MON bezbronne w cyberprzestrzeni

18 grudnia 2015

Przez kilka lat nieznani sprawcy wykradali wojskową korespondencję e-mailową. Sprawę wykryły cywilne służby specjalne. W związku z tym w latach 2013-2014 podjęto próbę uporządkowania i wzmocnienia tej formacji Sił Zbrojnych, która powinna zajmować się walką w cyberprzestrzeni. Niestety, działania te nie zostały doprowadzone do końca. Przeciwnie, w bieżącym roku powrócono do rozproszonej struktury instytucji odpowiedzialnych za bezpieczeństwo w tej sferze. Utracono przy tym wysokokwalifikowanych specjalistów. Nie wdrożono też planów stworzenia własnych rozwiązań zarówno dotyczących oprogramowania, jak i urządzeń, bazując na dostępnych produktach rynkowych. W rezultacie poziom bezpieczeństwa teleinformatycznego MON znacznie się obniżył. Prawdopodobnie proceder hakowania i wykradania korespondencji został wznowiony...

Defilada z okazji dnia Wojska Polskiego. Nie można wykluczyć, że w widocznej grupie najwyższych rangą oficerów i urzędników są osoby, których konta mailowe została zhakowane wieloletnim atakiem cybernetycznym... / Zdjęcie: MON

W grudniu 2014 zakończyła się w MON kompleksowa kontrola NIK dotycząca realizacji przez ten resort *Polityki ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* przyjętej przez Radę Ministrów 25 czerwca 2013. W wystąpieniu pokontrolnym, a szczególnie w opublikowanej w czerwcu 2015 *Informacji o wynikach kontroli realizacji przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP,* generalnie NIK oceniła działania instytucji państwowych bardzo negatywnie. Jednym z wyjątków był – choć z poważnymi zastrzeżeniami – resort obrony.

Niemal pozytywna ocena

Czym MON zasłużyło na taką opinię? Przede wszystkim tym, że utrzymywało zespół MIL-CERT (Oddział Bieżącego Zarządzania Bezpieczeństwem Teleinformatycznym),

stworzyło trójpoziomowy funkcjonalny System Reagowania na Incydenty Komputerowe (SRnIK) oraz powołało w 2013 specjalistyczną jednostkę wojskową – Narodowe Centrum Kryptologii (NCK).

Według NIK były też mankamenty: *resort obrony narodowej nie dysponuje jednak odpowiednią liczbą specjalistów posiadających wystarczające kwalifikacje w obszarze ochrony cyberprzestrzeni – stanukompletowania jednostek odpowiadających za bezpieczeństwo IT wynosił tylko 40%. Ponadto, cały system organizacyjny resortu powołany do ochrony cyberprzestrzeni zostałpodporządkowany NCK – nowej jednostce organizacyjnej zajmującej się tylko jednym z aspektów bezpieczeństwa informacji, jakim jest* poufność, *i będącej dopiero na etapieformowania. Z ustaleń kontroli wynika, że Kierownictwo NCK napotykało na istotne problemyzwiązane z rekrutacją wykwalifikowanego personelu (prawie półtora roku od utworzeniajednostki stan jej ukompletowania wynosił tylko 36%) oraz nie dysponowało infrastrukturą(bazą lokalową i zapleczem technologiczno-produkcyjnym) pozwalającą na rozpoczęcieefektywnej działalności. Stworzyło to, w ocenie NIK, duże ryzyko dla ciągłości działaniai efektywności struktur organizacyjnych resortu powołanych do ochrony cyberprzestrzeni.*

Uwagi NIK dotyczyły także podporządkowania całego systemu instytucjonalnego resortu związanego z bezpieczeństwem IT *jednej osobie, będącej jednocześnie m.in. Pełnomocnikiem Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni, Dyrektorem NCK oraz Przewodniczącym (...) resortowego Zespołu ds. Opracowania Projektu Założeń do Planu Obrony Cyberprzestrzeni RP.*

Wskazane przez NIK ryzyko, dotyczące odejścia ww. osoby z Ministerstwa, zmaterializowało się bezpośrednio po zakończeniu kontroli, w styczniu 2015, co skutkowało koniecznością dokonania istotnych zmian strukturalnych i kadrowych w systemie ochrony cyberprzestrzeni MON.

Wcześniejsza, krytyczna diagnoza

Oprócz tej kontroli w resorcie obrony, już w latach 2013-14 dokonano innego, całościowego badania stanu bezpieczeństwa cybernetycznego. Przeprowadził je, za aprobatą szefa ministerstwa, jego doradca ds. bezpieczeństwa cyberprzestrzeni wraz z zespołem ekspertów.

Wieloaspektowy audyt dotyczył przede wszystkim obszaru prawno-dokumentacyjnego (strategii, koncepcji, planów operacyjnych Sił Zbrojnych, sprawozdań wykonawczych i innych dokumentów resortu, także niejawnych), stanu ewidencyjnego (w tym stanów uzbrojenia i ilości jednostek wojskowych związanych z bezpieczeństwem

cybernetycznym, ich liczebności i kwalifikacji personelu), kierunków informatyzacji i środków finansowych przeznaczanych na bezpieczeństwo cybernetyczne.

Minister obrony narodowej Tomasz Siemoniak – wraz ze swoimi zastępcami, Czesławem Mroczkiem i Robertem Kupieckim – przed rozmowami z Thomasem A. Kennedym, prezesem zarządu i dyrektorem generalnym koncernu Raytheon. Resort obrony prowadzi postępowania przetargowe o wartości dziesiątek mld zł. Wiele wrażliwych danych o negocjacjach znajduje się w poufnej poczcie polskich urzędników. Jeżeli dostęp do tych danych mogły zdobyć służby obcego państwa, podobne działania mogą podejmować specjaliści wywiadu gospodarczego, także z grona państw sojuszniczych / Zdjęcie: MON

Ocena wynikająca z audytu była zdecydowanie krytyczna. Przedstawiano ją ministrowi obrony narodowej sukcesywnie, począwszy od kwietnia 2013 i przez cały 2014. Zaproponowano także kompleksową propozycję naprawy, a w zasadzie zamiar zbudowania prawdziwego, a nie fikcyjnego bezpieczeństwa cybernetycznego resortu. Na uwagę zasługiwały m.in. propozycje użycia polskich, niskobudżetowych rozwiązań komunikacyjnych, z polskim oprogramowaniem i urządzeniami stanowiącymi własność Skarbu Państwa, powstałymi w kraju dzięki pracom naukowo-badawczym. Niestety, wiele z ówczesnych wskazań jest aktualnych do dzisiaj.

Resortowa cyberkatastrofa

Na realne cyberbezpieczeństwo MON i Sił Zbrojnych RP składa się w pierwszej kolejności ochrona własnych systemów i sieci teleinformatycznych oraz systemów pola walki przed podsłuchem, przejęciem, wyłączeniem i zmianą treści komunikacji. Ochrona ta musi być realizowana za pomocą odpowiedniego oprogramowania oraz narzędzi cybernetycznych, w tym poprzez własne rozwiązania kryptograficzne. Cyberochrona powinna odbywać się zarówno w obszarze oprogramowania, jak i sprzętu (software i hardware). Dotyczy urządzeń sieciowych, serwerów i sprzętu użytkownika końcowego. Niezwykle ważna jest kompetencja badania zgodności na poziomie standardów oraz protokołów komunikacyjnych. Krótko mówiąc, cyberochrona ma stworzyć bezpieczną cyberprzestrzeń resortu obrony, czyli to, czego dziś tak bardzo... brak.

Audyt ujawnił, że w bezpieczeństwie teleinformatycznym zapóźnienia polskiej armii są wieloletnie. Stan swoistej *katastrofy* w tej dziedzinie budzi niepokój zwłaszcza, jeśli policzy się setki milionów złotych wydane na informatyzację armii, tysiące żołnierzy w korpusie łączności i deklarowaną przez Inspektorat Systemów Informacyjnych gotowość wojska do działania w warunkach pokoju, kryzysu i wojny. Widoczna była także niechęć MON do stosowania w praktyce dostępnych i sprawdzonych w administracji rządowej mechanizmów bezpieczeństwa. A przede wszystkim – niepoważne traktowanie minimalnych standardów bezpieczeństwa NATO.

Francuskie czołgi Leclerc w czasie wspólnych, polsko-amerykańsko-francuskich ćwiczeń Puma-15 w maju br. Manewry były odpowiedzią na wzrost zagrożenia międzynarodowego związanego z konfliktem rosyjsko-ukraińskim. Jak sojusznicy mają traktować naszą wiarygodność jako partnera, skoro nie jesteśmy w stanie skutecznie bronić naszych i ich tajemnic w cyberprzestrzeni? / Zdjęcie: 15. Giżycka Brygada Zmechanizowana

Należało więc podjąć stanowcze i pilne działania. Podstawowym było stworzenie w cyberprzestrzeni bezpiecznej *wojskowej wyspy*: zapewnienie bezpieczeństwa własnych systemów łączności i dowodzenia, osiągnięcie bezpieczeństwa komunikacji pomiędzy kierownictwem resortu oraz wewnątrz armii. Koniecznym stało się zintegrowanie skromnego grona osób zajmujących się profesjonalnie cyberbezpieczeństwem i zakończenie dzikiej, zakupowej informatyzacji wojska. Bez tego całkowicie pozbawione podstaw były swoiste rojenia o prowadzeniu aktywnych działań w Internecie, o jakiejkolwiek cyberobronie kraju. Jeśli samemu nie potrafi się zabezpieczyć własnych sieci i systemów teleinformatycznych...

Dopiero drugim etapem miało być zbudowanie zdolności Sił Zbrojnych do działań w cyberprzestrzeni. Kształtując bowiem bezpieczną *wyspę MON* Siły Zbrojne powinny nabywać kompetencji w zakresie właściwej polityki i architektury bezpieczeństwa, posługiwania się odpowiednim oprogramowaniem i narzędziami. Muszą również nabyć kompetencje kompilacji, trwałej zdolności identyfikacji, modyfikacji oraz łamania kodów źródłowych. Nie może to się, rzecz jasna, odbyć bez odbudowania wojskowego dekryptażu. Kompetencje takie muszą być zbudowane w wysokospecjalistycznej jednostce wojskowej lub w kilku jednostkach, których innowacyjność będzie respektowana przez pragmatykę wojskową. Ponadto działanie tego centrum

kompetencji musi być wspierane przez wojskowe służby specjalne.

Żołnierze pełniący służbę w tych jednostkach powinni stanowić wyodrębniony korpus osobowy SZ. Zdolność do działań w cyberprzestrzeni nie może przy tym powstać w środowisku teleinformatycznym spenetrowanym przez przestępców, transparentnym dla globalnych potęg cybernetycznych czy w sieciach IT, których poziom bezpieczeństwa jest niższy niż w średniej wielkości banku spółdzielczym. A taki poziom bezpieczeństwa jest dzisiaj w MON. Ta zdolność do działania Sił Zbrojnych musi być oparta na własnych, polskich technologiach, wytworzonych lub współtworzonych przez wojsko, oraz spolonizowanych rozwiązaniach dostępnych na rynku.

Dopiero mając zapewnioną ochronę własnych systemów oraz posiadając zdolności do działań w cyberprzestrzeni, można budować aktywną cyberobronę naszego kraju – czyli realne zdolności ofensywne (najlepsza obrona jest przecież atak). Cały proces powinien odbywać się w oparciu o polską naukę i polskie technologie. Bo wojsko, które nie potrafi ochronić własnych systemów i sieci teleinformatycznych, nie będzie w stanie bronić cyberprzestrzeni RP. Co gorsza, polskie wojsko nie jest przygotowane doktrynalnie i operacyjnie do prowadzenia takich działań.

Stan faktyczny: zdolności defensywne

W tak zarysowanej teraźniejszości pierwszą linią realnej obrony w cyberprzestrzeni RP stanowi System Reagowania na Incydenty Komputerowe MON (SRnIK). System kształtował się wraz z rozbudową sieci i systemów teleinformatycznych w resorcie obrony. Stał się niezbędny po stworzeniu przez Departament Informatyki i Telekomunikacji (DIT) sieci jawnej INTER-MON i zastrzeżonej MIL-WAN. Wprowadzenie po 2006 do INTER-MON usługi Blackberry miało zapewnić mobilny i bezpieczny system komunikacji kadry kierowniczej resortu. Faktycznie zwiększała ona wygodę użytkowników, ale nie poziom bezpieczeństwa, m.in. ze względu na całkowitą *przejrzystość* systemu dla krajów-producentów systemu (Kanada, USA).

Ćwiczenia dowódczo-sztabowe Rubin15 Wojewódzkiego Sztabu Wojskowego w Rzeszowie. W ich trakcie wykorzystywano m.in. zastrzeżoną sieć wojskową MIL-WAN / Zdjęcie: WSzW w Rzeszowie

Znany dzisiaj system ochrony, SRnIK, ustanowiono decyzją MON Nr 357 z 29 lipca 2008, integrując wcześniej istniejące instytucje. Został on ostatecznie ukształtowany jako trzypoziomowa struktura funkcjonalna, obecna wyłącznie na poziomie taktycznym, poszczególnych Jednostek Wojskowych.

Poziom pierwszy tworzyło Centrum Koordynacyjne, którego funkcję spełniało istniejące od 2006 Wojskowe Biuro Łączności i Informatyki (przekształcone w 2011 w Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych). W ramach RCZBSiUT utworzono Oddział Bieżącego Zarządzania Bezpieczeństwem Teleinformatycznym MIL-CERT, tak pozytywnie wyeksponowany w raporcie NIK. Poziom drugi to Centrum Wsparcia Technicznego, którego funkcję spełniało Centrum Zarządzania Systemami Teleinformatycznymi, przekształcone w 2011 w Resortowe Centrum Zarządzania Sieci i Usług Teleinformatycznych (RCZSiUT). Poziom trzeci stanowili administratorzy systemów i sieci IT podlegli dowódcom jednostek wojskowych wykorzystujących INTER-MON i MIL-WAN.

Nadzór nad SRnIK sprawował dyrektor DIT, jednocześnie przełożony RCZSiUT i RCZBSiUT. Obie te jednostki liczyły po kilkadziesiąt osób. Natomiast orientacyjna liczba administratorów systemów IT w MON to ok. 900 osób. Systemy SKW i SWW były wyłączone z SRnIK. System ten odpowiadał za analizę ryzyka, odpowiednie polityki i wytyczne, podręczniki reagowania na incydenty komputerowe, standardowe procedury operacyjne oraz działania praktyczne, reagowania na incydenty we współpracy z administratorami systemów i usług.

16 lutego 2012 minister obrony narodowej, decyzją Nr 38, utworzył stanowisko Pełnomocnika MON ds. Bezpieczeństwa Cyberprzestrzeni. Pełnomocnikiem został dyrektor DIT. Odpowiadał on – jako przełożony jednostek wojskowych stanowiących I i

II poziom SRnIK – za kształtowania i wykonanie polityki resortu w zakresie bezpieczeństwa, a także kształtował i wykonywał politykę informatyzacji ministerstwa, w tym politykę inwestycyjną i zakupową. Można stwierdzić, że wszystkie zdolności cyberochrony i defensywy cybernetycznej znajdowały się w zakresie jego odpowiedzialności. Co więcej, posiadał on niezbędne umocowania prawne oraz środki finansowe i personalne do wypełnienia swego zadania. SRnIK i DIT, zajmując się bezpieczeństwem cyberprzestrzeni MON, posługiwał się jednak wyłącznie sprzętowymi i programistycznymi rozwiązaniami komercyjnymi dostępnymi na rynku. Jedynym wyjątkiem stanowiła eksploatowana przez MIL-CERT sonda systemu Arakis udostępniona przez ABW.

Ponieważ DIT zajmował się informatyzacją MON, to dyrektor tego departamentu – mimo, że był również Pełnomocnikiem MON ds. Bezpieczeństwa Cyberprzestrzeni – nie zadbał, by w dokumentach planistycznych resortu tematyka cyberbezpieczeństwa została wyodrębniona jako osobny dział. Nakłady na ten cel w latach 2008-14 wchodziły w zakres informatyki i łączności, a kierownictwo resortu uznawało nakłady na informatyzację za równoznaczne z nakładami na cyberbezpieczeństwo.

Stan faktyczny: zdolności ofensywne

Możliwość aktywnego działania w cyberprzestrzeni miało zapewnić wojsku Centrum Bezpieczeństwa Cybernetycznego Sił Zbrojnych (CBC). Ta jednostka szczebla taktycznego została utworzona w 2010. Podporządkowano ją Zarządowi Planowania Systemów Dowodzenia i Łączności (P-6) Sztabu Generalnego. Pełną gotowość bojową jednostka miła osiągnąć w 2015. Niestety, do tego nie doszło. Ostatecznie CBC została rozwiązana przed upływem tego terminu.

Na skuteczność jednostki negatywny wpływ miało kilka czynników. Po pierwsze, nie udało się wykorzystać wszystkich przewidzianych sił – przed rozwiązaniem Centrum miało jedynie 60% ukompletowania. Po drugie, istniał stały konflikt kompetencyjny pomiędzy DIT a P-6. Departament traktował bowiem cyberbezpieczeństwo jako element informatyzacji, a Zarząd jako element wsparcia systemu dowodzenia. Wreszcie CBC, jako jednostka tajna, działała w swoistej izolacji – do końca 2013 nie współpracowała z jednostkami wojskowymi podległymi DIT. Co gorsza, ta teoretyczna *ofensywa* była tworzona w oderwaniu od realnych zagrożeń występujących w sieciach i systemach IT MON. CBC do końca swego istnienia opierało się o dostępne na rynku rozwiązania komercyjne.

Niestety, mimo odseparowania MIL-WAN od ogólnych sieci komputerowych, okazało się, że została ona zainfekowana poważnymi wirusami komputerowymi. Przyczyną jest łamanie przez użytkowników podstawowych zasad bezpieczeństwa, w tym m.in. wykorzystywanie tych samych nośników pamięci w komputerach wpiętych do sieci wojskowej i urządzeniach prywatnych... / Zdjęcie: Michał Likowski

Niewątpliwym sukcesem było natomiast zatrudnienie kilkudziesięciu żołnierzy zawodowych o przyzwoitych kwalifikacjach. Było ich trzy razy więcej niż liczyła obsada MIL-CERTU, odpowiadająca za reakcję na incydenty komputerowe w resorcie obrony...

Reasumując: w latach 2008-13 informatyzacja i cyberbochrona w wojsku były zarządzane przez DIT, podlegający Dyrektorowi Generalnemu MON, przy czym dyrektor DIT był jednocześnie Pełnomocnikiem MON ds. Bezpieczeństwa Cyberprzestrzeni. Jednak nie zajmował się on sieciami oraz systemami SKW i SWW. Było to pokłosie braku zintegrowanego podejścia do bezpieczeństwa teleinformatycznego w ministerstwie i SG WP oraz wyboru odpowiedzialności *zgodne z właściwością* danego organu. W rezultacie rozwijano w separacji zdolności defensywne i zaczątki ofensywy (CBC), bez wymiany doświadczeń między poszczególnymi jednostkami wojskowymi. Wreszcie, w resortowych systemach INTER-MON i MIL-WAN posługiwano się wyłącznie zabezpieczeniami komercyjnymi. Oficjalnie jednak środki finansowe i zasoby ludzkie były wystarczające. Zaś według sprawozdań, cyberbezpieczeństwo ministerstwa obrony było niezagrożone.

Obraz cyberklęski

Latem 2013 szef resortu obrony został poinformowany z zewnątrz – przez ABW – o skierowanym na jego serwery ataku cybernetycznym. Po sprawdzeniu MIL-CERT potwierdził kierunek i rozległość ataku hakerskiego na pocztę mon.gov.pl.

Skala katastrofy – długi czas ataku i jego rozległość – była porażająca. Okazało się, że dotychczasowe kilkuletnie wysiłki, niemałe pieniądze oraz wykwalifikowane kadry, w tym działania SRnIK i SKW, nie uchroniły MON przed wieloletnim atakiem

cybernetycznym. Minister musiał podjąć zdecydowane działania mające zdiagnozować zagrożenia i naprawić szkody. Przede wszystkim zmieniono Pełnomocnika ds. Bezpieczeństwa Cybernetycznego. Dyrektora DIT zastąpił od 1 października 2013 dyrektor NCK. Podporządkowano mu RCZBSIUT i CBC SZ. Opracowano plan naprawczy i rozpoczęto jego wdrożenie.

Wstępna analiza ataku cybernetycznego, przedstawiona na kierownictwie resortu w listopadzie 2013, wykazała przejęcie kont poczty mon.gov.pl, w tym kadry kierowniczej, i utratę bardzo wielu informacji. Według dyrektora NCK należało podjąć radykalne kroki zwiększające cyberbezpieczeństwo. Dlatego opracowano kompleksowe *Wytyczne w sprawie szczegółowych zasad i zadań w zakresie kontroli dostępu, poufności informacji oraz rozliczalności funkcjonowania systemu INTER-MON* z 30 grudnia 2013. Wytyczne te zostały skierowane do organizatora systemu i administratorów systemu. Wdrażanie *Wytycznych* trwało przez cały 2014. Przy czym organizator systemu, Inspektorat Systemów Informacyjnych (ISI, dawne DIT), stale kwestionował restrykcyjne jego zdaniem wymagania bezpieczeństwa.

Ćwiczenia Gronost@j-15. W przedsięwzięciu – w wirtualnej sieci – wzięło udział niemal pół tysiąca żołnierzy 17. Wielkopolskiej Brygady Zmechanizowanej. Wydarzenie pomaga uzmysłowić, jak duże znaczenie mają współczesne systemy komputerowe... / Zdjęcie: MON

Zintegrowanie NCK, CBC i RCZBSIUT pod kierownictwem nowego Pełnomocnika dało wymierny efekt. W lutym 2014 MIL-CERT wykrył samodzielnie odnowienie poprzedniego ataku (oznaczało to, że wcześniejsze kroki podjęte w sierpniu i wrześniu 2013 przez służby MON były nieefektywne). Ponadto okazało się, że organizator systemu INTER-MON nie przekazał administratorom nowych wymagań bezpieczeństwa. Stanowcza, pisemna reakcja ze strony Pełnomocnika w stosunku do ISI pozwoliła opanować sytuację i powstrzymać atak. O skuteczności podjętych *ad hoc* działań świadczy ponowne wykrycie samodzielne przez MIL-CERT zmiany wektora ataku na pocztę MON w sierpniu 2014 i jego powstrzymanie na etapie początkowym. Jednak potrzeba działań systemowych wymagała podjęcia przez ministra radykalnych decyzji naprawczych oraz wyciągnięcia konsekwencji wobec odpowiedzialnych za ten

katastrofalny stan rzeczy.

Równocześnie w marcu 2014, po powstrzymaniu kolejnej fazy ataku cybernetycznego na pocztę INTER-MON, Pełnomocnik ds. BC przedstawił ministrowi aneks do programu naprawczego, wraz z propozycjami radykalnej zmiany podejścia do tematyki cyberbezpieczeństwa. Niestety, te i inne propozycje zostały zignorowane.

Ostatecznie pełen raport, z analizą powłamaniową, został przedłożony ministrowi obrony narodowej w listopadzie 2014. Rozmiar strat był następujący: kilkaset kont zostało zhakowanych, m.in. pracowników Inspektoratu Uzbrojenia, pionu kadr, sekretariatu ministra ON i poszczególnych członków ścisłego kierownictwa resortu. Ponadto kilkaset tysięcy wiadomości zostało skradzionych. Była to poczta teoretycznie jawna, ale zawierała m.in. projekty stanowisk MON w obszarze międzynarodowym, notatki ze spotkań z partnerami, także z NATO, szczegóły zamówień i przetargów zbrojeniowych, sprawy kadrowe, notatki służbowe, projekty stanowisk itp. Atak trwał bez przerw od wiosny 2009 do lata 2013 (analiza powłamaniowa dotyczyła okresu od wiosny 2009, ze względu na zachowane najstarsze logi systemowe). Jednak według oceny zespołu analitycznego MIL-CERT, atak mógł rozpocząć się już w 2006.

Raport Pełnomocnika zawierał też informację o tymczasowym powstrzymaniu tej katastrofy i proponował pilne środki zaradcze, w tym zmiany funkcjonale, techniczne i organizacyjne. Diagnozował także przyczyny tego stanu rzeczy, m.in. błędne kierunki informatyzacji, niekompetencję organizatora systemu i powszechny brak dyscypliny użytkowników. Pełny raport w trybie niejawnym otrzymali: minister obrony, jego zastępcy, dowódca generalny Rodzajów SZ, dowódca operacyjny, szef SG i szefowie specjalnych służb wojskowych.

Mimo, że najwyżsi rangą przedstawiciele MON podzielali zawartą w raporcie diagnozę o realności zagrożenia bezpieczeństwa i obronności RP, to nie stał się on przedmiotem narady kierownictwa resortu ani jakiejkolwiek głębszej refleksji. Katastrofa informatyczna w resorcie obrony nie była problemem, natomiast kłopotem stały się sam tekst i jego autor. Od stycznia 2015 temat postanowiono *zamieść pod dywan*.

Równocześnie z atakiem na INTER-MON w 2013-2014 obserwowano stałą obecność złośliwego oprogramowania w niejawnym MIL-WAN. System ten jest równie rozległy, jak sieć jawna (obejmują po kilkadziesiąt tysięcy komputerów). MIL-WAN stanowi główną platformę przesyłania skanów dokumentów oraz niejawnej komunikacji elektronicznej wewnątrz MON, a także z zagranicą. System ten był i jest nadal penetrowany oraz stale infekowany z zewnątrz. Propozycje uszczelnienia i eliminacji zagrożeń były stale ignorowane przez organizatora systemu: DIT/ISI, SKW oraz Departament Ochrony Informacji Niejawnych MON.

Próba uzyskania cyberbezpieczeństwa

Po uzyskaniu jesienią 2013 odpowiednich uprawnień oraz podporządkowaniu RCZBSIUT i CBC, dyrektor NCK – będący jednocześnie Pełnomocnikiem MON ds. Bezpieczeństwa Cybernetycznego – rozpoczął pracę ukierunkowaną na zintegrowanie posiadanych zasobów oraz zbudowanie zdolności Sił Zbrojnych do cyberochrony i cyberobrony RP. W procesie modernizacji sił zbrojnych uzyskano wstępną zgodę szefa resortu, by w ramach *Programu rozwoju SZ RP w latach 2013-22* stworzyć nowy *Program operacyjnego wsparcia kryptologicznego i obrony cyberprzestrzeni*. Założenia tego programu mają umożliwić:

- zabezpieczenie wyłącznej jurysdykcji państwa polskiego w obszarze technologicznym nad wojskowymi systemami kierowania, dowodzenia i łączności,

- uzyskanie przez SZ RP gotowości do prowadzenia operacji w cyberprzestrzeni za pomocą polskich narzędzi informatycznych i oprogramowania,

- odbudowę kryptografii i kryptoanalizy wojskowej,

- uzyskanie przez Polskę wiodącej roli w wielonarodowych inicjatywach rozwoju sojuszniczych zdolności obronnych,

- podniesienia wiarygodności państwa na arenie międzynarodowej, w tym w ramach przyjętych zobowiązań sojuszniczych i partnerskich,

- dostosowanie narodowych zdolności przeciwdziałania zagrożeniom cybernetycznym do światowych standardów NATO w zakresie *Cyber Defence*.

Budynek natowskiego Centrum Doskonalenia Cyberobrony w Tallinie (NATO Cooperative Cyber Defence Centre of Excellence)... / Zdjęcie: NATO

Modernizacja ta mogła być możliwa przez zbudowanie dwóch współdziałających ze sobą centrów kompetencji: kryptologicznego – Narodowego Centrum Kryptologii, i cyberbezpieczeństwa – Centrum Operacji Cybernetycznych. Ponadto minister zaaprobował powstały w NCK *Strategiczny program naukowo-badawczy*. Został on złożony w Narodowym Centrum Badań i Rozwoju. Ma obejmować 33 szczegółowych projektów realizowanych w latach 2015-2025. Program ma także umożliwić stymulowanie polskich środowisk naukowych oraz przemysł obronny do tworzenia nowych, narodowych rozwiązań kryptologicznych i *Cyber Defence*, w tym do adaptacji i spolszczenia technologii zagranicznych używanych w armiach NATO.

W pierwszej połowie 2014 dyrektor NCK/Pełnomocnik MON ds. BC przygotował i doprowadził do zatwierdzenia przez ministra obrony narodowej w maju 2015 *Projektu Założeń do Planu Obrony Cyberprzestrzeni RP* oraz – miesiąc później – *Polityki resortu obrony narodowej w zakresie bezpieczeństwa cyberprzestrzeni*.

Cyber Command

Ponadto Pełnomocnik doprowadził do zatwierdzenia w sierpniu 2014 przez szefa resortu obrony koncepcji powołania Centrum Operacji Cybernetycznych (COC), w oparciu o możliwości istniejących już jednostek. COC miało powstać z połączenia MIL-CERT z CBC. Połączenie pionów – defensywnego z ofensywnym – planowano sfinalizować do końca 2015, jednocześnie zwiększając liczbę etatów. Ponieważ wielkość kadr wojskowych cyberbezpieczeństwa jest dramatycznie niska, przeto planowane dla COC ok.160-200 etatów było czymś niezbędnym w armii liczącej 100 tys. żołnierzy. Dzięki temu COC mogło stać się profesjonalną jednostką działającą na poziomie operacyjnym i taktycznym (poziom strategiczny nowego systemu miało tworzyć NCK, zapewniające jednocześnie wsparcie organizacyjne i logistyczne).

Centrum miało zostać wyposażone w dedykowane uzbrojenie cybernetyczne, zarówno do zapewnienia pełnego cyberbezpieczeństwa, jak i rozwijać zdolności ofensywne. Koncepcja COC zakładała powstanie mobilnych grup bojowych oraz zbudowania podstaw bazowych do tworzenia wojsk cybernetycznych w przyszłości. To polskie *Cyber Command* po osiągnięciu pełnej zdolności bojowej miało zostać podporządkowane Dowódcy Operacyjnemu. Odpowiednia infrastruktura została zaprojektowana na terenie kompleksu NCK w Legionowie. SG zabezpieczył odpowiednie środki finansowe. Wtedy jeszcze minister akceptował nowe podejście do kwestii *krypto* i *cyber*, prezentowane przez ówczesnego dyrektora NCK. Zakładało ono w pierwszej kolejności zapewnienie bezpieczeństwa cyberprzestrzeni w resorcie, a na tej podstawie zbudowanie zdolności do działań w cyberprzestrzeni z elementami

aktywnej cyberobrony.

Październik 2014 – poczatek budowy nowoczesnego ogrodzenia kompleksu Narodowego Centrum Kryptologii. Niestety, rozwój tej instytucji został poważnie zahamowany w ostatnich miesiącach / Zdjecie: Kronika NCK

Kluczowe zdolności do wykonywania zadań operacyjnych ochrony przed zagrożeniami cybernetycznymi miał zapewnić zmodernizowany System Reagowania na Incydenty Komputerowe (SRnIK). Jego zadania i potencjał modyfikowała Decyzja 243 MON z 18 czerwca 2014. Jego trzypoziomowa struktura pozostała niezmieniona. Nadal tworzyły ją: Zespół ds. Obrony Cybernetycznej NCK (czyli centrum koordynacyjne), MIL-CERT (centrum techniczne) oraz administratorzy sieci. System ten został wzmocniony przez żołnierzy z *ofensywnego* CBC. Znaleźli się oni w centrum koordynacyjnym i współpracowali z centrum technicznym. Wspólnie opracowywali koncepcję COC. Określili jego projektowaną strukturę, etat i zadania. W zintegrowaniu zasobów defensywnych i ofensywnych upatrywano nadzieję na zbudowaniu jednolitego zespołu kompetencji cyberbezpieczeństwa i zdolności do działań w cyberprzestrzeni.

W końcu 2014 kształtował się więc zintegrowany militarny system budowy kompetencji cyberbezpieczeństwa w siłach zbrojnych. Podlegał on Pełnomocnikowi MON ds. BC (dyrektorowi NCK) na poziomie strategicznym. Na poziomie operacyjnym połączenie MIL-CERT z CBC miało pozwolić na powstanie Centrum Operacji Cybernetycznych, które wraz z mobilnymi komponentami bojowymi, miało zabezpieczyć poziom taktyczny. COC miało stworzyć swoistą pierwszą linię obrony cyberprzestrzeni Polski. Z kolei zmodernizowany, trzypoziomowy SRnIK miał zapewnić ochronę systemów teleinformatycznych MON.

Pozytywne efekty integracji zaowocowały sukcesami na ćwiczeniach. W organizowanych przez Centrum Doskonalenia Cyberobrony w Tallinie natowskich ćwiczeniach *Locked Shields 2014* ekipa NCK, MIL-CERT i CBC zajęła pierwsze miejsce.

Domniemana wola ministra

Nowe, jednolite podejście spotkało się z krytyką zainteresowanych jednostek i komórek organizacyjnych MON, które odpowiadały dotychczas za cyberbezpieczeństwo. Co więcej, problemem okazał się kompletny chaos pojęciowy w obszarze *cyber* w resorcie. Dodając do tego kupowanie urządzeń i oprogramowania dostępnych na rynku komercyjnym (przy niechęci do rozwijania i kupowania własnych, tańszych rozwiązań), łatwo otrzymać obraz całkowitego braku usystematyzowania działań. Należało ten problem zdefiniować i rozstrzygnąć na poziomie podstawowym.

Projekt Założeń do Planu Obrony Cyberprzestrzeni RP, zatwierdzony przez ministra ON w maju 2014, został wykorzystany jako wkład resortu w pracach nad projektem *Doktryny Cyberbezpieczeństwa RP* podpisanej przez Prezydenta RP 22 stycznia 2015. Stwierdzono tam, że działania w cyberprzestrzeni – ze względu na swój specyficzny charakter i uwarunkowania – nie wpisują się w przyjęte dotychczas kanony wojskowego planowania operacyjnego. Mogą być jednak prowadzone na szczeblu taktycznym, operacyjnym i strategicznym oraz spowodować poważne skutki dla funkcjonowania infrastruktury krytycznej. Przenikają bowiem przez wszystkie zdolności występujące w katalogu zdolności SZ. Dlatego też nie można traktować jednostek do prowadzenia działań w cyberprzestrzeni wyłącznie jako jednego ze środków rażenia dostępnego dla dowódców. Tymczasem obecne procedury planowania operacyjnego są nieadekwatne do działań w cyberprzestrzeni.

Takie konstatacje oznaczały konieczność odejścia przy tworzeniu *Planu Obrony Cyberprzestrzeni*.. od sztywnych reguł planowania przyjętych dla sił konwencjonalnych przez Sztab Generalny. Postulowane niezbędne kierunki zmian są następujące:

- modyfikowanie przepisów prawnych – szczególnie dotyczy to ustaw: prawo telekomunikacyjne, o świadczeniu usług drogą elektroniczną, o stanie wojennym i o powszechnym obowiązku obrony;

- zmiany normatywno-planistyczne – w MON należy pilnie opracować i uzgodnić słownik terminów oraz pojęć dotyczących cyberprzestrzeni, katalogu środków technicznych i uzbrojenia cybernetycznego;

- włączenie do katalogu zdolności militarnych SZ zdolności do obrony cyberprzestrzeni w ramach systemu funkcjonalnego rażenia oraz do działań w cyberprzestrzeni, opracowanie nowej doktryny operacji w cyberprzestrzeni, wraz z instrukcją użycia środków technicznych i uzbrojenia cybernetycznego i wiele innych; ponadto należy zdefiniować i oznaczyć granicę cyberprzestrzeni MON i RP, określić zasoby IT podlegających obronie w ramach obrony cyberprzestrzeni RP, wypracować niezbędną dokumentację w zabezpieczeniu potrzeb logistycznych jednostek cybernetycznych w warunkach kryzysu i wojny; wreszcie należy skorelować *Plan Obrony Cyberprzestrzeni RP* z realizacją innych projektów obronnych w granicach geograficznych państwa, jak i

w cyberprzestrzeni; oczywiście konieczna jest jednolita analiza ryzyka i wiele innych ważnych przedsięwzięć;

- zmiany organizacyjno-funkcjonalne i techniczne – dla osiągnięcia zdolności do działań w cyberprzestrzeni konieczne jest utworzenie Centrum Operacji Cybernetycznych, co pozwoli wyodrębnić grupę zawodową żołnierzy zajmujących się cyberbezpieczeństwem, zorganizować elementy mobilne, zdolne do wsparcia operacji w ramach działań narodowych i sojuszniczych; należy też sklasyfikować kluczowe rozwiązania IT w MON i zwiększyć poziom ich bezpieczeństwa; objąć nadzorem SRnIK całość sieci teleinformatycznej resortu (obecnie jedynie ok. 63%) oraz wdrożyć jednolitą, bezpieczną platformę teleinformatyczną wsparcia dowodzenia i kierowania Siłami Zbrojnymi.

Plan i perspektywa kompleksu NCK w Legionowie / Zdjecie: Kronika NCK

Niestety, wykonanie tych zmian w konserwatywnym, zbiurokratyzowanym MON okazało się niezwykle trudne. W resorcie, gdzie od lat rządzi Sztab Generalny WP, który wszystko ma zaplanowane i... niczego nie potrzebuje, gdzie DIT MON, a obecnie ISI DG RSZ było i jest uparte w błędzie, gdzie SKW, która – podobnie jak DIT – ponosi odpowiedzialność z katastrofę INTER-MON – wszędzie wietrzy spisek odebrania mu znaczenia i władzy... W takiej sytuacji efektywne działanie mogło być możliwe jedynie przy pełnym poparciu i woli ministra obrony narodowej. Ostatecznie jednak okazało się, że była to tylko wola domniemana.

Brak współdziałania ze służbami

Niezrozumienie konieczności pilnej modernizacji myślenia w tym obszarze najlepiej można zaobserwować na przykładzie zadań i kompetencji Sił Zbrojnych oraz wojskowych służb specjalnych. Kwestie te zostały poruszone w piśmie do ministra obrony z 18 grudnia 2014. Podkreślono w nim konieczność współpracy obu podmiotów, jednocześnie wskazując na służebną rolę SKW i SWW wobec armii. Tym bardziej, że

zadania militarne SZ w cyberprzestrzeni różnią się diametralnie od działań służb. Z drugiej strony od 2006 ustawodawca wyłączył wojskowe służby specjalne z Sił Zbrojnych RP i podporządkował je bezpośrednio MON. Jednocześnie uznał za zasadne, zgodnie ze standardami NATO, rozwijanie systemu kompetencji cybernetycznej resortu obrony przez specjalistyczne jednostki wojskowe.

Przemawiają za tym wspomniane już różnice w zadaniach obu formacji. Siły Zbrojne mają np. prowadzić dekryptaż obcych transmisji wojskowych, chronić własne zasoby IT, odtwarzać sprawność i funkcjonalność systemów tworzących cyberprzestrzeń czy aktywnie zwalczać źródła zagrożeń. Muszą także działać w warunkach zagrożenia i wojny, a w czasie pokoju planować wykorzystanie sfery cywilnej na rzecz obronności kraju oraz współpracować z w tych obszarach z sojusznikami.

Natomiast SKW i SWW powinny się koncentrować na przeciwdziałaniu cyberterroryzmowi i cyberszpiegostwu, wykrywać cyberprzestępstwa oraz prowadzić cyberwywiad – dostarczać informacji o kompetencjach i zdolnościach oraz organizacji struktur wojskowych przeciwnika odpowiedzialnych za prowadzenie działań w cyberprzestrzeni, a także identyfikować i wskazywać cele do rażenia cybernetycznego u potencjalnych przeciwników. Oczywiście, podobnie jak dla armii, także służby powinny współdziałać w tej dziedzinie z instytucjami NATO i UE. Jak łatwo się domyślić, także i te postulaty nie zostały spełnione…

Dekompozycja systemu

Po 28 stycznia 2015 nowym dyrektorem NCK został funkcjonariusz SKW, a funkcje Pełnomocnika MON ds. Bezpieczeństwa Cyberprzestrzeni powierzono jednemu z wiceministrów. Wkrótce zaniechano integracji wojskowych zasobów cybernetycznych, pozbawiono NCK funkcji strategicznych i ograbiono z etatów. Wstrzymano też udział żołnierzy NCK w programie naukowo-badawczym *Rotor*, co może doprowadzić do załamania projektu wartego 120 mln zł i strategicznego z punktu bezpieczeństwa narodowego.

Definitywnie oddzielono pion defensywny od ofensywnego. 13 lipca 2015, Decyzją Nr 275 MON, ponownie przeorganizowano SRnIK. Utrzymano pozornie trzypoziomową strukturę funkcjonalną systemu, który formalnie nadal podlega Pełnomocnikowi MON ds. BC. W kontaktach międzynarodowych upoważniono SRnIK do używania określenia MIL-CERT PL.

Zespół specjalistów m.in. z NCK,CBC, MIL-CERT, WAT i CERT, który zajął I miejsce w ćwiczeniach Locked Shields 2014 wraz z Krzysztofem Bondarykiem – wrzesień 2014 / Zdjęcie: Kronika NCK

Cóż z tego, skoro nadzór nad SRnIK w systemach niejawnych MON przejął... Szef SKW. Ponadto jako Centrum Koordynacyjne systemu wyznaczono właściwą komórkę tej służby. Planowane wcześniej przekształcenie RCZBSIUT, NCK i CBC w dwa silne piony – odpowiedzialne za kryptografię NCK i za działania w cyberprzestrzeni COC – zostało zaniechane. CBC ograbiono z wakatów i temu kadłubkowi nadano nazwę COC. Tak zdewastowana jednostka ma zajmować się budowaniem zdolności ofensywnych polskiej armii... Zaś do NCK napłynęli niskokwalifikowani funkcjonariusze SKW. Nastąpiła też reorganizacja, w wyniku której kilku wysokiej klasy specjalistów z CBC i NCK odeszło ze służby.

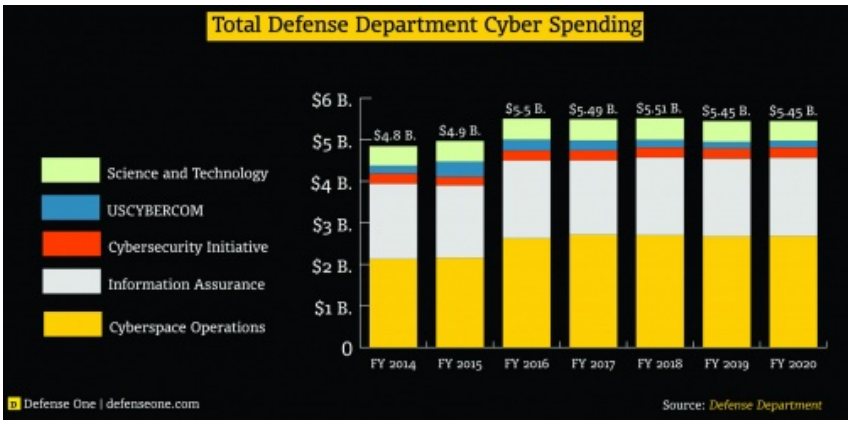
Ponieważ w podpisanym 30 grudnia 2014 przez ministra obrony narodowej *Aneksie do Programu rozwoju SZ na lata 2015-22* nie przewidziano nowych etatów wojskowych w obszarze operacji cybernetycznych, to budowanie przez MON jakiejkolwiek *ofensywy* czy też *cyberwojska* w najbliższym czasie może być wyłącznie czysto teoretyczne.

Obserwowany powrót wojskowych służb specjalnych na pole opuszczone przez WSI nie poprawi zdolności SZ RP w zakresie cyberbezpieczeństwa. Nie zbuduje zdolności do walki w cyberprzestrzeni ani cyberobrony. Przejęcie przez SKW zarządzania nad NCK, dążenie do zarzucenia projektu *Rotor* również ponuro rokuje nad odzyskaniem kompetencji kryptologicznych przez SZ RP.

Upadek pierwszej linii obrony

Jak widać, kierownictwo MON i wyższa kadra dowódcza nie ma świadomości zagrożeń z zakresu cybernetycznych występujących sieciach teleinformacyjnych resortu. Zdolności do działań w cyberprzestrzeni nie traktuje się też jako nieodzownej w przyszłości zdolności operacyjnej Sił Zbrojnych RP. Mimo że minister obrony i kierownictwo resortu było wielokrotnie informowane o zagrożeniach oraz skutkach braku działań naprawczych.

Przeciwnie, w 2015 wojsko zostało de facto pozbawione pierwszej linii obrony cybernetycznej w postaci sprawnego SRnIK. Zarzucono też plan sformowania w br. silnego Centrum Operacji Cybernetycznych, odpowiedzialnego za pełne cyberbezpieczeństwo. MON i SG zaaprobowały model *rozproszonej nieodpowiedzialności* za cyfrowe bezpieczeństwo sieci i systemów teleinformatycznych resortu.



Planowane jawne wydatki na amerykańskie działania w cyberprzestrzeni, w latach 2014-2020. Pentagon przeznacza na ten cel ok. 5 mld USD. Zwiększenie budżetu służby w 2016 o ponad 500 mln USD w większości pochłonie zatrudnienie dodatkowych 3 tys. cywilnych informatyków / Grafika: DO USA

W przestrzeni informatycznej trwa już bowiem niemal jawna wojna, toczona głównie między Waszyngtonem a Pekinem. Władze ChRL zapowiedziały, że do 2020 stworzą warunki do wygrania cybernetycznego starcia przez siły zbrojne Państwa Środka, co ma się też wiązać z ucyfrowieniem wojska, a szczególnie systemu dowodzenia. Jak wypada na tym tle Polska po latach kierowania MON przez Tomasza Siemoniaka, trudno nawet komentować... / Zdjęcie: NYT

Zupełnie niezrozumiałe jest przekazanie władztwa nad tym sektorem służbom specjalnym. Wszak mają one zupełnie inne zadania niż Siły Zbrojne. Wygląda to nie tylko na indolencję, ale na ucieczkę od odpowiedzialności, co będzie skutkowało kolejnym marnotrawstwem czasu i pieniędzy. Ufność, jaką kierownictwo MON pokłada w kompetencji SKW, przeczą fakty. Służba nie tylko nie potrafiła zapobiec ujawnionemu w 2013 wieloletniemu okradaniu użytkowników poczty INTER-MON, ale nie umie przerwać tego procederu obecnie. Z opublikowanych danych fińskiej spółki FSecure wynika, że atak na jawną sieć polskiego resortu obrony trwa nadal...

Krzysztof BONDARYK

Autor, gen. bryg. rez. Krzysztof Bondaryk w latach 1998-1999 był Podsekretarzem Stanu w MSWiA. W latach 2007-2013 pełnił funkcję Szefa Agencji Bezpieczeństwa Wewnętrznego, gdzie za jego kadencji m.in zbudowano Centrum Antyterrorystyczne (CAT) oraz CERT.gov.pl. Odtworzono też cywilny Radiokontrwywiad i zbudowano rządowy system niejawnej łączności mobilnej CATEL oraz odbudowano zdolności kryptologiczne ABW. Od 2 marca 2013 pracował w MON. Początkowo jako Radca Ministra, a 9 kwietnia 2013 został Pełnomocnikiem ds. utworzenia Narodowego Centrum Kryptologii. Był dyrektorem NCK od sierpnia 2013 do stycznia 2015. Jednocześnie – od października 2013 – był Pełnomocnikiem MON ds. Bezpieczeństwa Cyberprzestrzeni. Odszedł z MON na własną prośbę...
