroli Tom 1 str. 498, Tom 2 str. 396-409)

Przenoszenie osób realizujących zadania w zakresie cyberbezpieczeństwa odbywa się w oparciu o praktykę kadrową przyjętą w resorcie ON polegającą na tym, że organ wydający decyzje kadrowe powinien brać pod uwagę potrzeby każdej ze stron przenoszenia oraz zainteresowanego.

Minister Obrony Narodowej wyjaśnił, że *„w NCK oraz w specjalistycznych jednostkach organizacyjnych wykonujących działania operacyjne w cyberprzestrzeni, takich jak RCZBSiUT oraz CBC SZ, istnieje ścieżka awansowa, zarówno dla podoficerów jak i oficerów. Analiza potrzeb kadrowych została przeprowadzona w ramach opracowywania koncepcji Centrum Operacji Cybernetycznych (COC)."*

(dowód: akta kontroli Tom 1 str. 77, 91-92, 498, 512-530, Tom 2 str. 396-409)

Lokalizacja NCK

Zastępca dyrektora NCK na przywołanym posiedzeniu sejmowej Komisji Obrony Narodowej w dniu 7 maja 2014 r.[41] poinformował, że *„NCK nie dysponuje zapleczem dyslokacyjnym niezbędnym do pełnej realizacji specyficznych zadań statutowych. Narodowe Centrum Kryptologii wspierane przez wewnętrzne jednostki resortu obrony narodowej prowadzi prace koncepcyjno-projektowe oraz budowlane w docelowych lokalizacjach w celu ustanowienia siedziby i zaplecza technologiczno-produkcyjnego Centrum. Obecnie siedzibą NCK jest gmach Ministra ON w Warszawie, przy ul. Rakowieckiej."*

Ustalenia (uregulowania wewnętrzne) określające siedzibę NCK ulegały zmianie.[42]

Działania naprawcze

Do działań mających na celu polepszenie stanu w zakresie zasobów osobowych należą[43]:

- wdrożenie koncepcji Centrum Bezpieczeństwa Cybernetycznego (CBC) w celu integracji zasobów cyberbezpieczeństwa[44],
- podjęcie prac nad utworzeniem korpusu osobowego kryptologii i cyberbezpieczeństwa w celu umożliwienia sprawnego prognozowania, planowania i zarządzania z asobami osobowymi o raz wzmocnienia możliwości awansowania w zakresie szerokorozumianego cyberbezpieczeństwa i cyberobrony,

---

[41] Według publikowanego na stronie www.sejm.gov.pl zapisu przebiegu posiedzenia.

[42] Niepublikowane: decyzja Nr 197/MON z dnia 5 lipca 2013 r. w sprawie siedziby Narodowego Centrum Kryptologii, decyzja Nr 345/MON z dnia 20 listopada 2013 r. zmieniająca decyzję w sprawie siedziby Narodowego Centrum Kryptologii, decyzja nr 174/MON z dnia 5 maja 2014 r. zmieniająca decyzję w sprawie siedziby Narodowego Centrum Kryptologii.

[43] Ustalenia na podstawie analizy dokumentacji oraz wyjaśnień Ministra Obrony Narodowej i Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni.

[44] W sierpniu 2014 r. Minister Obrony Narodowej zaakceptował skorygowany, po konsultacjach wewnątrzresortowych, dokument (notatkę decyzyjną) – przedstawiony przez Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni – w sprawie koncepcji CBC.

- utworzenie na Wydziale Cybernetyki Wojskowej Akademii Technicznej nowego kierunku studiów Kryptologia i Cyberbezpieczeństwo, którego zadaniem jest kształcenie specjalistów w powyższych dziedzinach na potrzeby resortu ON,
- podjęcie prac wprowadzenia systemu zachęt mających na celu pozyskanie i utrzymanie pracowników o niezbędnych kwalifikacjach w obszarze ochrony cyberprzestrzeni (konsultacje resortowe),
- prowadzenie szkoleń oraz podjęcie prac koncepcyjno-organizacyjnych w celu stworzenia kompleksowego systemu szkoleń w zakresie cyberbezpieczeństwa.

(dowód: akta kontroli Tom 1 str. 77, 84, 91-92, 97-118, 458, Tom 2 str. 396-409)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

1.4. Cele, produkty i mierniki

Opis stanu faktycznego

W resorcie ON stosowane są następujące wskaźniki[45] (mierniki realizacji zadań):

- miernik oddziaływania – procentowy udział cyberprzestrzeni resoru ON będącej pod nadzorem SRnIK,
- miernik skuteczności – liczba wykrytych incydentów,
- miernik rezultatu – liczba obsłużonych incydentów.

Wskaźniki opracowano w powiązaniu z szacowaniem ryzyka. Osiągnięte wyniki realizacji wybranych wskaźników zostały przedstawione w raportach Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni[46]:

- Rocznym raporcie o stanie bezpieczeństwa cyberprzestrzeni RON w 2013 r.,
- Półrocznym raporcie o stanie bezpieczeństwa cyberprzestrzeni RON w 2014 r.

Jak wynika z wyjaśnień Ministra Obrony Narodowej i jego Pełnomocnika, *„informacje w zakresie osiągniętych wartości wskaźników są niejawne, ponieważ dotyczą wszystkich systemów (w tym niejawnych). Osiągnięte wyniki realizacji wybranych wskaźników zostały przedstawione w raportach będących dokumentami niejawnymi (obejmującymi wszystkie systemy będące w odpowiedzialności Ministra ON, w tym systemy niejawne narodowe i sojusznicze). Raporty sporządzone zostały dla wewnętrznych potrzeb resortu ON i nie były przekazywane do MAiC z uwagi na nieprzedstawienie przez MAiC warunków i zasad przekazywania informacji niejawnych."*

(dowód: akta kontroli Tom 1 str. 13-16, 446, 461)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

1.5. Projekty szczegółowe

Opis stanu faktycznego

Resort ON uczestniczył w pracach Zespołu zadaniowego do spraw ochrony portali rządowych[47] (reprezentowany był przez Dyrektora DIiT MON i Komendanta RCZBSiUT)

---

[45] W rządowej „Polityce..." nie określono m.in. szczegółowych celów, produktów (efektów) i mierników. Opracowanie przez MAiC globalnych, zagregowanych wskaźników celów i wskaźników realizacji *„Polityki..."* przewidywane jest w ramach jej aktualizacji.

[46] Dokumenty niejawne.

[47] Zespół powołany przez Przewodniczącego Komitetu Rady Ministrów do Spraw Cyfryzacji na mocy decyzji Nr 1/2012 z dnia 24 stycznia 2012 r. (zastąpiony przez Zespół zadaniowy do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej powołany decyzją Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji Nr 1/2014 z dnia 13 czerwca 2014 r.).

oraz w wytwarzaniu roboczych opracowań tego Zespołu, a także w uzgodnieniu *„Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej"*.

Jako dokument szczegółowy w odniesieniu do *„Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej"* (uszczegóławiający na gruncie resortowym niektóre elementy opisu systemu ochrony cyberprzestrzeni) została opracowana *„Polityka resortu obrony narodowej w zakresie bezpieczeństwa cyberprzestrzeni"* – dokument zaakceptowany przez Ministra Obrony Narodowej 13 czerwca 2014 r.

W uzasadnieniu do tego dokumentu zapisano, że narastające zjawisko trwałego uzależnienia zdolności państw do efektywnego funkcjonowania od sprawności i niezakłóconego działania systemów teleinformatycznych spowodowało powstanie nowych wyzwań i zagrożeń również o charakterze strategicznym. Zagrożenia te dotyczą również obszaru obronności państwa. Z tego względu kluczowe dla bezpieczeństwa Polski staje się zapewnienie poprawnego funkcjonowania oraz bezpiecznego korzystania z cyberprzestrzeni resortu ON. Bezpieczna cyberprzestrzeń RON jest warunkiem koniecznym dla posiadania przez Siły Zbrojne RP zdolności do obrony cyberprzestrzeni RP.

W ww. *„Polityce resortu ON..."* określono jej cele (zapewnienie bezpieczeństwa cyberprzestrzeni resortu ON dla sprawnego funkcjonowania resortu oraz stworzenie podstaw dla utrzymania przez Siły Zbrojne RP zdolności do obrony cyberprzestrzeni RP oraz ustanowienie prymatu bezpieczeństwa w procesie informatyzacji resortu ON), odniesienia prawne, przeznaczenie i zakres oddziaływania dokumentu (dotyczy wszystkich elementów cyberprzestrzeni resortu ON, znajdujących się na i poza terytorium RP), organizację zarządzania bezpieczeństwem cyberprzestrzeni resortu ON, zasady bezpieczeństwa informacji w cyberprzestrzeni (np. zasada ochrony wielowarstwowej / wielopoziomowej), odpowie dzialność za przestrzeganie *„Polityki..."* oraz czas obowiązywania (*„Polityka..."* podlega przeglądowi i aktualizacji w okresie rocznym).

Za właściwą realizację resortowej Polityki, w zakresie posiadanych uprawnień oraz w swoich obszarach kompetencyjnych, odpowiadają[48]: Pełnomocnik Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni, osoby odpowiedzialne za realizację SRnlK, Organizatorzy Systemów Funkcjonalnych SZ RP, kierownicy jednostek i komórek organizacyjnych, organizatorzy systemów teleinformatycznych oraz wszyscy użytkownicy cyberprzestrzeni RP.

Pełnomocnik Ministra ON ds. Bezpieczeństwa Cyberprzestrzeni wyjaśnił, że *„prowadzone w resorcie ON prace, ukierunkowanie na rozbudowę bezpieczeństwa cyberprzestrzeni, są wynikiem oraz są zbieżne z ustaleniami w tym zakresie, przyjętymi na szczeblach rządowym i ustawodawczym, a w szczególności:*

1) *„Rządowym programem ochrony cyberprzestrzeni RP na lata 2009-2011" przyjętym w marcu 2009 r. przez Komitet Stały Rady Ministrów. Dokument dotyczył domeny administracji rządowej (.gov) oraz części domeny .pl, która świadczy usługi dla sfery rządowej.*
2) *Ustawą 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 z 30 sierpnia 2011 r.[49] Wprowadzono w niej możliwość ogłoszenia stanu wojennego w razie zewnętrznego zagrożenia państwa, spowodowanego m.in. działaniami w cyberprzestrzeni.*

---

[48] Pkt 6.6. ww. *„Polityki resortu..."*.

[49] Dz.U. Nr 222 poz. 1323.

3) *„Polityką ochrony cyberprzestrzeni Rzeczypospolitej Polskiej" (załącznik do uchwały Rady Ministrów) przyjętą przez Radę Ministrów w dniu 25 czerwca 2013 r. Zakres oddziaływania Polityki, w odróżnieniu od „Rządowego programu...", został znacząco ograniczony. W szczególności, nie obejmuje ona swoim zasięgiem całej domeny .gov oraz nie dotyczy domeny .pl."*

(dowód: akta kontroli Tom 1 str. 14, 17-18, 22-23, 29-35, 200-210, 366-399)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

1.6. Kanały wymiany informacji. Udział resortu ON w tworzeniu krajowego systemu reagowania na incydenty komputerowe

Opis stanu faktycznego

Zgodnie z pkt. 1.5. rządowej *„Polityki..."*, w zakresie realizacji zadań związanych z bezpieczeństwem cyberprzestrzeni RP (Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. pełni rolę głównego zespołu CERT[50] w obszarze administracji rządowej i obszarze cywilnym. Analogicznie, w obszarze militarnym, rolę taką pełni Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych [jako CERT-MIL.PL]. Ważne jest zwiększenie udziału użytkowników cyberprzestrzeni RP w realizacji rządowej *„Polityki..."* przez konsultowanie jej zawartości oraz udział w koordynacji realizacji Polityki i jej przeglądów z przedstawicielami społeczeństwa i społeczności teleinformatycznej.

Klasyfikacja i porównywalność incydentów

W resorcie ON opracowano katalog (klasyfikację) incydentów oraz przyporządkowany do nich zbiór procedur działania.

Współpraca z innymi podmiotami polegała głownie na wymianie informacji w tym zakresie z innymi zespołami CERT, CSIRT[51] (odbywała się w ramach ABUSE-Forum lub na zasadach przyjętych w środowisku zespołów typu CERT) i nie doprowadziła do wypracowania ujednolicenia klasyfikacji incydentów oraz procedur reagowania.

Pełnomocnik Ministra Obrony Narodowej wyjaśnił, że obecnie klasyfikacja incydentów jest uaktualniana samodzielnie przez MIL-CERT.PL w celu zbliżenia jej do klasyfikacji używanej przez CERT.GOV.PL, przy zachowaniu specyfiki resortu ON - nowa klasyfikacja będzie wdrożona od początku 2015 r. Komendant RCZBSiUT stwierdził, że nie ma zapewnionej porównywalności ewidencji danych – każdy CERT indywidulanie ewidencjonuje incydenty, ze względu na właściwy sobie obszar działania.

(dowód: akta kontroli Tom 1 str. 52-75)

Współpraca i wymiana informacji

W dniu 12 listopada 2012 r. podpisano porozumienie między Ministrem Obrony Narodowej a Szefem Agencji Bezpieczeństwa Wewnętrznego w sprawie współpracy w zakresie reagowania na incydenty komputerowe oraz bezpieczeństwa teleinformatycznego. Efektem tego jest bezpośrednia współpraca między MIL-CERT.PL a CERT.GOV.PL na poziomie technicznym.

MIL-CERT.PL wykorzystuje:

- do wymiany informacji niejawnych - bezpieczny, niejawny kanał łączności CATEL,
- do kontaktów z innymi zespołami CERT - pocztę elektroniczną w sieci Internet.

[50] CERT (ang. Computer Emergency Response Team).

[51] CSIRT (ang. Computer Security Incident Response Team) - zespół powołany do reakcji na zdarzenia naruszające bezpieczeństwo w sieci Internet.

Istnieje także możliwość wykorzystania publicznego oprogramowania chroniącego informacje z wykorzystaniem publicznej kryptografii (klucz MIL-CERT.PL jest na stronie www.srnik.wp.mil.pl).[52]

Pełnomocnik Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni wyjaśnił, że *„RCZBSiUT realizuje zadania w zakresie reagowania na incydenty komputerowe w systemach teleinformatycznych resortu ON (nie zostały przydzielone mu inne zadania w ramach krajowego systemu reagowania na incydenty komputerowe ponad zapisy wynikające z rządowej „Polityki..."). Oczekiwane jest przyjęcie załącznika nr 1 do zarządzenia Nr 74 Prezesa RM z dnia 12 października 2011 r. w sprawie wykazu przedsięwzięć i procedur reagowania kryzysowego. Wymiana informacji z innymi zespołami CERT, CSIRT, ABUSE odbywa się w ramach ABUSE-Forum lub na zasadach przyjętych w środowisku zespołów typu CERT. W ramach SRnIK MIL-CERT.PL utrzymuje kontakty z organami bezpieczeństwa MSZ, Policji, ABW przekazując informacje w zakresie zagrożeń dla obszaru zainteresowania właściwych zespołów".*

(dowód: akta kontroli Tom 1 str. 52-75)

Współpraca w ramach Zespołu Zadaniowego KRMC

Przedstawiciele resortu ON uczestniczą w posiedzeniach zespołów powoływanych przez Komitet Rady Ministrów ds. Cyfryzacji (KRMC) (np. Zespołu zadaniowego do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej, którego Minister Obrony Narodowej jest członkiem, a Dyrektor NCK jest zapraszany jako głos doradczy).

NCK w odpowiedzi na ustalenia I Posiedzenia Zespołu Zadaniowego KRMC ds. ochrony cyberprzestrzeni RP z dnia 28 lipca 2014 r. przekazało Ministrowi Administracji i Cyfryzacji wkład resortu ON do *„Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP"* (obejmujący diagnozę stanu faktycznego oraz proponowane działania). W ww. dokumencie (wkładzie) w diagnozie stanu obecnego wskazano na brak wizji cyberbezpieczeństwa, brak kultury korporacyjnej, brak koncepcji rozwiązania systemowego, brak kultury technicznej, brak jednolitej taksonomii i terminologii, brak kompleksowych uregulowań prawnych, brak analizy rzeczywistych potrzeb oraz brak przeciwdziałania inwigilacji komercyjnej.

Ponadto - w ww. dokumencie - wskazano, że osiągniecie bezpieczeństwa wymagać będzie zmian w funkcjonowaniu struktur rządowych i administracyjnych oraz zorganizowania jednolitego i zhierarchizowania systemu zapewnienia bezpieczeństwa domeny gov.pl., a także wprowadzenie zmian w postępowaniu i mentalności kierownictw oraz personelu ministerstw i urzędów, w zakresie przetwarzania informacji. Dopiero uzyskanie zdolności do zapewnienia cyberbezpieczeństwa stworzy podstawy do budowy zdolności do cyberobrony. Polska – jak stwierdzono w ww. dokumencie - posiada potencjał do realizacji tych zadań w oparciu o możliwości resortu ON. Ponadto zaproponowano, aby Minister Administracji i Cyfryzacji oparł się o dostępne rządowi zasoby kompetencyjne i powołał w ramach ww. Zespołu Zadaniowego stałą grupę ekspercką, składająca się z przedstawicieli instytucji rządowych posiadających kompetencje i realne zdolności w zakresie cyberbezpieczeństwa i cyberobrony, tj. NASK/CERT.PL, ABW/CERT.GOV.PL oraz MON(NCK)/MIL-CERT.PL.

(dowód: akta kontroli Tom 1 str. 366-399, 443-450, 461, 499-511, Tom 2 str. 243-246)

Współdziałanie w zakresie wymiany informacji w ramach Systemu Reagowania Kryzysowego NATO

W celu zapewnienia warunków do pełnienia przez Rządowe Centrum Bezpieczeństwa roli Krajowego Punktu Kontaktowego (głównego) w zakresie wymiany informacji

[52] W myśl zaleceń pkt. 4.3. rządowej *„Polityki..."*.

w ramach Systemu Reagowania Kryzysowego NATO[53] oraz wykonywania zadania zapewnienia obiegu informacji między krajowymi i zagranicznymi organami i strukturami zarządzania kryzysowego - 10 maja 2013 r. zostało zawarte porozumienie pomiędzy RCZBSiUT a RCB w sprawie warunków udostępnienia terminala systemu PL-NS NOAN[54].

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

1.7. Narodowa strategia ochrony CRP. Prace nad dokumentami o charakterze długoterminowym i doktrynalnym

Opis stanu faktycznego

W resorcie ON podjęto prace przyczyniające się do stworzenia dokumentu o charakterze doktrynalnym w zakresie ochrony cyberprzestrzeni RP i bezpieczeństwa narodowego.

Zespół ds. Opracowania Projektu Założeń do Planu Obrony Cyberprzestrzeni RP

Z dniem 5 lipca 2013 r. w resorcie ON, na podstawie ww. decyzji ww. Nr 196/MON, powołano – podległy bezpośrednio Ministrowi Obrony Narodowej - nieetatowy Zespół do Spraw Opracowania Projektu Założeń do Planu Obrony Cyberprzestrzeni Rzeczypospolitej Polskiej. Na przewodniczącego Zespołu wyznaczono Radcę Ministra – gen. bryg. rez. Krzysztofa Bondaryka, a na wiceprzewodniczącego Zespołu - Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni[55].

Z dniem 1 października 2013 r. przewodniczącym i wiceprzewodniczącym Zespołu została ta sama osoba, t j. g en. bryg. rez. Krzysztof Bondaryk. Sytuacja ta zaistniała w związku z powierzeniem mu, na mocy decyzji Ministra Obrony Narodowej, funkcji Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni.[56]

W ramach prac Zespołu Sztab Generalny WP wykonał opracowanie w zakresie obszarów (zadań): *„Wskazanie i opisanie zidentyfikowanych czynników, w tym punktów krytycznych ograniczających proces pozyskania zdolności Sił Zbrojnych w zakresie cyberobrony w aspekcie legislacyjno-prawnym, organizacyjno-strukturalnym i finansowym"* oraz *„Identyfikacja możliwości wykorzystania potencjału współpracy z Europejska Agencja Obrony i Organizacją Traktatu Północnoatlantyckiego"*.

Minister Obrony Narodowej wyjaśnił, *że „prace Zespołu przebiegały w dwóch etapach:*

1) *analityczno-sprawozdawczym – w którym dokonano wnikliwej analizy i oceny stanu obecnego w ośmiu obszarach tematycznych wskazanych w ww. decyzji Nr 196/MON;*
2) *koncepcyjno-realizacyjnym – w którym wykonano opracowanie „Projekt Założeń do Planu Obrony Cyberprzestrzeni Rzeczypospolitej Polskiej"*[57]."

Zespół zakończył prace 24 lutego 2014 r. Przewodniczący Zespołu 12 marca 2014 r. złożył *„Meldunek w sprawie zakończenia prac Zespołu"*[58], którego załącznikiem był ww. *„Projekt Założeń do Planu Obrony..."*.

---

[53] NATO Crisis Response System (NCRS).

[54] PL-NS NOAN (ang. Polish NATO Secret NATO Office Automation Network – System Automatyzacji Prac Biurowych) - Polska Sieć Automatyzacji Procesów Biurowych NATO o klauzuli NATO SECRET.

[55] Ponadto w skład Zespołu wchodzą – na mocy § 4 ww. decyzji powołującej Zespół - Sekretarz: Komendant RCZBSiUT, członkowie – przedstawiciele m.in.: dyrektora DIiT, Szefa Zarządu PSDiŁ - P6, dyrektora NCK, Zespołu ds. Nowego Systemu Kierowania i Dowodzenia Siłami Zbrojnymi RP.

[56] Zgodnie z § 3 ww. decyzji Nr 196/MON z dnia 5 lipca 2014 r. przewodniczącym Zespołu jest ww. Radca Ministra, a wiceprzewodniczącym ww. Pełnomocnik. Przed 1 października 2013 r. funkcję ww. Pełnomocnika (i w związku z tym także funkcję wiceprzewodniczącego ww. Zespołu) pełnił dyrektor Departamentu Informatyki i Telekomunikacji MON.

[57] Dokument niejawny.

„Projekt Założeń do Planu Obrony Cyberprzestrzeni Rzeczypospolitej Polskiej" – zaakceptowany przez Ministra ON w dniu 21 maja 2014 r.[59] został przekazany w ramach resortu ON do wiadomości i służbowego wykorzystania. Ww. *„Projekt Założeń..."* został wykorzystany w pracach nad projektem *„Doktryny bezpieczeństwa cyberprzestrzeni RP"*.

„Projekt Założeń..", po skonsultowaniu z Biurem Bezpieczeństwa Narodowego[60], został skierowany do wiadomości wyznaczonych jednostek w ramach Sił Zbrojnych RP.

(dowód: akta kontroli str. Tom 1 8-18, 46, Tom 2 str. 113-143)

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Sztab Generalny WP uczestniczył w pracach nad opracowaniem *„Doktryny Cyberbezpieczeństwa Rzeczypospolitej Polskiej"* prowadzonych przez BBN. Doktryna ma stanowić, według jej zapisów, wspólną podstawę podejmowania działań na rzecz cyberbezpieczeństwa RP i stać się punktem odniesienia dla nowych rozwiązań w tym zakresie, stanowiąc uszczegółowienie zapisów *„Strategii Bezpieczeństwa Narodowego"* w tym obszarze. Rekomendacje ujęte w *„Doktrynie..."* powinny być stosownie wykorzystywane przez wszystkie podmioty publiczne i prywatne w planowaniu i organizowaniu działań oraz przygotowaniu systemu cyberbezpieczeństwa.

(dowód: akta kontroli Tom 1 str. 8-18, 446, 462-463, 468-493, Tom 2 str. 113-143)

Prace nad doktryną działań Sił Zbrojnych RP w cyberprzestrzeni

W resorcie ON realizowano prace nad opracowaniem kompleksowej doktryny działań Sił Zbrojnych RP w cyberprzestrzeni, określającej całościowe defensywne i ofensywne zasady zaangażowania SZ RP. Ogólne zasady użycia Sił Zbrojnych RP w obszarze cyberprzestrzeni są określone w niejawnych dokumentach Sztabu Generalnego WP.

Prace nad projektem *„Doktryny Działań Cybernetycznych"* realizowało Centrum Bezpieczeństwa Cybernetycznego SZ (sformowane na podstawie ww. decyzji Nr Pf-29/Org/SSG/ZOiU-P1 Ministra Obrony Narodowej z dnia 26 kwietnia 2010 r.[61]), któremu powierzono zadanie przygotowania doktryny prowadzenia operacji w cyberprzestrzeni.

(dowód: akta kontroli str. Tom 1 8-18, Tom 2 str. 109-112)

Możliwość wykorzystania potencjału resortu ON w sytuacji kryzysowej

W zakresie wykorzystania potencjału resortu obrony narodowej w sytuacji zagrożeń i incydentów związanych z cywilną cyberprzestrzenią RP - Centrum Bezpieczeństwa Cybernetycznego SZ – zgodnie ze swoim zakresem kompetencyjnym w czasie jego podporządkowania pod Zarząd Planowania Systemów Dowodzenia i Łączności – P6 Sztabu Generalnego WP otrzymało zadania z *„Katalogu przedsięwzięć szczegółowych resortu obrony narodowej ujętych w środkach reagowania kryzysowego"*. Wykorzystanie potencjału resortu ON w sytuacjach kryzysowych określone jest w *„Krajowym Planie Zarządzania Kryzysowego"* opracowanym przez Rządowe Centrum Bezpieczeństwa.

---

[58] Dokument niejawny.

[59] Dokument niejawny.

[60] Meldunek w sprawie realizacji konsultacji z BBN, dotyczących ww. *„Projektu Założeń do Planu Obrony Cyberobrony Rzeczypospolitej Polskiej"*.

[61] Dokument niejawny. Zgodnie z ww. decyzją Nr Z-45/Org./P1 Ministra Obrony Narodowej z dnia 13 listopada 2013 r. CBC SZ zostało przekazane wraz z zadaniami w bezpośrednie podporządkowanie spod P6 SGWP do Dyrektora NCK.

W badanym okresie[62] nie wystąpiły sytuacje wykorzystania potencjału resortu ON do zapobiegania lub minimalizowania skutków incydentów w cywilnej cyberprzestrzeni RP.

(dowód: akta kontroli str. Tom 1 8-18, Tom 2 str. 109-112)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

Uwagi dotyczące badanej działalności opisanej w rozdziale 1

NIK zwraca uwagę, że w badanym okresie (zwłaszcza w latach 2013-2014) podejmowano w resorcie ON różnorakie działania w zakresie zmian sytemu instytucjonalnego w celu zapewnienia zwiększenia ochrony cyberprzestrzeni. Jednakże w toku badania zidentyfikowano obszary, w których istnieją czynniki mogące mieć wpływ na utrzymanie odpowiednio wysokiego poziomu kompetencji i jakość realizacji zadań w resorcie ON, na które należy zwrócić uwagę.

1. Problemy o charakterze systemowym:

   a) brak zatwierdzonego i normatywnie opisanego całościowego docelowego modelu organizacji systemu ochrony cyberprzestrzeni z określonym harmonogramem realizacji (dokonywanie zmian *ad hoc* w systemie instytucjonalnym i w strukturach organizacyjnych);

   b) brak oszacowania zasobów i kosztów dotyczących ochrony cyberprzestrzeni (oszacowanie i pozyskanie zasobów ludzkich i finansowych ma fundamentalne znaczenie dla realizacji zadań);

   c) brak umiejscowienia działalności w zakresie ochrony cyberprzestrzeni w strukturze budżetu zadaniowego i w procesie planowania wydatków resortu ON (brak możliwości zapewnienia z wyprzedzeniem finansowania zadań).

   Należy zauważyć, że podejmowano prace w tym zakresie, w tym w ramach Zespołu do Spraw Opracowania Projektu Założeń do Planu Obrony Cyberprzestrzeni Rzeczypospolitej Polskiej. Jednak w końcowym dokumencie Zespół:

   - nie zidentyfikował zasobów ludzkich i infrastrukturalnych niezbędnych do cyberobrony państwa w SZ RP oraz w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
   - nie zdefiniował składników uzbrojenia cybernetycznego oraz wskaźników zdolności Sił Zbrojnych do prowadzenia działań w cyberprzestrzeni;
   - nie przygotował harmonogramu prac modernizacyjnych w resorcie ON oraz modelu docelowego rozwiązania strukturalno-organizacyjnego w zakresie obrony cyberprzestrzeni RP.

2. Izba wskazuje obszary ryzyka mogące mieć wpływ na realizację zadań:

   a) wielość i specyfika zmian w ramach systemu instytucjonalnego (zmiany w ramach SRnIK, budowanie nowych struktur np. NCK, zmiana podporządkowania podmiotów i zmiana zadań) - może mieć negatywny wpływ na potencjał innych jednostek (np. ISI) oraz realizację podpisanych porozumień[63] i powodować utrudnienia lub problemy w realizacji zadań;

   b) brak określania z wyprzedzeniem potrzebnych środków finansowych – może mieć znaczący wpływ na ich zapewnienie;

[62] Do 21 sierpnia 2014 r.

[63] Podpisanych przez Dyrektora DIiT MON w imieniu Ministra Obrony Narodowej porozumienia z Departamentem Obrony USA, ABW oraz Microsoft.

c) oparcie systemu na nowej, formującej się jednostce o profilu działalności wyspecjalizowanej w jednym tylko elemencie z zakresu bezpieczeństwa teleinformatycznego (kryptologii), prowadzonej głównie w ramach działalności naukowo-edukacyjnej i badawczo-rozwojowej (NCK) – może mieć wpływ na koncepcję rozwoju systemu (np. rozwijanie jedynie wybranych specjalności);

d) oparcie systemu na jednej osobie kierującej, której odejście mogłoby zagrozić ciągłości funkcjonowania[64] jednostek i systemu na gruncie prawnym.

Gen. bryg. rez. Krzysztof Bondaryk jest Pełnomocnikiem Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni (funkcja społeczna), Pełnomocnikiem Ministra Obrony Narodowej ds. Utworzenia Narodowego Centrum Kryptologii (funkcja społeczna), Dyrektorem Narodowego Centrum Kryptologii (funkcja etatowa), Radcą Ministra Obrony Narodowej ds. Bezpieczeństwa Cybernetycznego (funkcja społeczna), przewodniczącym (jako radca Ministra) i wiceprzewodniczącym (jako Pełnomocnik Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni) resortowego nieetatowego Zespołu ds. Opracowania Projektu Założeń do Planu Obrony Cyberprzestrzeni RP.

e) nieskorelowanie zmian faktycznych ze zmianami uregulowań wewnętrznych.

Decyzją Nr 196/MON z dnia 5 lipca 2013 r. w sprawie powołania Zespołu...[65] na przewodniczącego Zespołu wyznaczono Radcę Ministra – gen. bryg. rez. Krzysztofa Bondaryka, a na wiceprzewodniczącego Zespołu - Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni. Od 1 października 2013 r. przewodniczącym i wiceprzewodniczącym Zespołu była ta sama osoba, tj. gen. bryg. rez. Krzysztof Bondaryk (sytuacja ta zaistniała w związku z powierzeniem, na mocy decyzji Ministra Obrony Narodowej, Radcy Ministra Obrony Narodowej - gen. bryg. rez. Krzysztofowi Bondarykowi – funkcji Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni).[66] Mimo zaistnienia ww. sytuacji, nie zmieniono ww. decyzji Nr 196/MON z 5 lipca 2014 r. – nadal pozostały: zapis w § 3 (dotyczący składu Zespołu) i § 4 („Pracami Zespołu kieruje jego Przewodniczący, a w przypadku nieobecności Przewodniczącego – Wiceprzewodniczący.").

Ponadto NIK zwraca uwagę na konieczność wzmocnienia współpracy resortu Obrony Narodowej i Ministerstwa Administracji i Cyfryzacji, w tym na potrzebę wypracowania sposobu przekazania informacji, szczególnie niejawnych, do MAiC (m.in. o wskaźnikach, wydatkach) w celu wypełniania przez MON, określonych w rozdziale 6 rządowej *„Polityki..."*, powinności informowania w tym zakresie.

(dowód: akta kontroli Tom 1 str. 6, 13-16, 24-28, 38, 43-51, 61-75, 101-102, 198-210, Tom 2 str. 109-349)

Wyjaśnienia Ministra Obrony Narodowej w sprawie uwag NIK

Minister Obrony Narodowej przedstawił swoje stanowisko w tym zakresie wyjaśniając, że:

1. *„W sierpniu 2013 r. po zatwierdzeniu Modelu 2013, w resorcie ON (RON) miał miejsce poważny incydent teleinformatyczny (zorganizowany i długotrwały atak na konta poczty elektronicznej), wymagający podjęcia radykalnych działań naprawczych. Ani ówczesny Pełnomocnik MON ds. Obrony Cyberprzestrzeni (Dyrektor DIiT MON), ani DIiT oraz jednostki mu podległe nie zidentyfikowały faktu*

[64] Obok ewentualnych korzyści wynikających z właściwości osobowych.

[65] W sprawie powołania Zespołu do Spraw Opracowania Założeń do Planu Obrony Cyberprzestrzeni Rzeczypospolitej Polskiej.

[66] Zgodnie z § 3 ww. decyzji Nr 196/MON z dnia 5 lipca 2014 r. przewodniczącym Zespołu jest ww. Radca Ministra, a wiceprzewodniczącym ww. Pełnomocnik. Przed 1 października 2013 r. funkcję Pełnomocnika (i w związku z tym także funkcję wiceprzewodniczącego ww. Zespołu) pełnił dyrektor DIiT MON.

wystąpienia incydentu. Informacja o trwającym ataku została przekazana przez źródła spoza resortu. (...) Stąd decyzja o (...) wdrożeniu nowego podejścia do kwestii bezpieczeństwa cyberprzestrzeni resortu. Istotą nowego podejścia jest:

1) *rozdzielenie odpowiedzialności w RON za informatyzację (eksploatację i rozwój systemów teleinformatycznych) i cyberbezpieczeństwo, poprzez rozdzielenie stanowisk Szefa ISI i Pełnomocnika ds. Bezpieczeństwa Cyberprzestrzeni;*

2) *scentralizowanie struktur organizacyjnych realizujących kluczowe zadania w zakresie obrony cybernetycznej (w tym cyberbezpieczeństwa) w RON:"*

   a) NCK jako centrum kompetencyjne w zakresie kryptologii;

   b) jednostki podległe NCK (RCZBSiUT jako kluczowy komponent SRnIK oraz CBC SZ do prowadzenia działań obronnych w cyberprzestrzeni).

„Powyższe decyzje są skorelowane z decyzją dotyczącą wprowadzenia Modelu 2013 i dostosowują go do realnych wymagań w zakresie cyberbezpieczeństwa i cyberobrony. (...) Ponadto w dniu 13 sierpnia 2014 r. Minister ON zaakceptował Notatkę Decyzyjną w sprawie utworzenia w resorcie obrony narodowej Centrum Operacji Cybernetycznych z 5.08.2014 r."[67]

2. *„Podporządkowanie RCZBSiUT pod NCK, oprócz pozytywnych, realnych skutków (...), nie spowodowało pogorszenia jakości współpracy z podmiotami zewnętrznymi, zarówno krajowymi, jak i zagranicznymi. Podporządkowanie RCZBSiUT pod NCK nie wpłynęło na obniżenie zdolności ISI w zapewnianiu bezpieczeństwa teleinformatycznego."*

   Według Ministra Obrony Narodowej *„obecne uwarunkowania prawne i statutowe ISI są wystarczające do prowadzenia efektywnych prac na rzecz uzyskania akceptowalnego poziomu bezpieczeństwa".* Inspektorat odpowiada za informatyzację całego resortu obrony narodowej, organizując i kierując procesami planowania, dostarczania, wsparcia eksploatacji oraz użytkowania systemów teleinformatycznych stosownie do wypracowanych kierunków rozwoju przez organizatorów systemów funkcjonalnych, świadczy usługi dla wszystkich użytkowników w RON i jest regularnie informowany przez Centrum Techniczne SRnIK o liczbie i charakterze incydentów komputerowych. Uczestniczy także w spotkaniach, uzgodnieniach i szkoleniach[68] oraz realizuje zadania w zakresie bieżącego reagowania na incydenty komputerowe. Zgodnie z decyzją nr 243/MON z 2014 r. administratorzy systemów teleinformatycznych z podległych szefowi ISI jednostek stanowią trzeci poziom SRnIK.

3. *„Zgodnie z ww. decyzją Nr 262/MON z 2013 r. obsługę merytoryczną Pełnomocnika MON ds. Bezpieczeństwa Cyberprzestrzeni zapewnia ISI (...). Większość prac (...) Pełnomocnik wykonuje osobiście. NCK zapewnia jedynie (...) obsługę biurową (...). Minister ON (...) nakazał formalne uregulowanie sytuacji faktycznej w decyzji zmieniającej decyzję w sprawie powołania Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni. Projekt tego dokumentu jest*

---

[67] Dokument zawiera korektę propozycji zawartych w Notatce Decyzyjnej z 22.04.2014 r. *w sprawie utworzenia w resorcie obrony narodowej Centrum Operacji Cybernetycznych* (dokument niejawny).

[68] M.in. w bieżącym roku zrealizowano cykl spotkań roboczych w ramach realizacji *„Wytycznych Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni w sprawie szczegółowych zasad i zadań w zakresie kontroli dostępu do systemu, poufności informacji oraz rozliczalności funkcjonowania systemu INTER-MON"*, mających na celu wspólne wypracowanie kierunków i koncepcji zmian.

obecnie procedowany. Zgodnie z jego zapisami za obsługę merytoryczną Pełnomocnika będzie odpowiedzialne NCK."

4. *„Priorytetem jest możliwie szybkie wprowadzenie rozwiązań organizacyjnych i technicznych, umożliwiających wykrywanie i likwidację incydentów komputerowych, tj. realne zwiększenie poziomu bezpieczeństwa cyberprzestrzeni. Jednocześnie opracowywane są rozwiązania legislacyjne, mające na celu doprecyzowanie stanu faktycznego. (...)."*
5. *Faktem jest, że od 01.10.2013 r. ta sama osoba pełniła funkcję Przewodniczącego i Wiceprzewodniczącego Zespołu. Nie miało to (...) wpływu na tok prac Zespołu.*

Ponadto Minister Obrony Narodowej wyjaśnił, że *„podczas prac przewodniczący Zespołu zwrócił się do wojskowych ośrodków akademickich o wykonanie opracowań dotyczących kwestii definicyjnych i terminologicznych z obszarów cyberbezpieczeństwa i cyberobrony. Prace Zespołu walnie przyczyniły się do późniejszego sformułowania przez Pełnomocnika ds. Bezpieczeństwa Cyberprzestrzeni koncepcji sformowania Centrum Operacji Cybernetycznych oraz zmodyfikowania SRnIK."* Zespół wskazał również na potrzebę *„podjęcia prac związanych z utworzeniem nowego korpusu osobowego w SZ RP „Kryptologia i cyberbezpieczeństwo"*.

(dowód: akta kontroli str. Tom 1 8-12, 443-463, Tom 2 str. 109-112)

Ocena cząstkowa

Kontrola wykazała, że w resorcie ON podejmowane były działania w zakresie budowania systemu instytucjonalnego ochrony cyberprzestrzeni i ram dla jego funkcjonowania ukierunkowane na rozbudowę bezpieczeństwa cyberprzestrzeni, które w wielu aspektach były zbieżne z założeniami rządowej *„Polityki..."*. W szczególności utworzono i rozwijano system reagowania na incydenty komputerowe, opracowano katalog (klasyfikację) incydentów i przyporządkowany do nich zbiór procedur działania, prowadzono wymianę informacji z innymi podmiotami państwowymi realizującymi zadania w zakresie ochrony cyberprzestrzeni RP, określono wskaźniki (mierniki realizacji zadań) w powiązaniu z szacowaniem ryzyka, przyjęto *„Politykę resortu obrony narodowej w zakresie bezpieczeństwa cyberprzestrzeni"* oraz *„Projekt Założeń do Planu Obrony Cyberprzestrzeni"*.

W działalności kontrolowanej jednostki stwierdzono natomiast problemy w postaci:

- dokonywanie zmian *ad hoc* w systemie instytucjonalnym i w strukturach organizacyjnych, tj. przy braku zatwierdzonego i normatywnie opisanego całościowego docelowego modelu organizacji systemu ochrony cyberprzestrzeni z określonym harmonogramem realizacji,
- braku oszacowania zasobów i kosztów dotyczących ochrony cyberprzestrzeni,
- braku umiejscowienia działalności w zakresie ochrony cyberprzestrzeni w strukturze budżetu zadaniowego i w procesie planowania wydatków resoru ON.

2. Szacowanie ryzyka związanego z zagrożeniami w CRP

2.1. Szacowanie ryzyka na podstawie rządowej „Polityki..."

Opis stanu faktycznego

W pkt. 2 rządowej *„Polityki..."* wskazano, że istnieje potrzeba wypracowania, na podstawie prowadzonej analizy ryzyka, minimalnych standardów bezpieczeństwa, zgodnie z którymi będą zabezpieczane zidentyfikowane zasoby i systemy, dzięki którym są realizowane konstytucyjne obowiązki Państwa.

W pkt. 3.1. rządowej *„Polityki..."* wskazano, że szacowanie ryzyka związanego z funkcjonowaniem cyberprzestrzeni jest kluczowym elementem procesu bezpieczeństwa cyberprzestrzeni, determinującym i uzasadniającym działania podejmowane w celu jego obniżenia do akceptowalnego poziomu. W celu osiągnięcia akceptowalnego poziomu bezpieczeństwa, założono, iż każda jednostka administracji rządowej, w terminie

do 31 stycznia każdego roku przekaże do ministra właściwego ds. informatyzacji sprawozdanie podsumowujące wyniki szacowania ryzyka (wg wzorca opracowanego przez ministra właściwego ds. informatyzacji).

Resort ON w dniu 14 lutego 2014 r. (tj. po ww. terminie 31 stycznia) otrzymał od Ministra Administracji i Cyfryzacji dokument pt. *„Koncepcja i założenia do metodyki oceny ryzyka przygotowania sprawozdania dotyczącego cyberbezpieczeństwa"*, w której zapisano, że ze względu na stosunkowo małe doświadczenie jednostek w zakresie zarządzania ryzykiem, jak również harmonogram prac związanych z *„Polityką..."*, zakłada się, że w roku 2014 sprawozdanie (za rok 2013) zostanie przygotowane w formule wstępnej. W roku 2014 jednostki będą mogły przygotować się do tego, aby sprawozdanie za rok 2014 (sporządzone w styczniu 2015 r.) mogło być przygotowane w wersji docelowej (z pogłębioną analizą skutków i prawdopodobieństwa).

Resort ON zrealizował zadanie dotyczące szacowania ryzyka związanego z zagrożeniami występującymi w cyberprzestrzeni zgodnie z metodyką otrzymaną z MAiC (resort ON nie uczestniczył w przygotowaniu metodyki). Przekazano do MAiC (7 maja 2014 r.) analizę ryzyka dotyczącą procedur bezpieczeństwa stosowanych w RON (w zakresie jawnego systemu INTER-MON za 2013 r.). Przeprowadzona analiza ryzyka skupiła się na dwóch najistotniejszych zasobach dla resortu ON w obszarze zaufania obywatela do administracji publicznej, tj. serwerach usług będących w bezpośredniej gestii resortu ON oraz resortowej poczcie elektronicznej (serwerach poczty). W toku przeprowadzonej analizy ewaluacji ryzyka dokonanej przez Pełnomocnika Ministra Obrony Narodowej ds. spraw Bezpieczeństwa Cyberprzestrzeni jego poziom w przypadku ww. zasobów określono jako „duże" lub „bardzo duże".

(dowód: akta kontroli Tom 1 str. 61-72, 272-277, 289, 464-467, Tom 2 str. 247-260)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

2.2. Określanie zagrożeń i szacowanie ryzyka ich wystąpienia w dokumentacji z zakresu zarządzania kryzysowego

Opis stanu faktycznego

W pkt. 2 rządowej *„Polityki..."* zalecono, aby działania dotyczące bezpieczeństwa infrastruktury teleinformatycznej były komplementarne w stosunku do działań mających na celu ochronę infrastruktury krytycznej Państwa.

Kwestia zagrożeń bezpieczeństwa cyberprzestrzeni została ujęta w *„Raporcie cząstkowym MON"* oraz w *„Raporcie o zagrożeniach bezpieczeństwa narodowego"*.

W 2011 r. w resorcie ON podjęto[69] się zadania weryfikacji ilości obiektów wojskowych zgłoszonych do *„Jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy"*. Skoncentrowano się na współpracy z RCB oraz pomiędzy komórkami i jednostkami organizacyjnymi resortu ON, które zgłosiły obiekty wojskowe do wspomnianego wykazu. W ramach uzgodnień, ograniczono liczbę obiektów wojskowych z dziesięciu do trzech. Dyrektor RCB w maju 2013 r. potwierdził ujęcie w wykazie trzech obiektów wojskowych, zgłoszonych przez MON. Opracowano informację dotyczącą charakterystyki obiektów wojskowych zgłoszonych do ww. *Jednolitego wykazu* na potrzeby Narodowego Programu Ochrony Infrastruktury Krytycznej (POIK). Informacja została przekazana do RCB dwukrotnie: w grudniu 2010 r. (w sprawie 10 obiektów) oraz we wrześniu 2011 r. (w sprawie 3 obiektów). W rozważanych wariantach brano pod uwagę także infrastrukturę teleinformatyczną[70].

---

[69] W badanym okresie system instytucjonalny w zakresie zarządzania kryzysowego w ramach resortu ON ulegał zmianom.

[70] Szczegółowe informacje stanowią informacje niejawne.

Dyrektor NCK poinformował, że w celu oceny kompletności i merytorycznej poprawności planów ochrony systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, będącej we właściwości Ministra Obrony Narodowej, stosowana jest analiza ryzyka, zgodna z metodyką przyjętą przez Ministerstwo Administracji i Cyfryzacji. 30 grudnia 2013 r. Pełnomocnik Ministra Obrony Narodowej ds. spraw Bezpieczeństwa Cyberprzestrzeni wydał *„Wytyczne w sprawie szczegółowych zasad i zadań w zakresie kontroli dostępu do systemu, poufności informacji oraz rozliczalności funkcjonowania systemu INTER-MON"*, których celem jest określenie minimalnych standardów bezpieczeństwa, jakim powinien odpowiadać nowoczesny, bezpieczny system teleinformatyczny.

Resort ON brał udział przygotowaniu Krajowego Planu Zarządzania Kryzysowego. Do zakończenia kontroli prowadzona była analiza zasadności wprowadzenia kolejnych zmian do KPZK zaproponowanych przez RCB (w lipcu 2014 r.).

W 2010 r. Zarząd Planowania Operacyjnego - P3 Sztabu Generalnego WP opracował *„Plan Zarządzania Kryzysowego MON"*, który został wprowadzony do użytku w resorcie ON[71]. Od 1 stycznia 2011 r. zadania związane z przygotowaniem Planu i jego aktualizacji przejęło Centrum Zarządzania Kryzysowego. W lipcu 2012 r. RCB poinformowało o konieczności zachowania spójności planów sporządzanych przez ministrów i kierowników urzędów centralnych z *„Krajowym Planem Zarządzania Kryzysowego"* - dołączono *„Wskazówki do przygotowania (aktualizacji) planów zarządzania kryzysowego"*. W CZK MON dokonano aktualizacji *„Planu Zarządzania Kryzysowego MON"* biorąc je pod uwagę (w grudniu 2012 r. dokument przekazano do RCB). W ramach ww. aktualizacji w *„Planie..."* ujęto charakterystykę zagrożeń i ryzyko ich wystąpienia, a także siatkę bezpieczeństwa zawierającą zestawienie potencjalnych zagrożeń ze wskazaniem podmiotu wiodącego przy ich usuwaniu oraz podmiotów współpracujących. Wśród zagrożeń ujęto m.in. atak terrorystyczny w cyberprzestrzeni oraz atak na systemy łączności i teleinformatyczne. W styczniu 2013 r., na podstawie wniosków z funkcjonowania systemu zarządzania kryzysowego i ustaleń międzyresortowych z listopada 2012 r., Minister Obrony Narodowej wydał decyzję[72], która przewidywała m.in., że nowy plan zarządzania kryzysowego zostanie przygotowany do 30 września 2013 r., a prace w tym zakresie będą koordynowane przez Szefa Sztabu Generalnego WP. W SGWP zostały wydane m.in. wytyczne Zastępcy Szefa SGWP (w maju 2013 r.) w sprawie opracowania załączników funkcjonalnych oraz planów dziedzinowych do *„Planu Zarządzania Kryzysowego resortu obrony narodowej"*, w których określono, że w ramach planu dziedzinowego *„Udział Sił Zbrojnych RP w przeciwdziałaniu zagrożeniom terrorystycznym"* zostanie opracowany aneks *„Udział Sił Zbrojnych w przeciwdziałaniu atakom terrorystycznym w cyberprzestrzeni"* (za jego przygotowanie odpowiadał Departament Informatyki i Telekomunikacji MON). Ponadto, ujęto w nich projekt katalogu zdolności Sił Zbrojnych RP, który docelowo miał stanowić integralną część *„Planu Zarządzania Kryzysowego resortu obrony narodowej"*. W katalogu zawarto m.in. pozycję „bezpieczeństwo teleinformatyczne" obejmującą monitorowanie zagrożeń w systemach teleinformatycznych, zabezpieczenie systemów teleinformatycznych przed atakami, analizę oprogramowania złośliwego oraz przeciwdziałanie jego skutkom, analizę skutków naruszenia systemów teleinformatycznych oraz przywracanie funkcjonalności systemów teleinformatycznych po atakach w cyberprzestrzeni.

---

[71] Decyzja Nr 466/MON Ministra Obrony Narodowej z dnia 14 grudnia 2010 r. w sprawie wprowadzenia do użytku w resorcie obrony narodowej *„Planu Zarządzania Kryzysowego Ministerstwa Obrony Narodowej"* (dokument niepublikowany).

[72] Decyzja Nr 370/MON Ministra Obrony Narodowej z dnia 19 listopada 2012 r. w sprawie opracowania *„Planu Zarządzania Kryzysowego resortu obrony narodowej"* (dokument niepublikowany).

Przyjęto, że na podstawie ww. katalogu zostaną opracowane szczegółowe karty zdolności (zawierające m.in. wykaz posiadanych zasobów Sił Zbrojnych RP), które zostaną zawarte w *„Planie Zarządzania Kryzysowego resortu obrony narodowej"*.

W związku z planowanym od 1 stycznia 2014 r. wejściem zmian w Systemie Kierowania i Dowodzenia SZ RP, w tym zwłaszcza rozformowaniem Centrum Zarządzania Kryzysowego MON[73], zaistniała konieczność zmiany wcześniej przyjętych terminów opracowania *„Planu..."*. 24 grudnia 2013 r. Minister Obrony Narodowej wydał decyzję Nr 438/MON zmieniającą decyzję w sprawie opracowania *„Planu Zarządzania Kryzysowego resortu obrony narodowej"*. Określono w niej m.in., że od 1 stycznia 2014 r. zadania związane z opracowaniem przedmiotowego *„Planu..."* koordynuje Dowódca Operacyjny RSZ.

(dowód: akta kontroli Tom 1 str. 120-197, Tom 2 str. 104-395)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

Ocena cząstkowa

Kontrola wykazała, że resort ON zrealizował zadanie dotyczące szacowania ryzyka związanego z zagrożeniami występującymi w cyberprzestrzeni zgodnie z metodyką otrzymaną z MAiC. W resorcie ON podejmowane były działania w ramach planowania zarządzania kryzysowego w zakresie określenia zagrożeń i szacowania ryzyka ich wystąpienia.

3. Działania resortu ON w ramach ochrony cyberprzestrzeni RP

3.1. Ustanowienie i kontrola wymogów w zakresie bezpieczeństwa cyberprzestrzeni RP

Opis stanu faktycznego

W pkt. 2 rządowej *„Polityki..."* wskazano konieczność prowadzenia działań mających na celu zapewnienie bezpieczeństwa infrastruktury teleinformatycznej Państwa, tj. zapewnienie poprawności i ciągłości funkcjonowania systemów teleinformatycznych, obiektów i instalacji wykorzystywanych do realizacji konstytucyjnych zadań Państwa.

Zgodnie z decyzją Nr 261/MON[74] zasadniczym środowiskiem pracy komórek i jednostek organizacyjnych resortu ON są resortowe wewnętrzne - odseparowane od sieci Internet – systemy teleinformatyczne organizowane na potrzeby jednostek i komórek organizacyjnych. W szczególności systemy teleinformatyczne "MIL-WAN" oraz "CATEL", a poza nimi organizuje się w resorcie ON system "INTER-MON" zapewniający dostęp do sieci Internet. Decyzja określa również, że Pełnomocnik Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni kreuje politykę bezpieczeństwa teleinformatycznego związaną z funkcjonowaniem systemu "INTER-MON" i określa zasady zapewniające utrzymanie oraz rozwój bezpieczeństwa teleinformatycznego systemu. Szef ISI jest organizatorem systemu "INTERMON" i na podstawie wytycznych Pełnomocnika określa w drodze wytycznych niezbędne elementy zapewniające rozwój oraz utrzymanie systemu.

W grudniu 2013 r. Pełnomocnik ds. Bezpieczeństwa Cyberprzestrzeni wydał *„Wytyczne Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni w sprawie szczegółowych zasad i zadań w zakresie kontroli dostępu do systemu, poufności informacji oraz rozliczalności funkcjonowania systemu INTER-MON"* (dokument niejawny), które określają sposób tworzenia i zarządzania bezpieczeństwem systemów teleinformatycznych

[73] W związku z przeformowaniem z dniem 1 stycznia 2014 r. Centrum Zarządzania Kryzysowego MON w Centrum Operacyjne MON, zadania zarządzania kryzysowego zostały przekazane do Dowództwa Operacyjnego RSZ. DORSZ przekazano w styczniu 2014 r. m.in. opracowany przez CZK MON projekt *„Planu Zarządzania Kryzysowego resortu obrony narodowej"*.

[74] Decyzji Nr 261/MON z dnia 19 września 2013 r. (weszła w życie z dniem 1 października 2013 r.).

wchodzących w skład jawnej resortowej sieci komputerowej INTER-MON. W lipcu 2014 r. Szef ISI przedstawił Pełnomocnikowi informację o stanie realizacji na dzień 30 czerwca 2014 r. *„Harmonogramu realizacji Wytycznych..."*.

Ponadto do podstawowych[75] regulacji opracowanych w resorcie ON w ww. zakresie należą m.in.: zalecenia do projektowania i budowy sieci strukturalnych, wytyczne w zakresie użytkowania systemu INTER-MON, procedura tworzenia strony WWW, wykaz obowiązujących standardów sprzętu informatyki i oprogramowania, regulamin realizacji usług telekomunikacyjnych, zalecenia do konfiguracji urządzeń sieciowych w STI MIL-WAN, zasady świadczenia usługi dostępu do sieci Internet, wytyczne w sprawie prezentacji graficznej serwisów WWW, zalecenia w zakresie wymagań bezpieczeństwa teleinformatycznego na budowę i eksploatację lokalnych sieci bezprzewodowych WLAN z dostępem do Internetu, katalog usług ISI w INTER-MON, zasady pozyskiwanie i zarządzania oprogramowaniem informatycznym, normy należności naliczeniowego sprzętu informatyki, tymczasowa instrukcja organizacji projektowania, wdrażania i eksploatacji systemów informatycznych oraz instrukcja prowadzenia gospodarki materiałowo-technicznej sprzętem informatyki i oprogramowaniem.

Ponadto, w systemie teleinformatycznym MIL-WAN prowadzony jest Serwis Bezpieczeństwa Teleinformatycznego SRnIK. W serwisie tym prezentowane są treści z zakresu bezpieczeństwa teleinformatycznego zawierające aktualności, porady, materiały szkoleniowe, raporty o stanie bezpieczeństwa, a także biuletyn informacyjny.

Weryfikacja obowiązujących i zalecanych regulacji opiera się na zasadach obiegu korespondencji służbowej oraz centralizacji realizacji zapotrzebowywanych usług.

W związku z zaistnieniem w sierpniu 2013 r. w resorcie ON poważnego incydentu teleinformatycznego, Minister Obrony Narodowej 18 września 2013 r. zaakceptował *„Program naprawczy w zakresie bezpieczeństwa teleinformatycznego w resorcie obrony narodowej"*[76]. 17 lutego 2014 r. Pełnomocnik Ministra Obrony Narodowej złożył *Meldunek w sprawie realizacji „Programu naprawczego..."* (stan na dzień 14 lutego 2014 r.) i 24 lutego 2014 r. wydał *Aneks do „Programu naprawczego..."*. Kolejny *Meldunek...* złożono w lipcu 2014 r. według stanu na 1 lipca 2014 r.[77] We wdrażaniu *„Programu naprawczego..."* uczestniczą także m.in. ISI i Dowództwo Generalne Rodzajów SZ.

(dowód: akta kontroli Tom 1 str. 203, 211-225, Tom 2 str. 272-324)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

3.2. Ćwiczenia i testy

Opis stanu faktycznego

W latach 2012-2014 przedstawiciele resortu ON uczestniczyli w ćwiczeniach systemu bezpieczeństwa cyberprzestrzeni organizowanych przez:

- NATO (w tym CCDCOE[78] w Tallinie) i USEUCOM: CMX, CWIX (2012, 2013, 2014), Combined Endeavor i Cyber Endeavor (2012, 2013), LOCKED SHILEDS (2013, 2014), STEADFAST COBALT 13, FLEXIBLE LEADER 2013.

  Ćwiczenia odbywały się w formie warsztatów (CWIX, Cyber Endeavor i Combined Endeavor, LOCKED SHIELDS), ćwiczeń praktycznych (LOCKED SHIELDS) oraz ćwiczeń specjalnych łączności zgrywających lub doskonaląco-zgrywających (Combined Endeavor, STEADFAST COBALT), ćwiczeń sztabowych (CMX) i dyskusji

[75] Oprócz powszechnie obowiązujących aktów normatywnych i normalizacyjnych (np. Polskie Normy).

[76] Dokument niejawny.

[77] Dokumenty niejawne.

[78] NATO Cooperative Cyber Defence Centre of Excellence – Centrum Doskonalenia Cyber Obrony.

(FLEXIBLE READER). Ze strony polskiej udział brali przedstawiciele resortu ON (w tym RCZBSiUT, CBC SZ) i innych podmiotów (NASK).

Ćwiczenia miały na celu: doskonalenie interoperacyjności między sojusznikami, doskonalenie obrony systemów teleinformatycznych przed atakami, doskonalenie współdziałania w zakresie zarządzania kryzysowego (w tym również w zakresie kryzysu w cyberprzestrzeni), sprawdzenie systemów łączności i informatyki przeznaczonych dla Sił Odpowiedzi NATO oraz poprawę międzynarodowej współpracy pomiędzy liderami cyberbezpieczeństwa).

- Zarząd Planowania Systemów Dowodzenia i Łączności – P6 Sztabu Generalnego WP: STOKROTKA (2012, 2013) i ASTER 13.

  Ćwiczenia odbywały się w formie: warsztatów (ASTER) i ćwiczeń specjalnych łączności doskonaląco-zgrywających (STOKROTKA). Ćwiczenia te były organizowane dla resortu ON – uczestniczyli w nich przedstawiciele wielu jednostek (w tym CBC SZ) – miały na celu testowanie interoperacyjności zautomatyzowanych systemów dowodzenia oraz sprawdzenie poziomu bezpieczeństwa teleinformatycznego, a także doskonalenie obrony systemów teleinformatycznych przed atakami.

- Podmioty prywatne i organizacje pozarządowe: CYBEREXE 2012 (warsztaty mające na celu doskonalenie współpracy między zespołami CERT w przypadku ataku cybernetycznego na infrastrukturę krytyczną kraju) z udziałem podmiotów: prywatnych (z sektorów: telekomunikacji, energetyki i paliw) i państwowych, w tym z resortu ON (RCZBSiUT) i innych (RCB, WAT).

Minister Obrony Narodowej poinformował, że każdorazowo po odbyciu ćwiczeń opracowywane były wnioski lub sprawozdania. Wnioski z uczestnictwa w ćwiczeniach były brane pod uwagę w działalności służbowej.

Przedstawiciele resortu ON nie wzięli udziału, mimo zaproszenia przez RCB[79], w kwietniu 2014 r. w – organizowanych przez ENISA[80] - ćwiczeniach Cyber Europe 2014.

Minister Obrony Narodowej wyjaśnił, że *RCZBSiUT oraz CBC SZ nie uczestniczyły w ww. ćwiczeniach Cyber Europe 2014, bowiem obszar współpracy z ENISA został przypisany CERT Polska, posiadającemu swoich przedstawicieli w jej strukturach.*

(dowód: akta kontroli Tom 1 str. 76, 80-83, 428-436, Tom 2 str. 1-31)

W badanym okresie w resorcie ON przeprowadzone były przez MIL-CERT i CBC SZ testy systemów teleinformatycznych, w tym: systemu DUNAJ (badanie wybranej podatności wybranego obiektu), systemu INTER-MON (testy penetracyjne), systemu KTSA (badanie podatności aplikacji), systemu SI EMITER (testy bezpieczeństwa), systemu ASOC (testy bezpieczeństwa) oraz dokonano analizy kodu złośliwego (MIL-CERT - we współpracy z SKW oraz CERT.GOV.PL). W 2008 r. przeprowadzono we współpracy z ABW testy witryn MON.

Minister Obrony Narodowej wyjaśnił, że przed każdym wykonywanym testem bezpieczeństwa systemu lub sieci tworzony był plan testów wraz harmonogramem prac. Dokumenty te każdorazowo zatwierdzał organizator systemu lub przełożony komendanta jednostki testującej.

---

[79] RCB skierowało w lutym 2014 r. do Ministra ON zaproszenie do wzięcia udziału przez przedstawicieli resortu ON (zespołu zajmującego się bezpieczeństwem teleinformatycznym) w fazie pierwszej (technicznej) ćwiczeń Cyber Europe 2014, polegającej na analizie wybranego incydentu przez przebywających w swoim miejscu pracy uczestników. Zarządzanie ćwiczeniem miało odbywać się poprzez dedykowaną platformę internetową utworzoną przez agencję ENISA.

[80] Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (European Union Agency for Network and Information Security).

(dowód: akta kontroli Tom 1 str. 76, 83, Tom 2 str. 1-103)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

3.3. Ustanowienie systemu reagowania na incydenty w cyberprzestrzeni

Opis stanu faktycznego

Status Centrum Wsparcia Technicznego Systemu Reagowania na Incydenty Komputerowe (MIL-CERT.PL) został określony w *„Szczegółowym zakresie działania WBBŁiI"* (od 01.04.2011 r. - RCZBSiUT), decyzji 357/MON z 29 lipca 2008 r., decyzji 243/MON z 18 czerwca 2008 r. i w okresie objętym kontrolą nie ulegał zmianie. Przyjęcie i wdrażanie rządowej *„Polityki..."* nie wpłynęło na status formalny oraz zakres zadań wykonywanych przez MIL-CERT.PL.

Informacje o powołaniu Systemu Reagowania na Incydenty Komputerowe (SRnIK) zostały podane za pośrednictwem korespondencji do jednostek i instytucji resortu ON pismem Dyrektora Departamentu Informatyki i Telekomunikacji[81].

SRnIK posiada strony informacyjne: w MIL-WAN – sbt.ron.int oraz w INTER-MON – www.srnik.wp.mil.pl.

MIL-CERT.PL nie wykonuje usług wykraczających poza zakres formalnie określonego mandatu.

MIL-CERT.PL nie pełni roli krajowego punktu kontaktowego ds. wymiany informacji z innymi narodowymi zespołami CERT. Wyjątek stanowi podpisane porozumienie[82] pomiędzy Szefem ABW a NATO CDMB, które wskazuje odpowiedzialność MON za domeny wykorzystywane przez podmioty wojskowe.

Zadania przydzielone MIL-CERT.PL w ramach krajowego systemu zarządzania kryzysowego pokrywają się z zadaniami Centrum Technicznego SRnIK – zgodnie z decyzją 243/MON z dnia 18.06.2014 r.

MIL-CERT.PL nie uczestniczył w procesie identyfikacji krytycznej infrastruktury informatycznej państwa, szacowania ryzyka oraz opracowywania planów ciągłości działania. MIL-CERT.PL nie otrzymał żadnych zadań w przypadku wystąpienia sytuacji kryzysowej związanej z funkcjonowaniem infrastruktury teleinformatycznej państwa[83].

(dowód: akta kontroli Tom 1 str. 52-60, 443-463)

Zespół MIL-CERT.PL wykorzystuje różne źródła informacji o zagrożeniach, podatnościach i incydentach: system ARAKIS, platformę N6 (NASK), ABUSE Forum, biuletyny Microsoftu, NCIRC-u, CERT.GOV.PL, współpracuje z ŻW, SKW, CERT.GOV.PL i Policją oraz otrzymuje informacje z systemów bezpieczeństwa teleinformatycznego RON.

RCZBSiUT opracowało klasyfikację incydentów, na podstawie której można dokonywać ich identyfikacji oraz przyporządkowany do nich zbiór procedur działania:

- *„Standardowe procedury operacyjne resortowe SRnIK"* – procedury na potrzeby administratorów i użytkowników resortu ON;

---

[81] Z dnia 25 stycznia 2007 r.

[82] Memorandum of understanding between NATO Cyber Defence Management Authority (CDMA) and National Security Authority of the Republic of Poland concerning co-operation on Cyber Defence (Short Title: PL NSA - NATO CDMA MoU, Version 12 April 2011) – MCISA.

[83] Sprawy podziału zadań w zakresie ochrony infrastruktury krytycznej reguluje Decyzja Nr 14/MON Ministra Obrony Narodowej z dnia 27 stycznia 2014 r. w sprawie podziału odpowiedzialności za realizację zadań zarządzania kryzysowego z zakresu ochrony infrastruktury krytycznej w resorcie obrony narodowej (Dz. Urz. z 2014 r. poz. 33).

– „Standardowe procedury operacyjne lokalne SRnIK" – procedury na potrzeby Centrum Technicznego SRnIK.

Tabela nr 1. Usługi oferowane przez MIL-CERT.PL w latach 2012-2014[84].

Podmioty, na rzecz których świadczono usługi (np. poczta, portale internetowe)	**Działania prewencyjne**	**Reagowanie na incydenty i zagrożenia**	**Obsługa artefaktów**	**Usługi wpływające na podniesienie ogólnego poziomu bezpieczeństwa IT**	**Inne usługi**
Instytucje rządowe i inne podmioty publiczne		Wymiana informacji			
Operatorzy informatycznej infrastruktury krytycznej					
Inne krajowe zespoły CERT	Wymiana informacji	Wymiana informacji		Wymiana informacji	
Indywidualni użytkownicy cyberprzestrzeni np. domen (w tym także spoza RON)	Ochrona antywirusowa /antyspamowa	Obsługa incydentów, analiza kodu złośliwego			
Inne krajowe podmioty będące użytkownikami administratorami cyberprzestrzeni		Wymiana informacji			
Inni (w MON)	Szkolenia, ochrona antywirusowa/anty spamowa, system DLP (ochrona przed wyciekiem danych), wymiana informacji	Obsługa incydentów, analiza kodu złośliwego, wymiana informacji		Systemy bezpieczeństwa teleinformatycznego: - IPS, - firewall, - webgateway. - antywirus / antyspam	

Opracowanie własne kontrolera NIK. Źródło: Informacje RCZBSiUT.

(dowód: akta kontroli Tom 1 str. 52-60)

Klasyfikacja incydentów jest zamieszczona na portalu sbt.ron.int w niejawnym systemie teleinformatycznym MIL-WAN oraz w *„Podręczniku reagowania na incydenty komputerowe w resorcie obrony narodowej"*. Poszczególne kategorie odnoszą się nie do użytkowników, ale do występujących incydentów. Standardowe procedury operacyjne resortowe SRnIK były zamieszczane na portalu sbt.ron.int - obecnie w opracowaniu jest nowa wersja procedur – mają zostać opublikowane na portalu po zatwierdzeniu.

W latach 2012-2014 obsłużono 11.174 incydentów komputerowych w systemach teleinformatycznych resortu ON[85]. Wszystkie incydenty są istotne, jednak – w opinii RCZBSiUT - bardzo poważnym był incydent dotyczący poczty elektronicznej (system INTER-MON). MIL-CERT.PL prowadzi roczną ewidencję obsłużonych incydentów, która zawiera m.in. numer incydentu, datę zgłoszenia, kategorię incydentu, źródło informacji o incydencie, miejsce wystąpienia incydentu, nazwę systemu teleinformatycznego, w którym wystąpił incydent, zagrożenie (wirus, trojan, botnet itp.), nazwa użytkownika zalogowanego do komputera na którym wystąpił incydent.

(dowód: akta kontroli Tom 1 str. 52-75)

[84] Brak danych liczbowych (w resorcie ON nie prowadzono statystyk w zakresie ilości działań).

[85] Według informacji Komendanta RCZBSiUT na dzień 22.08.2014 r. Bardziej szczegółowe informacje stanowią informacje niejawne zamieszczone w ww. raportach o stanie bezpieczeństwa cyberprzestrzeni RON.

Zasoby Zespołu MIL-CERT.PL

Zespół MIL-CERT.PL posiada[86] 21 etatów (11 żołnierzy zawodowych, w tym 2 nieobsadzone (vacaty) i 1 żołnierz zawodowy oddelegowany (poza MIL-CERT.PL) oraz 10 pracowników wojska).

MIL-CERT.PL dysponuje centralnie zarządzanymi systemami bezpieczeństwa:

- w sieci wewnętrznej MON (zastrzeżonej): centralna ochrona antywirusowa; centralny system DLP - system zapobiegający wyciekowi danych;
- w sieci INTER-MON (jawnej): centralnie zarządzane firewalle; centralnie zarządzane IPS, systemy WebGateway, systemy antywirusowe / antyspamowe na bramkach internetowych;
- urządzenia do informatyki śledczej;
- oprogramowanie specjalistyczne.

Komendant RCZBSiUT wyjaśnił, że budżet roczny MIL-CERT.PL związany jest z kosztami etatowymi utrzymania zespołu. Koszty związane z zakupem, wdrażaniem i utrzymaniem systemów bezpieczeństwa teleinformatycznego w latach 2012-2014 to około 15,6 mln. zł.

(dowód: akta kontroli Tom 1 str. 52-75, 443-463)

Współpraca MIL-CERT.PL z innymi podmiotami, w tym CERT

MIL-CERT.PL w ramach krajowego systemu reagowania na incydenty komputerowe wykorzystuje bezpieczny kanał łączności CATEL[87].

Do kontaktów z innymi zespołami CERT wykorzystywana jest poczta elektroniczna w sieci Internet. Komunikacja pomiędzy Zespołami typu CERT jest szyfrowana.

Komendant RCZBSiUT wyjaśnił, że odrębnym trybem przekazywane są incydenty istotne wymagające natychmiastowej reakcji, gdzie odbiorców ustala się według potrzeb.

Incydenty podlegają raportowaniu do organizatorów systemów teleinformatycznych resortu ON oraz Pełnomocnika ds. Bezpieczeństwa Cyberprzestrzeni raz na tydzień.

Od 2014 roku Pełnomocnik ds. Bezpieczeństwa Cyberprzestrzeni wykonuje roczny raport o stanie bezpieczeństwa cyberprzestrzeni resortu ON.

W Zespole MIL-CERT.PL wskaźnikiem monitorowania realizacji jego głównych zadań jest wykrywalność incydentów prezentowana w meldunku tygodniowym na wideokonferencji służb teleinformatycznych RON.

Współpraca MIL-CERT.PL jest organizowana na podstawie osobnych porozumień, które określają zakres współpracy oraz kanały komunikacji:

- porozumienie między Ministrem Obrony Narodowej a Szefem Agencji Bezpieczeństwa Wewnętrznego w sprawie współpracy w zakresie reagowania na incydenty komputerowe oraz bezpieczeństwa teleinformatycznego;
- porozumienie pomiędzy Departamentem Obrony USA a Ministrem Obrony Narodowej RP dotyczącego współpracy w zakresie bezpieczeństwa informacji i sieci komputerowych.

W ramach NATO MIL-CERT.PL współpracuje ze swoim odpowiednikiem NATO-wskim – NCIRC[88]. Resort ON nie realizuje zadań punktu kontaktowego NATO (NATO Focal Point)

---

[86] Według informacji Komendanta RCZBSiUT na dzień 22.08.2014 r.

[87] System CATEL wykorzystywany jest do przetwarzania informacji niejawnych w ramach Sieci Łączności Rządowej w oparciu o rozporządzenie Prezesa Rady Ministrów z dnia 16 września 2010 r. w sprawie szczegółowych zasad wykonywania działalności telekomunikacyjnej w Sieci Łączności Rządowej (Dz. U. Nr 177, poz. 1192). Jednostką organizującą CATEL jest ABW.

– zadanie te realizowane są przez ABW jako Krajową Władzę Bezpieczeństwa (Szef ABW wraz z kadrowym zapleczem technicznym stanowi Krajowy Punkt Centralny w ramach polityki ochrony cyberprzestrzeni NATO).

Realizowana jest wymiana informacji z innymi zespołami i podmiotami krajowymi[89].

Pełnomocnik Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni wyjaśnił, że *„na spotkaniach grup roboczych MON, w swoich wystąpieniach podkreśla istotną rolę współpracy z innymi instytucjami tworzącymi Krajowy System Reagowania na Incydenty Komputerowe w cyberprzestrzeni RP."*

Zespół MIL-CERT.PL dysponuje danymi kontaktowymi administratorów systemów teleinformatycznych, które pozwalają na wymianę informacji i bieżące koordynowanie działań w sytuacji zagrożenia lub wystąpienia incydentu - jest w posiadaniu danych kontaktowych do około 900 administratorów lokalnych w resorcie ON oraz do administratorów systemów teleinformatycznych w następujących instytucjach: ISI; RCZSiUT, Centrum Wsparcia Teleinformatycznego i Dowodzenia Marynarki Wojennej; Centrach Wsparcia Teleinformatycznego: Sił Powietrznych, Wojsk Lądowych; Zespołach Zarządzania Wsparciem Teleinformatycznym: w Warszawie, w Krakowie, w Bydgoszczy i we Wrocławiu oraz Centrum Wsparcia Mobilnych Systemów Dowodzenia.

Komendant RCZBSiUT wyjaśnił, że *„dobór osób kontaktowych wynika z ich zakresu obowiązków (...)."*

(dowód: akta kontroli Tom 1 str. 52-75, 443-463)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

3.4. System wczesnego ostrzegania

Opis stanu faktycznego

Resort ON bierze udział w projekcie ARAKIS[90] jako jego użytkownik od 2008 r. Po zakończeniu testów, resort ON planuje wdrożenie kolejnych sond systemu ARAKIS 2.0. Ponadto w resorcie ON funkcjonuje system ostrzegania przed zagrożeniami / ochrony przed zagrożeniami. Celem ww. projektów jest podwyższenie bezpieczeństwa systemów teleinformatycznych resortu ON. Mierniki jego osiągniecia oparte są na bazie liczby wykrytych incydentów komputerowych.

Pełnomocnik Ministra ON wyjaśnił, że cele te nie będą nigdy osiągnięte w 100 % ze względu na charakter cyberprzestrzeni i ciągle zmieniające się zagrożenia. Wdrażanie tych systemów powoduje zmniejszenie prawdopodobieństwa udanego ataku na systemy teleinformatyczne resortu ON. Obecnie zainstalowano ww. systemy w trzech jednostkach świadczących usługę dostępu do sieci Internet dla jednostek i instytucji resortu ON.

Resort ON nie bierze udziału w opracowaniu projektu szczegółowego do rządowej *„Polityki..."* określającego sposób rozbudowy systemu wczesnego ostrzegania.

(dowód: akta kontroli Tom 1 str. 62, 66-67, Tom 2 str. 1-103)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

3.5. Szkolenia i działania edukacyjne

Opis stanu faktycznego

Zagadnienia dotyczące obszaru ochrony cyberprzestrzeni i bezpieczeństwa teleinformatycznego ujęte są w programach kształcenia dla kandydatów na oficerów oraz programach kursów realizowanych w ramach systemu doskonalenia zawodowego

---

[88] NATO Cyber Incident Response Center.

[89] Więcej na temat współpracy krajowej w rozdziale 1.6. niniejszego wystąpienia.

[90] ARAKIS.GOV. Szczegółowe informacje stanowią informacje niejawne.

żołnierzy. Ponadto na Wydziale Cybernetyki WAT utworzono nowy kierunek studiów Kryptologia i Cyberbezpieczeństwo, którego zadaniem jest kształcenie specjalistów w powyższych dziedzinach na potrzeby resortu ON.

Dodatkowo w celu poprawy świadomości na temat cyberzagrożeń w resorcie ON prowadzone są specjalistyczne szkolenia dla potrzeb personelu cyberbezpieczeństwa oraz szkolenia dla użytkowników.

Proces szkolenia odbywa się w oparciu o wymagania przedstawione w KOS[91]. Wymagania szkoleniowe zawarte w Karcie Opisu Stanowiska podlegają okresowej aktualizacji odpowiednio do stawianych zadań.

Minister Obrony Narodowej wyjaśnił, że tworzone są możliwości szkoleniowe z zakresu cyberbezpieczeństwa. *„Specjalistyczne szkolenia dla personelu cyberbezpieczeństwa oparte są głównie o szkolenia dostępne na rynku cywilnym oraz o szkolenia i kursy dostępne w jednostkach szkolnictwa NATO (NCISS w Latinie, CCDCOE w Tallinie). Obecnie RCZBSiUT prowadzi szkolenia m.in. z zakresu bezpiecznego użytkowania sieci INTER-MON. Zgodnie z praktyką ogólnowojskową kwestie monitorowania szkoleń znajdują się w gestii dowódców jednostek. Potrzeby w zakresie szkoleń pozostają w gestii kierowników jednostek i komórek organizacyjnych, którzy zgłaszają je do RCZBSiUT."*

W latach 2012–2014 w obszarze cyberbezpieczeństwa dla MON i innych jednostek organizacyjnych resortu ON RCZBSiUT zrealizowało m.in. szkolenia[92] z zasad bezpiecznego użytkowania komputera podłączonego do sieci Internet, analizy ryzyka w systemie Bezpieczeństwa Informacji, mechanizmów działania współczesnych zagrożeń (na przykładzie Zeusa, Suxneta, Aurory), Polityki Bezpieczeństwa Cyberprzestrzeni, socjotechniki w bezpieczeństwie teleinformatycznym, bezpieczeństwa systemów teleinformatycznych (zagrożeń, przeciwdziałania, zasad postępowania) oraz szkolenia specjalistyczne (na potrzeby np. CBC SZ, DIiT MON / ISI) – realizowane m.in. przez firmy komercyjne – w kraju i zagranicą (np. w NATO CCDCOE w Tallinie).

(dowód: akta kontroli Tom 1 str. 77, 84-91, Tom 2 str. 1-31)

W resorcie ON Centrum Techniczne SRnIK organizuje dla personelu komórek i jednostek organizacyjnych szkolenia z zakresu reagowania na incydenty komputerowe oraz bezpieczeństwa teleinformatycznego. Prowadzi również portale informacyjne w sieciach INTER-MON (jawna) i MIL-WAN (niejawna) dotyczące obsługi incydentów komputerowych i prowadzonych działań informacyjnych.

Żandarmeria Wojskowa uruchomiła projekt profilaktyczny *„Bezpieczeństwo użytkowników w sieci"*, który jest skierowany do środowiska wojskowego. W 2012 r. w ramach tego projektu podpisano porozumienie pomiędzy Żandarmerią Wojskową a firmą Microsoft dotyczące współpracy w obszarze bezpieczeństwa użytkowników sieci. Podpisanie porozumienia umożliwiło ŻW przygotowanie 48 instruktorów do prowadzenia zajęć. Żandarmeria Wojskowa w 2013 r. przeprowadziła 140 szkoleń, w których uczestniczyło 4170 osób.

(dowód: akta kontroli Tom 1 str. 78, 92)

Minister Obrony Narodowej poinformował, że w resorcie ON prowadzone są prace koncepcyjno-organizacyjne w celu stworzenia kompleksowego systemu szkoleń w zakresie cyberbezpieczeństwa oraz zapewnienia odpowiedniego poziomu świadomości wśród wyższej kadry kierowniczej i dowódczej. Przewiduje się, że system szkoleń wykorzysta krajowe możliwości jednostek szkolnictwa wojskowego (WAT, AON, AMW, WSOWL, CSŁil) oraz jednostki szkolnictwa państw członkowskich NATO. W celu wykorzystania możliwości

---

[91] Karta Opisu Stanowiska – dokument obowiązujący w resorcie ON, w którym określone są zadania oraz wymagane przeszkolenie dla danego stanowiska.

[92] Według stanu na 26.08.2014 r.

szkoleniowych oferowanych przez kraje członkowskie NATO planuje się podpisanie porozumienia w sprawie uczestnictwa resortu ON w międzynarodowym projekcie szkoleniowym z obszaru cyberbezpieczeństwa o nazwie Multinational Cyber Defense Education and Training.

(dowód: akta kontroli Tom 1 str. 77, 91)

W zakresie szkoleń resort ON nie otrzymywał zaleceń i wytycznych od innych podmiotów (w tym MAiC) realizujących zadania w zakresie ochrony cyberprzestrzeni RP.

(dowód: akta kontroli Tom 1 str. 77, 90)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

3.6. Wsparcie badań i rozwoju

Opis stanu faktycznego

Tematy badań naukowych resortu ON dotyczące ochrony cyberprzestrzeni proponowane i realizowane są w ramach:

- resortowego *„Planu badań naukowych prac rozwojowych i studyjnych"* (wykonawcy wyłaniani w wyniku procedur przetargowych realizowanych przez MON)[93],
- zarządzania przez Narodowe Centrum Badań i Rozwoju realizacją badań naukowych lub prac rozwojowych na rzecz obronności i bezpieczeństwa państwa (wykonawcy wyłaniani w konkursach organizowanych przez NCBR)[94].

W latach 2010–2014[95] (do dnia 18 sierpnia 2014 r.) w zakresie dotyczącym ochrony cyberprzestrzeni w realizacji było łącznie 13 projektów badawczych[96], w tym:

- 10 tematów badań naukowych zgłoszono (do finansowania) w ww. resortowych planach badań, z tego 5 projektów – zakończono i 5 projektów – w realizacji,
- 3 projekty uzyskały finansowanie w wyniku przeprowadzonych przez NCBR postępowań konkursowych[97], z tego 1 projekt – zakończono i 2 projekty – w realizacji.

---

[93] Do dnia 21 lipca 2014 r. kwestie realizacji badań naukowych w MON regulowane były decyzją Nr 199/MON Ministra Obrony Narodowej z dnia 21 lipca 2005 r. w sprawie wprowadzenia do użytku *„Instrukcji o realizacji badań naukowych i prac studyjnych w resorcie obrony narodowej"* (Dz.Urz. MON Nr 13, poz. 104 ze zm.). Obecnie obowiązuje decyzja Nr 299/MON Ministra Obrony Narodowej z dnia 21 lipca 2014 r. w sprawie koordynacji, planowania i realizacji badań naukowych w resorcie obrony narodowej (Dz.Urz. MON z 2014 r. poz. 248).

[94] NCBR na podstawie wniosków Ministra Obrony Narodowej przygotowuje i ogłasza kolejne konkursy na realizacje badań naukowych i projektów rozwojowych z obszaru bezpieczeństwa i obronności państwa, w tym projekty z obszaru ochrony cyberprzestrzeni. Wynikiem przeprowadzonych postępowań konkursowych jest wyłoniony wykonawca projektu, z którym Dyrektor NCBR podpisuje umowy na ich realizację.

Ciałem decyzyjnym, wspierającym Dyrektora NCBR jest Komitet Sterujący NCBR (przedstawiciele MON, MSWA, MNiSW, ABW oraz przedstawiciele środowisk przemysłu zbrojeniowego, technologii informacyjnych i energetyki - wskazywani przez Ministra Obrony Narodowej).

Finansowanie badań naukowych i prac rozwojowych z obszaru bezpieczeństwa i obronności państwa regulowane są ustawą o zasadach finansowania nauki z dnia 30 kwietnia 2010 r. (Dz.U. Nr 96, poz. 615 ze zm.) oraz rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 4 stycznia 2011 r. w sprawie sposobu zarządzania przez Narodowe Centrum Badań i Rozwoju realizacją badań naukowych lub prac rozwojowych na rzecz obronności i bezpieczeństwa państwa (Dz.U. Nr 18, poz. 91). Sposób nadzoru w ramach resortu ON nad ww. projektami określono w decyzji Nr 59/MON Ministra Obrony Narodowej z dnia 26 lutego 2014 r. w sprawie wytycznych dotyczących planowania i realizacji w resorcie obrony narodowej czynności nadzoru nad projektami dotyczącymi obronności i bezpieczeństwa państwa realizowanymi poza resortem obrony narodowej (Dz.Urz. MON z 2014 r. poz. 74).

[95] Tematy badań naukowych z obszaru ochrony w cyberprzestrzeni były umieszczane w resortowym *„Planie badań naukowych prac rozwojowych i studyjnych"* od roku 2010.

[96] W tym także realizowane przez konsorcja podmiotów (np. NASK, Wojskowy Instytut Łączności).

Tematy zgłaszane przez instytucje resortu ON, opiniowane były przez koordynatorów badań naukowych lub uzgadniane przez Radę Uzbrojenia. Wyniki 5 zakończonych w latach 2012–2014 tematów badań naukowych, w postaci demonstratorów technologii i oprogramowania, zostały przejęte i wdrożone przez właściwych gestorów, wyniki 1 projektu, realizowanego w NCBR, zostały odebrane przez Zespół Nadzorujący i czekają na przekazanie gestorowi.

Wymienione wyżej 13 projekty realizowano w latach 2012-2014 dotyczyły następujących głównych dziedzin szczegółowych: zabezpieczenia przed emisją ujawniającą od sprzętu teleinformatycznego, w tym wizyjną i elektromagnetyczną; informatycznego sprzętu klasy TEMPEST; zabezpieczenia przed podsłuchem laserowym oraz inpersonalizacją abonenta w systemach teleinformatycznych; zarządzania bezpieczeństwem teleinformatycznym resortu ON; tworzenia oprogramowania do wykrywania ukrytych funkcji w sprzęcie i kanałach informacyjnych; dynamicznego zarządzanie widmem sprzętu łączności; łączności satelitarnej.

Jak wyjaśnił Minister Obrony Narodowej *„głównym celem realizacji projektów informatycznych (...) było uzyskanie narzędzi do weryfikacji zabezpieczeń systemów teleinformatycznych, zarządzania systemami teleinformatycznymi resortu ON, jak również uzyskanie systemów do testowania i szkolenia. (...) Tematyka projektów badawczych była zgodna z zamierzeniami resortu w tym zakresie, zawartymi w dokumencie „Priorytetowe kierunki badań naukowych resortu obrony narodowej w latach 2013-2022" oraz we wcześniejszej wersji tego dokumentu obejmującej lata 2009-2021."*

W ramach realizacji tych projektów informatycznych, ujętych w planach badań naukowych resortu ON w latach 2012-2014 (do dnia 20 sierpnia 2014 r.), wydatkowano łącznie kwotę: 5 986 693 zł[98]. W tym samym okresie w NCBR wydatkowano kwotę 39 025 638 zł[99]. W projektach tych nie wyszczególniano podziału na cyberbezpieczeństwo i informatyzację.

W badania z obszaru ochrony cyberprzestrzeni były zaangażowane uczelnie (m.in. WAT, AMW, Politechnika Warszawska) oraz instytuty badawcze (m.in. WIŁ, NASK). Wymienione podmioty angażowane były do wyłaniania wykonawców, w konkursach NCBR oraz procedurach przetargowych MON.

Od 1 grudnia 2013 r. NCK jest zaangażowane (w ramach konsorcjum) w realizację jednego projektu (współfinansowanego przez NCBR niejawnego projektu naukowo-badawczego „ROTOR") związanego z budową systemu zarządzania bezpieczeństwem teleinformatycznym resortu ON, mającego na celu stworzenie centrum kompetencji i odpowiedzialności w RON w obszarze kryptologii.

W 2014 r. NCK zgłosiło do resortowego projektu planu badań naukowych na lata 2015-2016 propozycję 5 nowych tematów badań naukowych z obszaru ochrony

---

[97] Nie wszystkie wnioskowane projekty uzyskały finansowanie - resort ON w 2011 r. oraz 2013 r. skierował do NCBR wnioski na uruchomienie 6 tematów z obszaru ochrony w cyberprzestrzeni, z których 3 ww. projekty uzyskały wsparcie.

[98] Informacje o wysokości środków przeznaczanych na badania naukowe w obszarze techniki i technologii obronnych, są elementem planowania budżetowego resortu i rozpisane są szczegółowo w resortowym planie badań naukowych, który od roku 2013 jest dokumentem zastrzeżonym. Informacje o wysokości środków na realizację badań naukowych są upubliczniane na zasadach przyjętych w MON dla trybów postępowań, według których wyłaniani są wykonawcy poszczególnych projektów (np. podczas otwarcia ofert zamawiający informuje o wysokości środków, które planuje przeznaczyć na realizację zamówienia). Wysokość zakontraktowanej kwoty wydatków zawarta w umowach na ich realizację jest informacją do wiadomości wykonawcy i zamawiającego na zasadach ogólnych (prawa handlowego).

[99] W przypadku konkursów NCBR, upubliczniane są informacje ogólne o wysokości kwot na realizację łącznie wszystkich umów. W ramach prac Sejmowej Komisji Obrony Narodowej przekazywane były bardziej szczegółowe informacje dotyczące finansowania projektów w poszczególnych priorytetowych obszarach badawczych oraz z wyszczególnieniem kwot na realizację niektórych projektów.

w cyberprzestrzeni i kryptologii. NCK wnioskowało do Departamentu Nauki i Szkolnictwa Wojskowego (DNiSW) MON o utworzenie nowego, odrębnego Programu Strategicznego Badań Naukowych i Prac Rozwojowych w NCBR w obszarach kryptologii i cyberbezpieczeństwa. Na lata 2015-2025 zaproponowano 10 projektów dotyczących cyberbezpieczeństwa i 23 kryptologii. Uruchomienie projektów strategicznych jest procedowane przez DNiSW.

(dowód: akta kontroli Tom 1 str. 78, 92-96, 206-207, 290, 404-424, Tom 2 str. 1-31)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

Ocena cząstkowa

Kontrola wykazała, że w resorcie ON podejmowano działania w zakresie wzmacniania zdolności w ramach ochrony cyberprzestrzeni, w tym: ustanowiono wymogi w zakresie bezpieczeństwa teleinformatycznego, przedstawiciele resortu ON brali udział w ćwiczeniach systemu bezpieczeństwa cyberprzestrzeni, przeprowadzano testy systemów i sieci teleinformatycznych, ustanowiono i rozwijano zespół MIL-CERT.PL, w resorcie funkcjonował, w ramach infrastruktury teleinformatycznej, system wczesnego ostrzegania przed zagrożeniami, realizowano działania w zakresie szkoleń i działania edukacyjne, a także wspierano działalność badawczą i rozwojową.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[100], wnosi o:

1. Podjęcie, w uzgodnieniu z Ministrem Administracji i Cyfryzacji, działań mających na celu zdefiniowanie roli i zadań resortu ON w ramach budowanego systemu ochrony cyberprzestrzeni RP.
2. Opracowanie katalogu (wykazu) propozycji koniecznych zmian legislacyjnych i podjęcie działań legislacyjnych w celu nadania Siłom Zbrojnym odpowiednich uprawnień i możliwości w odniesieniu do realizacji zadań związanych z ochroną / obroną cyberprzestrzeni RP.
3. Przygotowanie modelu docelowego rozwiązania strukturalno-organizacyjnego w zakresie ochrony / obrony cyberprzestrzeni RP wraz z harmonogramem prac modernizacyjnych w resorcie ON i wnioskami do centralnych planów rzeczowych (w zakresie zadań finansowanych 2015 r. i 2016 r.).
4. Określenie (oszacowanie) do końca I kwartału 2015 r. potrzebnych zasobów finansowych, infrastrukturalnych i osobowych w ramach resortu ON w celu realizacji zadań ochrony / obrony cyberprzestrzeni w 2015 r. i latach następnych.
5. Umieszczenie działalności w zakresie ochrony / obrony cyberprzestrzeni w strukturze działań w ramach budżetu zadaniowego, wypracowanie metodologii planowania wydatków w tym zakresie oraz przeprowadzenie odpowiednich zmian budżetowych.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Zgodnie z art. 54 ustawy o NIK przysługuje Panu Ministrowi prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do Prezesa Najwyższej Izby Kontroli.

[100] Dz.U. z 2012 r. poz. 82 ze zm.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Warszawa, dnia 2... grudnia 2014 r.

Wiceprezes
Najwyższej Izby Kontroli
Wojciech Kutyła

podpis