ZAGROŻENIA CYBERNETYCZNE. BROŃ KATEGORII „D”

autor:
płk rez. **Marek Napierała**

➡ Przygotowanie do wojny w cyberprzestrzeni jest równie ważne jak przygotowanie do wojny konwencjonalnej.

➡ Niektóre państwa już teraz intensywnie inwestują w zdolności cybernetycznej obrony i rażenia. Przodują w tym Amerykanie, Rosjanie, Chińczycy i Brytyjczycy. Jest to stosunkowo tania broń, dająca ogromną przewagę w początkowej fazie konfliktu oraz w trakcie jego trwania, dzięki swojej nieprzewidywalności i asymetryczności oraz trudności wykrycia źródła ataku.

➡ Na szczycie NATO w 2016 roku w Warszawie sojusz uznał cyberprzestrzeń za obszar działań militarnych, na równi z działaniami lądowymi, powietrznymii morskimi.

Autor: **płk. rez. Marek Napierała**, ekspert fundacji Stratpoits, absolwent studiów podyplomowych „Sieci komputerowe i aplikacje internetowe” na Politechnice Poznańskiej.

Tytuł: **Zagrożenia cybernetyczne. Broń kategorii „D”**

System obrony państwa składa się z wielu elementów militarnych i niemilitarnych połączonych w jeden organizm. Tylko synergia tych sektorów może przynieść pozytywne efekty. W okresie transformacji nastąpiło wiele zmian, które wpłynęły na poziom obronności państwa. Między innymi zawieszono odbywanie zasadniczej służby wojskowej oraz osłabiono zdolności mobilizacyjne. Aktualnie wielu młodych i sprawnych ludzi nie posiada żadnego przeszkolenia wojskowego jak również przydziału mobilizacyjnego na wypadek wystąpienia zagrożenia zewnętrznego. Niektóre z tych elementów zastępuje się innymi, czego przykładem jest próba implementacji Wojsk Obrony Terytorialnej do systemu obrony.

Permanentnie trwają zmiany strukturalne oraz modernizacyjne, spowodowane dynamiką sytuacji geopolitycznej, rozwojem technologicznym, uczestnictwem w Organizacji Traktatu Północnoatlantyckiego, a także udziałem w misjach w Iraku, Afganistanie i na Bałkanach.

Główny wysiłek modernizacji naszej armii skoncentrowany jest na budowaniu konwencjonalnego potencjału obronnego. Staramy się pozyskiwać sprzęt i rozwiązania, by w ramach członkostwa w NATO, zrównoważyć potencjał militarny przeciwnika. Nie doceniamy jednak zagrożeń wynikających z możliwości zastosowania działań niekonwencjonalnych. Można odnieść wrażenie, że stosunkowo marginalnie traktowany jest obszar zagrożeń cybernetycznych. Nie ma dzisiaj dziedziny życia, która nie byłaby bezpośrednio lub pośrednio uzależniona od informatyki. Dotyczy to również wojska, które wykorzystuje nowoczesne systemy kierowania, wspomagania dowodzenia, rozpoznania, w okresie pokoju i wojny.

Nie ulega wątpliwości, że wojna informacyjna w cyberprzestrzeni trwa. Trwa również wyścig zbrojeń w tym obszarze. Wszyscy, korzystający z współczesnych rozwiązań technologicznych, uczestniczymy w niej. Doświadczamy tego w serwisach informacyjnych i na portalach społecznościowych. Klasycznym przykładem jest sytuacja z 2016 roku, kiedy ówczesny minister Obrony Narodowej, Antoni Macierewicz publicznie ogłosił, że Egipcjanie sprzedali Rosjanom francuskie okręty Mistrale. Te sensacyjne doniesienia pochodziły z rosyjskiego portalu, powiązanego z tamtejszym resortem obrony i były elementem gry operacyjno-informacyjnej, mającej na celu eskalowanie napięć wewnętrznych i na arenie międzynarodowej. Zostały mu one dostarczone przez analityków Służby Wywiadu Wojskowego, bez żadnej weryfikacji. Innym przykładem jest publikowanie informacji na portalach informacyjnych i społecznościowych o rzekomych wypowiedziach wysokich

rangą dowódców, krytykujących poczynania ministra ON. Przoduje w tym Niezależny Dziennik Polityczny, którego powiązania z rosyjskimi służbami specjalnymi prześledziła redakcja OKO Press[1].

Cyberwojna to zjawisko, które pojawiło się w następstwie powszechnego dostępu do informacji oraz technologii informatycznych. Powszechność zastosowania mediów elektronicznych i korzystania z zasobów internetowych dotyczy również wojska. Współczesna armia nie opiera się wyłącznie na zasobach ludzkich i konwencjonalnych środkach walki. Wojsko sięga po nowe, zaawansowane technologicznie środki walki, zinformatyzowane środki dowodzenia i łączności, inteligentne systemy rozpoznania i kierowania działaniami.[2]

Do języka wojskowego wchodzi pojęcie nowego rodzaju broni, która umownie została oznaczona literą „D”[3]. Mianem tym określa się urządzenia, oprogramowanie, oraz działania zmierzające do wykrycia i odparcia lub przeprowadzenia ataku na wybrane cele za pośrednictwem sieci. W wyniku tego działania możliwe jest udaremnienie lub przejęcie kontroli nad kluczowymi elementami infrastruktury krytycznej: energetyką, transportem naziemnym, morskim i powietrznym, telekomunikacją, zakładami produkcyjnymi, czy wreszcie nad instytucjami odpowiedzialnymi za obronę.

Wiele państw intensywnie inwestuje w zdolności cybernetycznej obrony i rażenia, przodują w tym: Amerykanie, Rosjanie, Chińczycy i Brytyjczycy. Jest to stosunkowo tania broń, dająca ogromną przewagę w początkowej fazie konfliktu i w czasie jego trwania, dzięki swojej nieprzewidywalności i asymetryczności oraz trudności wykrycia źródła ataku.

Zakłada się, że działania w cyberprzestrzeni obejmować będą cztery etapy:

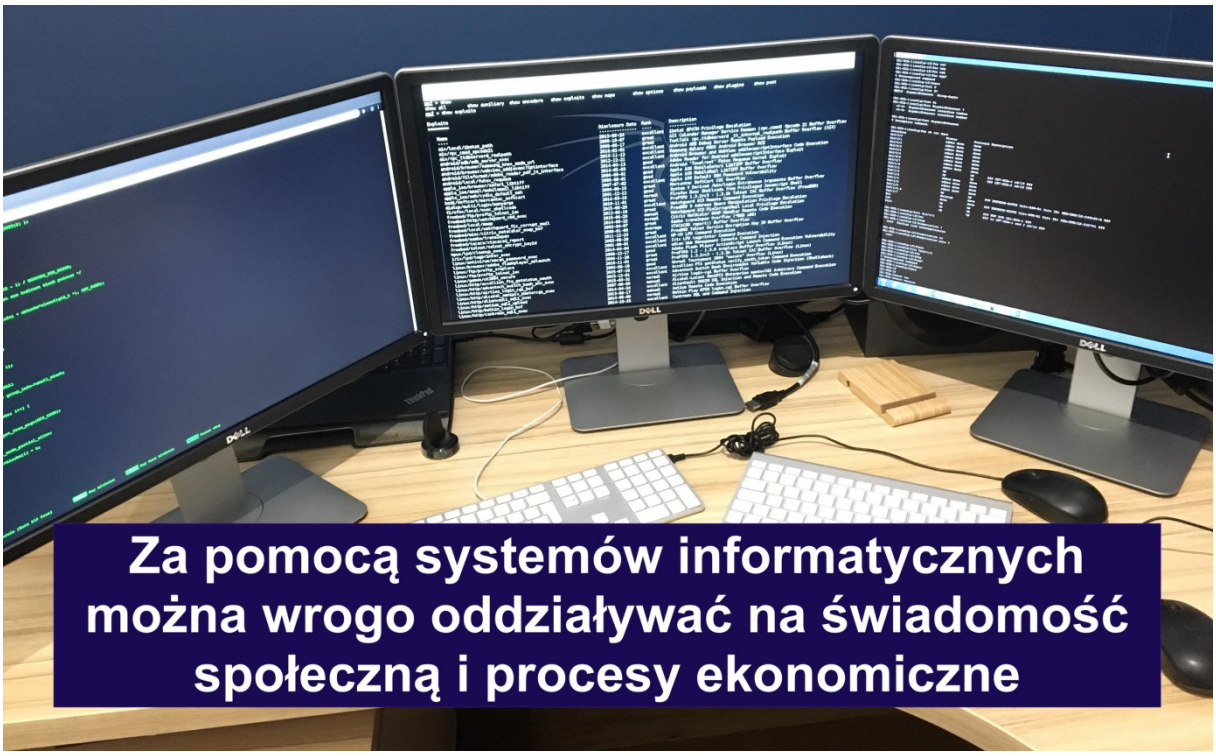
1. Gromadzenie i archiwizowanie danych o przeciwniku, dających podstawy do analiz i ocen zdolności bojowych.
2. Badanie oprogramowania pod kątem odporności na atak oraz ocena skuteczności stosowanych metod.
3. Implementacja narzędzi umożliwiających atak.
4. Przejęcie kontroli nad systemem lub jego unieruchomienie.

[1] P. Szczepaniak, K. Szczygieł, https://oko.press/polskie-fejki-rosyjska-dezinformacja/.

[2] Andrzej Urbanek, *Cyberwojna – zagrożenie asymetryczne współczesnej przestrzeni bezpieczeństwa*, 2016 s. 1.

[3] Od słowa Digital (cyfrowa).

Warto zauważyć, że pierwsze dwa etapy, są realizowane na bieżąco, dużo wcześniej niż oficjalne rozpoczęcie konfliktu. Odnotowano wiele przypadków ataków na instytucje państwowe, systemy wojskowe NATO, które prawdopodobnie są próbami sprawdzania odporności struktury. Najpoważniejszy, jak dotąd, atak został przeprowadzony w 2008 roku na amerykański wojskowy system komputerowy. Poprzez prosty pendrive dołączony do komputera będącego własnością wojska w bazie wojskowej na Bliskim Wschodzie oprogramowanie szpiegowskie rozprzestrzeniło się niepostrzeżenie zarówno do tajnych, jak i do jawnych systemów. W ten sposób powstał „informatyczny przyczółek" z którego ściągnięto tysiące plików danych do serwerów będących pod zagraniczną kontrolą[4].



Fot. Łukasz Napierała

Podstawą podejmowania trafnych decyzji jest **informacja**, rozumiana jako narzędzie rozpoznania, ale także manipulacji oraz **umiejętność dokonywania analizy i wyciągania wniosków**. Zasada ta dotyczy również armii, jej dowódców na każdym poziomie. Informacja musi być wiarygodna i dostarczona na czas. Dowódca nawet najmniejszego pododdziału, by zrealizować zadanie musi otrzymać niezbędne dane, przeprowadzić analizę oraz podjąć decyzję co do sposobu realizacji zadania. Nowoczesne systemy w znacznym zakresie

[4] https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/PL/index.htm

wyręczają żołnierzy z prowadzenia skomplikowanych obliczeń, niemniej decyzja co do zastosowania rodzaju środków i sposobu ich użycia należy do dowódcy.

Od czasu, kiedy człowiek prowadzi zorganizowane działania siłowe przeciwko drugiemu, wykorzystywana jest informacja i dezinformacja. Na przełomie dziejów udoskonalono jedynie sposoby jej pozyskiwania i dystrybuowania. Historia konfliktów jest pełna przykładów, kiedy wojska ponosiły klęskę, nie z powodu słabszego potencjału, lecz dlatego że dowódcy nie dysponowali aktualnymi informacjami o przeciwniku, lub dysponowali informacjami błędnymi, przygotowanymi przez przeciwnika.

W dobie błyskawicznego przekazu informacyjnego, dziedzina pozyskiwania i dystrybucji informacji, nabiera szczególnego znaczenia i jest kluczowa do prowadzenia działań militarnych. Współczesne systemy pozyskiwania oraz przetwarzania informacji oparte są na rozwiązaniach teleinformatycznych umiejscowionych w warstwie fizycznej i aplikacji. Zniszczenie infrastruktury lub zainfekowanie oprogramowania może dać przewagę jednej ze stron konfliktu.

Nie ulega wątpliwości, że współczesny konflikt zbrojny poprzedzony będzie intensywnymi działaniami w cyberprzestrzeni, co najmniej w kilku obszarach. Pierwszy z nich to przeprowadzenie na szeroką skalę, na terenie przeciwnika, kampanii dezinformacyjnej, mającej na celu wywołanie oczekiwanych reakcji społecznych np. negatywnego odbioru działań władz państwowych w zakresie sojuszu lub polityki zagranicznej. W tym celu, strony konfliktu, będą dążyły do przejęcie ośrodków informacyjnych. W przeszłości działania te polegały na fizycznym opanowaniu obiektów i przejęciu rozgłośni radiowych, węzłów i szlaków komunikacyjnych oraz placówek pocztowych. Współcześnie da się to czynić na odległość. Tam, gdzie nie uda się zdalnie przejąć infrastruktury przesyłowej, systemów przetwarzania i przechowywania danych, można będzie dokonać fizycznego ich zniszczenia. Społeczeństwo poddane propagandowemu oddziaływaniu, tracące poczucie bezpieczeństwa, będzie bardziej podatne na manipulację, skłonne do negatywnych i nieprzewidywalnych reakcji.

Drugi obszar to cybernetyczny atak na infrastrukturę krytyczną, w celu osłabienia potencjału obronnego, wywołania paniki, poczucia lęku oraz dezorganizacji życia społecznego. Za pomocą zainfekowanego oprogramowania, lub po przejęciu infrastruktury informatycznej będzie można sparaliżować całkowicie życie gospodarcze. Zdalne powodowanie zniszczeń na terenie przeciwnika, bez strat własnych, a często bez ujawniania

własnej tożsamości, jest bez wątpienia marzeniem każdego dowódcy. Dzięki powszechnemu dostępowi do sieci komputerowych i coraz dalej idącej informatyzacji i automatyzacji procesów przemysłowych te marzenia stają się rzeczywistością.

Łatwo sobie wyobrazić jakie skutki dla funkcjonowania państwa może wywołać zakłócenie dostawy energii elektrycznej, gazu, paliw ciekłych. Współcześnie wszystkie dziedziny życia uzależnione są od energii zewnętrznej i systemów teleinformatycznych. Jak może wyglądać sytuacja po ataku cybernetycznym na infrastrukturę krytyczną pokazała sytuacja w Wenezueli w marcu 2019. Według informacji płynących z tego kraju doszło do awarii elektrowni w wyniku ataku cybernetycznego. Przerwy w dostawach prądu, sparaliżowały kraj, uniemożliwiły m.in. pracę szpitali.

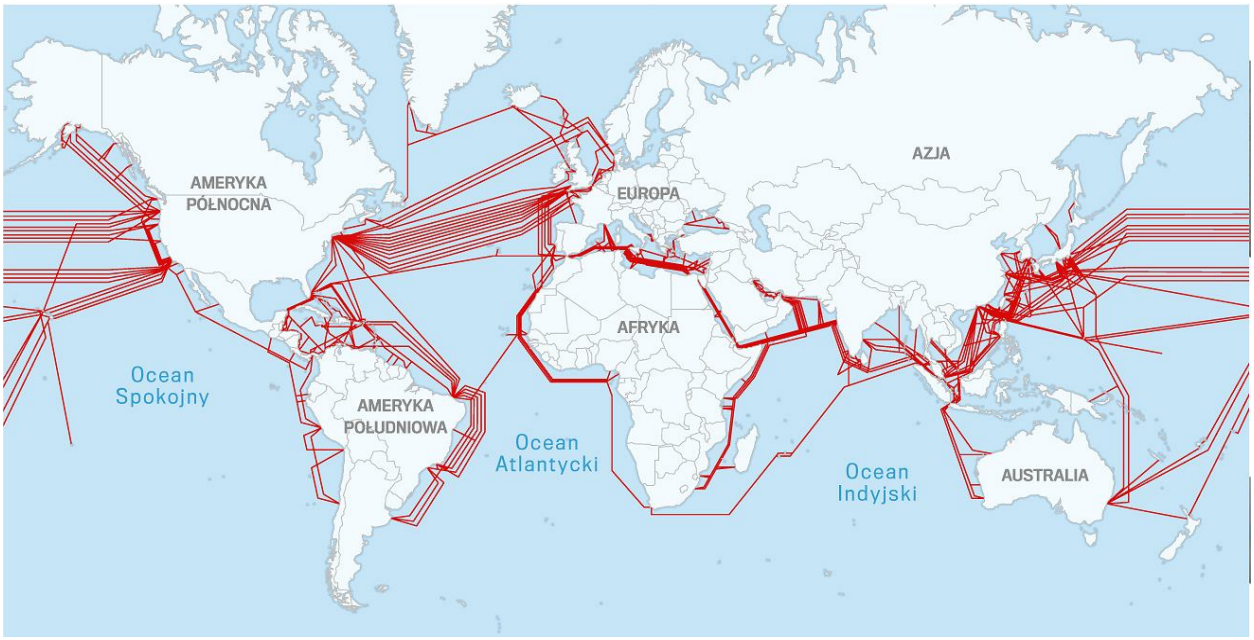
Należy założyć, że bezpośrednio przed działaniami militarnymi i w trakcie ich trwania przeprowadzane zostaną ataki cybernetyczne na strukturę wojskową. Łatwo będzie można pokonać najlepiej uzbrojoną i wyszkoloną armię, która nie otrzyma na czas istotnych danych do planowania obrony, informacji o przeciwniku lub pozyska informacje nieprawdziwe, niezweryfikowane, celowo rozpowszechniane przez przeciwnika.

Niezależnie od samej informacji niezmiernie istotna jest infrastruktura, przeznaczona do transportu informacji, przechowywania czy dystrybucji. Zachowanie jej, w stanie nienaruszonym, w okresie działań wojennych, ma kluczowe znaczenie dla powodzenia operacji wojskowych.

W przypadku wojny globalnej pewne jest oddziaływanie na infrastrukturę krajową, ale bardzo prawdopodobne wydaje się również oddziaływanie na infrastrukturę rozproszoną. Niewątpliwie, w dobie swobodnego dostępu do informacji, przepływu danych finansowych, atak na infrastrukturę fizyczną sieci internetowej spowodowałby chaos globalny.

Według danych opublikowanych w "New York Times" odnotowano dużą aktywność rosyjskiej floty w rejonach oceanów, przez które biegną transatlantyckie światłowody stanowiące system międzykontynentalnej łączności przewodowej. Kablami tymi przepływa cała światowa łączność i bez których Internet, czy gospodarka w obecnej formule, nie mogłyby istnieć. Można się jedynie domyślać, że Rosjanie weryfikują możliwość ataku

paraliżującego Europę i Amerykę. Swoje doniesienia dziennik opiera na rozmowach z anonimowym przedstawicielem armii amerykańskiej.[5]



Źródło: http://wyborcza.pl/1,145452,19196816,wojna-informacyjna-czy-wojny-o-kable-sparalizuja-swiat.html

Fizyczne zniszczenie wszystkich kabli teleinformatycznych, łączących Europę z Ameryką Północną jest możliwe, ale trudne ze względu na ich ilość i rozproszenie. Bardziej prawdopodobny wydaje się precyzyjny atak na kluczowe łącza, który spowoduje ogromny spadek przepustowości, a w konsekwencji obserwowalny brak dostępu do sieci, dla dużej części użytkowników Internetu. Automatycznie może ucierpieć system wymiany informacji sojuszniczych.

Skutki fizycznego uszkodzenia łącz informatycznych obserwowane były m.in. w Pakistanie. Doszło tam do uszkodzenia dwóch z czterech kabli łączących kraj z siecią globalną, co doprowadziło do problemów z dostępem do Internetu dla 70% użytkowników.

Kolejnym istotnym problemem dla wojska jest wykorzystywanie sygnału GPS w działaniach militarnych. Nie ulega wątpliwości, że w okresie konfliktu podejmowane będą próby oddziaływania na sygnał nawigacyjny poprzez jego zakłócenie lub zlikwidowanie źródła emisji.

[5] M. Kucharczyk, https://www.tvn24.pl/magazyn-tvn24/kable-bez-ktorych-stanie-swiat,12,237

Obecnie Rosjanie, o czym niedawno informowali Norwedzy, dokonują ataków typu spoofing[6] na system GPS. Tak zainfekowany sygnał powoduje błędne odczyty. Jest to prawdopodobnie próba testowania możliwości oddziaływania na urządzenia w zastosowaniu niemilitarnym, ponieważ wojsko wykorzystuje technologię szyfrowanego sygnału oraz pracuje na innych częstotliwościach. Najbardziej prawdopodobnym scenariuszem, w razie konfliktu zbrojnego, są ataki typu jamming[7] dla sygnału GPS, polegające na jego zakłóceniu, czyli praktycznym jego wyłączeniu na danym obszarze. W ten sposób można bezpośrednio oddziaływać na strukturę militarną, korzystającą z sygnału GPS i powodować ogromne zniszczenia. Sprawa jest o tyle istotna, że Rosja oraz Chiny dysponują własnymi systemami nawigacji satelitarnej GLONASS oraz BEIDOU.

Problem zagrożeń cybernetycznych w Polsce dostrzeżony został kilka lat wcześniej, niemniej do tej pory w tym względzie niewiele zrobiono. Powstało Narodowe Centrum Kryptologii oraz komórka ds. zagrożeń cybernetycznych w ramach Służby Kontrwywiadu Wojskowego. Priorytetowym zadaniem pierwszej instytucji było stworzenie narodowego systemu kryptologicznego, natomiast drugiej, ustalanie i neutralizacja zdarzeń i incydentów cybernetycznych w jednostkach i instytucjach podległych MON. To zdecydowanie za mało.

Od 2008 roku w ówczesnym Ministerstwie Spraw Wewnętrznych i Administracji oraz m.in. w ABW prowadzone były czynności mające na celu przygotowanie kompleksowej, narodowej strategii przeciwdziałania zagrożeniom występującym w cyberprzestrzeni. W toku prac powstało siedem projektów strategii. Żaden z wymienionych dokumentów nie został zatwierdzony przez Radę Ministrów i przyjęty do realizacji, co wynikało przede wszystkim z ich niskiej jakości oraz nierzetelnego przygotowania. W efekcie stworzono projekt dokumentu „Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej”. Dokument ten został przyjęty, a koordynację realizacji jego postanowień powierzono ministrowi właściwemu ds. informatyzacji.

Na szczycie NATO w 2016 roku w Warszawie sojusz uznał cyberprzestrzeń za obszar działań militarnych, na równi z lądem, przestrzenią powietrzną oraz wodami. W 2017 roku polski rząd przyjął pierwszą strategię cyberbezpieczeństwa pod nazwą „Krajowe ramy

[6] Grupa ataków na systemy teleinformatyczne polegająca na podszywaniu się pod inny element systemu informatycznego. Efekt ten osiągany jest poprzez umieszczanie w sieci preparowanych pakietów danych lub niepoprawne używanie protokołów.

[7] Atak powoduje, że w zasięgu urządzenia będącego źródłem zakłóceń tworzy się „bańka”, w której obrębie żaden odbiornik nie będzie działać poprawnie.

polityki bezpieczeństwa cybernetycznego Rzeczypospolitej Polskiej na lata 2017-2022". Jest ona kontynuacją działań podejmowanych w przeszłości przez administrację rządową oraz dokumentem koncepcyjnym i wykonawczym w stosunku do „Doktryny cyberbezpieczeństwa RP"[8], opublikowanej przez Biuro Bezpieczeństwa Narodowego w 2015 roku. W sierpniu 2018 roku weszła w życie ustawa o krajowym systemie cyberbezpieczeństwa. Nakłada ona na Ministra Obrony Narodowej zadania związane m.in. z potrzebą zapewnienia zdolności Sił Zbrojnych RP do prowadzenia działań militarnych w cyberprzestrzeni[9].

Wreszcie w lutym bieżącego roku podjęto decyzję o powołaniu Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni na bazie Narodowego Centrum Kryptologii i Inspektoratu Informatyki. Powołano również pełnomocnika MON ds. utworzenia wojsk obrony cyberprzestrzeni, który obejmie funkcję dyrektora Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni. Na bazie Centrum Operacji Cybernetycznych sformowane zostaną Siły Obrony Cyberprzestrzeni, które docelowo zostaną przekształcone w wojska obrony cyberprzestrzeni.

Niestety na początku drogi do tworzenia systemu obrony w cyberprzestrzeni odnotowano wpadki. W 2012 roku został ogłoszony przetarg na stworzenie programu do prowadzenia działań cybernetycznych. Informacja o ogłoszeniu konkursu na stworzenie polskiej cyberbroni pojawiła się na stronach Narodowego Centrum Badań i Rozwoju, która nadzoruje projekt, powstający na zlecenie Ministerstwa Obrony Narodowej. Można było się z niego dowiedzieć, że „Projekt 29" to wirus, pozwalający przejmowanie kontroli nad urządzeniami sieciowymi i mobilnymi. Ma służyć celowej dezaktywacji niektórych urządzeń, prowadzeniu nasłuchu, wykradaniu danych. Powstający wirus miał być na tyle skomplikowanym narzędziem, że Wojsko Polskie nie było w stanie stworzyć go za pomocą własnych środków. O tym, że wiele państw posiada swoje botnety i wirusy wiadomo od dawna, jednak informacje do opinii publicznej nigdy nie były przekazywane przez organa państwa[10].

Jak wskazuje powyższy przykład jednym z ważniejszych problemów jest pozyskiwanie sprzętu i oprogramowania oraz kadr do realizacji tego zadania. Ważne, jakie środki MON

[8] http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf

[9] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz.U. 2018 poz. 1560.

[10] https://tech.wp.pl/polska-armia-i-projekt-29-pracuja-nad-wojskowym-wirusem-6034830853476993a

przeznaczy na zakup wyposażenia i czy będą one wystarczające do realizacji celów, czy będziemy w stanie zakupić urządzenia i oprogramowanie zaawansowane technologicznie. Równie istotną kwestią jest pozyskiwanie kadry z odpowiednim wykształceniem i doświadczeniem. Trzeba mieć świadomość, że wyszkolony i doświadczony informatyk, znający rzemiosło, zarabia w Polsce średnio kilkanaście tysięcy złotych, a więc tyle co generał w wojsku. Z problemami kadrowymi w dziedzinie informatycznej borykają się wszystkie armie, w tym USA. Firmy cywilne chętnie zatrudniają informatyków i specjalistów od telekomunikacji ze szlifami oficerskimi. Są nawet skłonne ponieść zwrot kosztów nauki swojego przyszłego pracownika. Dlatego niezbędnym wydaje się stworzenie systemu motywacyjnego.

Utworzenie struktur wojsk cybernetycznych w Polsce jest koncepcją trafną, choć już bardzo spóźnioną. W stosunku do innych państw, w tym członków NATO, pozostajemy daleko w tyle. Rosja dawno korzysta z tej formuły. Przykładem jest choćby konflikt rosyjsko-ukraiński, gdzie Rosjanie przed i w trakcie działań militarnych przeprowadzili kampanię dezinformacyjną. Przez dłuższy czas świat nie był w stanie stwierdzić kim naprawdę są tzw. "zielone ludziki".

Nie ma rozwiązań, które w pełni uchronią kraj, czy sojusz przed atakami cybernetycznymi, co nie oznacza, że nie należy z tym nic robić. Zasadnym jest tworzenie oraz implementacja systemów narodowych, hybrydowych, kompatybilnych oraz łączenie ich w ramach sojuszu. Oczywistym jest, że potrzebne są na badania ogromne środki finansowe, przy założeniu, że mamy potencjał ludzki. Tą drogą podążają Amerykanie. W 2003 roku uruchomili projekt własnej sieci światłowodowej łączącej dowództwa na świecie. DARPA[11] (Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności) pracuje nad stworzeniem bezprzewodowej technologii transmisji danych, której przepustowość dorównywałaby łączom światłowodowym. Takie rozwiązania będą w perspektywie alternatywą dla istniejących i powszechnie dostępnych systemów, a tym samym będą bardziej odporne na ingerencję.

Nie ma odwrotu od implementacji najnowocześniejszych technologii teleinformatycznych w wojsku. Sprzęt, uzbrojenie i wyposażenie musi nadążać za rozwiązaniami innowacyjnymi, w przeciwnym razie nie spełni kryterium skuteczności.

[11] Defense Advanced Research Projects Agency DARPA (Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności) amerykańska agencja rządowa zajmująca się rozwojem technologii wojskowej działająca w strukturach Departamentu Obrony.

Trudno sobie wyobrazić niszczenie rakiet, czy statków powietrznych przeciwnika bez nowoczesnych technologii wykrywania i naprowadzania lub prowadzenie rozpoznania bez udziału drona. Standardem jest, w przypadku pojawienia się nowych rozwiązań technologicznych, poszukiwanie takich, które będą przeciwwagą. W chwili, kiedy wyprodukowano środki bojowe zdolne przenosić konwencjonalne i niekonwencjonalne ładunki wybuchowe na znaczne odległości, natychmiast wdrożono prace nad stworzenie systemu ochrony przed rakietami.

Trzeba mieć świadomość, że każda ze stron konfliktu będzie korzystała z nowinek technologicznych, pozostaje natomiast problem uodpornienia się na ataki niekonwencjonalne poprzez stosowanie rozwiązań dedykowanych lub alternatywnych.

W dobie powszechnego dostępu do informacji, bezprzewodowej komunikacji, uzależnienia od współczesnych źródeł energii, zasadnym jest podejmowanie działań świadomościowych wobec ludności cywilnej na wypadek ich braku. Niezbędne wydaje się również prowadzenie szkoleń, na każdym poziomie rozwoju, w zakresie umiejętności radzenia sobie w sytuacjach trudnych.

Do przeciwstawienia się agresji zewnętrznej potrzebna jest korelacja działań konwencjonalnych i tych z obszaru zagrożeń cybernetycznych. Państwo pozbawione dostaw energii, sparaliżowane komunikacyjnie straci potencjał obronny i zostanie zaanektowane przez przeciwnika.

O kierunkach rozwoju i modernizacji Sił Zbrojnych RP powinni decydować politycy na podstawie potrzeb sygnalizowanych przez dowódców, opartych o analizy zagrożeń zewnętrznych i wewnętrznych. Często jednak dzieje się tak, że te decyzje uwarunkowane są względami politycznych, a nawet populistycznymi i nie koniecznie odpowiadają realnym potrzebom wojska.

| PUBLIKACJE

www.stratpoints.eu