Krzysztof Liedel
Paulina Piasecka

Cyberbezpieczeństwo
Piąte pole walki
Diagnoza i rekomendacje

INSTYTUT BRONISŁAWA KOMOROWSKIEGO

Konrad Adenauer Stiftung

Krzysztof Liedel / Paulina Piasecka

Cyberbezpieczeństwo. Piate pole walki

Diagnoza i rekomendacje

Bezpieczeństwo państwa w dobie zagrożeń

Dynamika zmian z środowisku bezpieczeństwa wzrasta w ostatnich latach w zauważalny sposób. Wśród najważniejszych przyczyn takiego stanu rzeczy wymienić należy - poza wyczerpującą się premią bezpieczeństwa wynikającą z zakończenia przed ćwierćwieczem zimnej wojny - także pojawienie się nowych strategii i taktyk działania w przestrzeni międzynarodowej stosowanych przez aktywnych aktorów państwowych i niepaństwowych.

Innym czynnikiem, który wpływa na zmianę percepcji bezpieczeństwa oraz konieczność stworzenia nowych mechanizmów zabezpieczania państwa, jego interesów i obywateli, jest pojawianie się nowych cech bezpieczeństwa, warunkujących zmianę jego paradygmatu[1]. Wśród tych cech wymienić należy informacyjność, sieciowość, asymetryczność oraz integracyjność.

Informacyjność bezpieczeństwa, będąca następstwem rewolucji informacyjnej, zmienia paradygmat procesu bezpieczeństwa wyznaczany przez relacje między dwoma pierwotnymi i najbardziej elementarnymi czynnikami wszelkiej ludzkiej działalności, energetycznym i niematerialnym – informacyjnym. Asymetryczność bezpieczeństwa jest powodowana głównie rewolucją polityczną, za jaką można uznać rozpad świata dwubiegunowego oraz coraz silniejszym zaznaczaniem w stosunkach międzynarodowych działania aktorów pozapaństwowych, w tym zwłaszcza międzynarodowych sieci terrorystycznych. Usieciowienie bezpieczeństwa wynika przede wszystkim z jednoczesnego występowania dwóch zjawisk, jakimi są rewolucja informacyjna i globalizacja. Zwieńczeniem nowych cech bezpieczeństwa jest jego integracyjność, tj. łączenie wysiłków militarnych (obronnych) i niemilitarnych (ochronnych, wsparcia) w ramach procesu bezpieczeństwa.

Z pojęciem integracyjności bezpieczeństwa bezpośrednio wiąże się pojęcie transsektorowości bezpieczeństwa, które zaistniało w Strategicznym Przeglądzie Bezpieczeństwa Narodowego, zrealizowanym przez Biuro Bezpieczeństwa Narodowego na polecenie Prezydenta RP, Bronisława Komorowskiego. Zgodnie ze sformułowaną w procesie Przeglądu definicją **transsektorowe (transpodmiotowe) obszary bezpieczeństwa narodowego** (bezpieczeństwa państwa) to „części zintegrowanego

[1] Koziej S. "Nowa jakość bezpieczeństwa na progu XXI wieku", źródło: https://www.bbn.gov.pl/pl/wydarzenia/2562,quotNowa-jakosc-bezpieczenstwa-na-progu-XXI-wiekuquot-wystapienie-Szefa-BBN-w-AO.html

bezpieczeństwa narodowego obejmujące swą treścią problematykę właściwą jednocześnie różnym podmiotom, dziedzinom i sektorom tego bezpieczeństwa (np. bezpieczeństwo zewnętrzne lub wewnętrzne, albo kwestie związane z współczesnymi procesami transnarodowymi i asymetrycznymi zjawiskami i procesami bezpieczeństwa, jak np. bezpieczeństwo informacyjne, **w tym cyberbezpieczeństwo**, bezpieczeństwo antyterrorystyczne, przeciwdziałanie proliferacji broni masowego rażenia, zwalczanie przestępczości zorganizowanej). Są one często wyodrębniane z uwagi na jakościowo nowe i pilne w danym okresie potrzeby praktyczne, nie mające wyraźnego adresata w istniejącej strukturze wykonawczej podmiotu)."

W takich warunkach bezpieczeństwa, mając świadomość jego zmieniającego się paradygmatu, działali ministrowie obrony państwo członkowskich NATO, podejmując podczas Szczytu NATO w Warszawie w 2016 r. decyzję o uznaniu cyberprzestrzeni za piątą (poza lądem, morzem, powietrzem i przestrzenią kosmiczną) płaszczyznę walki. Jak stanowi „Komunikat ze szczytu NATO w Warszawie wydany przez Szefów Państw i Rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Warszawie w dniach 8 i 9 lipca 2016 r.":

- cyberataki stanowią oczywiste wyzwanie dla bezpieczeństwa Sojuszu i mogą być równie szkodliwe dla współczesnych społeczeństw, co konwencjonalny atak,
- cyberobrona jest częścią podstawowych zadań obrony zbiorowej NATO,
- NATO posiada mandat do obrony w cyberprzestrzeni uznanej za obszar działań, w którym NATO musi bronić się tak samo skutecznie jak w powietrzu, na lądzie i na morzu.

Ta konstatacja wpływa na sposób postrzegania zagrożeń w cyberprzestrzeni i warunkuje potrzebę pogłębionej refleksji odnośnie granic bezpieczeństwa państwa i działań niezbędnych dla ich zabezpieczenia.

Bezpieczeństwo informacyjne jako kategoria nadrzędna

Kategoria cyberbezpieczeństwa powinna być rozpatrywana w relacji do całości obszaru bezpieczeństwa państwa. Szczególnie istotnym pojęciem w kontekście umiejscowienia cyberbezpieczeństwa na mapie bezpieczeństwa państwa jest pojęcie bezpieczeństwa informacyjnego.

Bezpieczeństwo informacyjne państwa, a zatem proces bezpieczeństwa realizowany w i na potrzeby środowiska informacyjnego, to transsektorowy obszar bezpieczeństwa, którego treść odnosi się do środowiska informacyjnego **(w tym cyberprzestrzeni)** państwa. Celem tego procesu jest zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej poprzez panowanie we własnej, wewnętrznej, krajowej infosferze oraz efektywną ochronę interesów narodowych w zewnętrznej (obcej) infosferze.

Osiąga się to poprzez realizacje takich zadań jak: zapewnienie adekwatnej ochrony posiadanych zasobów informacyjnych oraz ochrony przed wrogimi działaniami dezinformacyjnymi i propagandowymi (w wymiarze defensywnym) przy jednoczesnym zachowaniu zdolności do prowadzenia wobec ewentualnych przeciwników (państw lub innych podmiotów) działań ofensywnych w tym obszarze.

Środowisko informacyjne to zbiór osób, organizacji i systemów, służących gromadzeniu, przetwarzaniu, rozpowszechnianiu i działaniu na podstawie informacji (z włączeniem cyberprzestrzeni). Środowisko to składa się z trzech powiązanych ze sobą wymiarów, które w sposób ciągły wchodzą w interakcje z osobami, organizacjami i systemami. Zaliczane są do nich wymiary: poznawczy (czynnik ludzki), informacyjny (dane i informacje) oraz fizyczny (świat „realny")[2]. Wymiar fizyczny składa się z systemów dowodzenia i kontroli, kluczowych decydentów oraz infrastruktury wspierającej, która umożliwia jednostkom i organizacjom osiąganie celów. Jest to wymiar, w którym znajdują się sieci komunikacyjne i fizyczne platformy przetwarzania danych. Wymiar ten obejmuje (choć nie jest ograniczony): ludzi, narzędzia komunikacji i kontroli, gazety, książki, komputery, smartfony, tablety oraz jakiekolwiek inne komponenty, które mogą zostać poddane fizycznemu pomiarowi.

Wymiar informacyjny obejmuje to gdzie i jak informacja jest gromadzona, przetwarzana, przechowywana, dystrybuowana i chroniona. To wymiar, w którym dokonuje się proces dowodzenia i kontroli, oraz w którym przekazywane są intencje głównych decydentów. Działania w tym wymiarze wpływają na zawartość i sposób przepływu informacji.

---

[2] Information Operations, Joint Publication 3-13, Incorporating Change 1, Joint Chiefs of Staff, 20 November 2014.

Wymiar poznawczy dotyczy umysłów osób, które przekazują, odbierają, reagują bądź działają na podstawie informacji. Odnosi się do przetwarzania, percepcji, osądu i procesów decyzyjnych jednostki lub grupy. Wpływają na nie różne czynniki, z uwzględnieniem przekonań kulturowych, norm, podatności, motywacji, emocji, doświadczeń, moralności, edukacji, zdrowia psychicznego, tożsamości i ideologii. Zdefiniowanie tych czynników w danym środowisku jest kluczowe dla zrozumienia, w jaki sposób najefektywniej można oddziaływać na umysł decydenta i kreować pożądane skutki. Jako taki, wymiar poznawczy stanowi najważniejszy komponent środowiska informacyjnego.

Do **zagrożeń informacyjnych związanych z funkcjonowaniem w cyberprzestrzeni** należą: dezinformacja, trolling, wroga propaganda, zakłócające realizację istotnych zadań administracji publicznej oraz sektora prywatnego; ataki powodujące zakłócenia funkcjonowania sieci teleinformatycznych w sektorach i instytucjach o podwyższonym stopniu wrażliwości, w tym tworzących infrastrukturę krytyczną; istnienie technologicznych luk, które dają szansę, także niezauważonej, ingerencji w treści portali internetowych oraz wpływania na zdolności do działania w cyberprzestrzeni.

Kluczowe pojęcia i obszary działania: cyberbezpieczeństwo i bezpieczeństwo cyberprzestrzeni

Planowanie działań na rzecz cyberbezpieczeństwa państwa, jego sektora publicznego i prywatnego, a także jego obywateli, wymaga dookreślenia pojęć związanych z tym obszarem funkcjonowania systemów bezpieczeństwa. Odwołać się w tym miejscu można do „Doktryny cyberbezpieczeństwa RP", która podjęła tę tematykę, wyróżniając dwa odrębne pojęcia opisujące bezpieczeństwo państwa w kontekście jego funkcjonowania w cyberprzestrzeni.

Pierwszym z nich jest **pojęcie cyberbezpieczeństwa**, czyli bezpieczeństwo państwa w cyberprzestrzeni. Pojęcie to definiowane jest jako proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni.

Kolejnym pojęciem opisanym z Doktrynie jest **bezpieczeństwo cyberprzestrzeni**, a zatem część cyberbezpieczeństwa państwa, obejmująca zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni państwa wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych.

Zaznaczyć należy, że wśród najważniejszych **celów działań na rzecz cyberbezpieczeństwa** zidentyfikować można następujące:

- ocena warunków cyberbezpieczeństwa, w tym rozpoznawanie zagrożeń, szacowanie ryzyk i identyfikacja szans,
- zapobieganie (przeciwdziałanie) zagrożeniom, redukowanie ryzyk i wykorzystywanie szans,
- obrona i ochrona własnych systemów i zgromadzonych w nich zasobów,
- zwalczanie (dezorganizowanie, zakłócanie i niszczenie) źródeł zagrożeń (aktywna obrona oraz działania ofensywne),
- po ewentualnym ataku – odtwarzanie sprawności i funkcjonalności systemów tworzących cyberprzestrzeń.

Wśród **praktycznych przedsięwzięć**, których celem jest zapewnienie efektywności działania państwa w cyberprzestrzeni jako na piątej płaszczyźnie konfliktu wskazać można:

- zapewnienie posiadania przez państwo zdolności obrony i ochrony własnych systemów teleinformatycznych i zgromadzonych w nich zasobów, a także zdolności do aktywnej obrony i działań ofensywnych w cyberprzestrzeni, zintegrowanych z pozostałymi zdolnościami sił zbrojnych państwa,
- tworzenie i wzmacnianie struktur wojskowych przeznaczonych do realizacji zadań w cyberprzestrzeni, dysponujących zdolnościami w zakresie rozpoznawania, zapobiegania i zwalczania cyberzagrożeń,
- koordynowanie inicjatyw badawczo-rozwojowych, także w ramach współpracy cywilno-wojskowej, na rzecz cyberbezpieczeństwa,

- koordynowanie współpracy wyspecjalizowanych (działowych) centrów cyberbezpieczeństwa w celu uzyskania pełnej, współdzielonej świadomości sytuacyjnej,
- bieżące monitorowanie i wzmacnianie bezpieczeństwa sieci wykorzystywanych do dystrybucji i przechowywania informacji zakwalifikowanych jako informacje niejawne,
- rozwijanie środków kontrwywiadowczych w cyberprzestrzeni poprzez optymalizację rozwiązań na poziomie programistycznym, jak i fizycznych zabezpieczeń sieci,
- implementowanie systemów przeciwdziałania potencjalnym naruszeniom systemu w czasie rzeczywistym:
    - lokowanie w cyber-otoczeniu własnych systemów komputerowych pasywnych sensorów mających na celu wykrywanie potencjalnego złośliwego kodu w pakietach danych pochodzących z intrenetu,
    - redukowanie i konsolidowanie zewnętrznych punktów dostępu do sieci internet w celu minimalizowania ryzyk dla sieci wykorzystywanych na potrzeby systemu bezpieczeństwa państwa,
- wzmacnianie wysiłków edukacyjnych w obszarze cyberbezpieczeństwa ze szczególnym uwzględnieniem programów szkoleniowych w obszarze zdolności defensywnych i ofensywnych w cyberprzestrzeni,
- dbałość o długofalowe partnerstwo i współpracę pomiędzy sektorem publicznym i prywatnym, zwłaszcza w odniesieniu do prywatnych operatorów kluczowych elementów krytycznej infrastruktury teleinformatycznej państwa.

Podkreślić trzeba, że ochrona działań własnych w cyberprzestrzeni, a także zabezpieczenie informacji w środowisku bezpieczeństwa wiąże się nierozerwalnie z **rozwojem systemów kryptograficznych**. Szanse w dziedzinie cyberbezpieczeństwa stwarza skuteczne wykorzystanie potencjału naukowego w dziedzinie nauk informatycznych i matematycznych, dający możliwość rozwijania narodowych systemów służących cyberbezpieczeństwa oraz kryptologii, w tym kryptografii, zapewniających suwerenne panowanie nad systemami teleinformatycznymi należącymi do państwa. Urządzenia utajniające są najwrażliwszym elementem systemów łączności i informatyki. Aby uzyskać odpowiedni poziom efektywności wykorzystania urządzenia

utajniającego pożądana jest pełna kontrola nad tym sprzętem, a co ważniejsze nad algorytmem i kluczem kryptograficznym, co skłania do zakupu urządzeń tego typu tylko produkcji własnej. Jednak technologia ta jest trudna do opanowania i wdrożenia nie jest łatwa, stąd liczba producentów jest niewielka.[3]

Kategorie wrogich działań i operacji w cyberprzestrzeni

Zrozumienie tego, czym są operacje w cyberprzestrzeni staje się możliwe dzięki nadaniu pojęciom z nim związanym określonych granic oraz przedmiotowych i podmiotowych punktów odniesienia. Biorąc pod uwagę, iż jest to stosunkowo nowy obszar działań, który szybko musiał zostać zintegrowany z dotychczasowymi działaniami różnych rodzajów sił zbrojnych, niezbędne stało się wypracowanie ram pojęciowych służących planowaniu na poziomie operacyjnym i taktycznym.

Rozważania metodologiczne oparte o bezpośrednie efekty działań w cyberprzestrzeni pozwalają na wskazanie sześciu kategorii zewnętrznych wrogich działań[4]:

1. skanowanie (scanning) – polegające na sprawdzaniu lub skanowaniu pod kątem znalezienia słabych (wrażliwych na atak) punktów systemu – kategoria ta całkowicie wyklucza podejmowanie jakichkolwiek działań, których celem miałoby być zyskanie dostępu do tego systemu, polega najczęściej na skanowaniu portów i śledzeniu ruchu w sieci;
2. naruszenie systemu (intrusion) – polega na uzyskaniu dostępu do systemu komputerowego (nawet bez kradzieży/ niszczenia danych), często wykorzystujące słabe zabezpieczenie systemów;
3. gromadzenie danych (data collection) – celowe gromadzenie prywatnych, chronionych danych („prywatnych" w rozumieniu „nie należących do domeny publicznej; „chronionych" w rozumieniu „objętych celowym wysiłkiem mającym nie dopuścić do przedostania się ich do domeny publicznej"), nie

[3] W Polsce prowadzone są prace w dziedzinie kryptografii w różnych ośrodkach politechnicznych (m.in. w WAT, gdzie kształci się specjalistów z dziedziny kryptografii. Ponadto prace konstrukcyjne prowadzono w WIŁ.

[4] Robert Belk, Matthew Noyes, On the Use of Offensive Cyber Capabilities. A Policy Analysis on Offensive US Cyber Policy, Harvard Kennedy School of Government, 2012, s. 42-111.

zawsze wymaga naruszenia systemu, może być realizowane z wykorzystaniem monitorowania komunikacji, wywiadu sygnałowego itp.;

4. cyberatak – zewnętrzne działanie w cyberprzestrzeni, mające skutki w postaci zakłócenia funkcjonowania lub zniszczenia (logicznego bądź fizycznego) w stosunku do danych lub systemów (może obejmować działania takie, jak rozproszona odmowa dostępu – DDoS, po manipulowanie procesami przemysłowymi – np. Stuxnet) [5];
5. cyber-kontratak – ograniczone zewnętrzne cyber-operacje w celu powstrzymania wrogich działań w sposób, który wpływa na systemy komputerowe przeciwnika;
6. cyber-siła (cyber force) – odnosi się do cyberataków z tak daleko posuniętymi efektami fizycznymi, że powinny być uznawane za „użycie siły" zgodnie z prawem międzynarodowym (choć skodyfikowanie pojęcia „użycie siły" w kontekście nowych technologii i metod ataku pozostaje wyzwaniem dla społeczności międzynarodowej).

Jako przykład praktycznego podejścia do klasyfikacji działań w cyberprzestrzeni posłużyć może leksykon operacji stworzony dla potrzeb amerykańskiej armii[6]:

- operacje w cyberprzestrzeni – stosowanie cyber-zdolności w tych sytuacjach, w których pierwotnym celem jest realizacja zadań poprzez cyberprzestrzeń lub w cyberprzestrzeni; operacje takie obejmują działania w sieciach komputerowych lub działania na rzecz Globalnego Węzła Informacji (Sieci Informacyjnych Departamentu Obrony: DODIN – Department of Defense Information Networks)[7];
- operacje sieciowe (NetOps) – operacje prowadzone w celu wykorzystania i obrony Globalnego Węzła Informacji;

---

[5] Autorzy analizy stosują odmienną od powszechnej definicję, w której „atak" to nie każde nieuprawnione wejście do systemu, ale tylko taki jego rodzaj, który wiąże się z wyrządzeniem szkód.

[6] "DOD Cyberspace Operations Lexicon", Joint Chiefs of Staff, źródło: http://www.hsdl.org/?abstract&did=734860&advanced=advanced

[7] Globalny Węzeł Informacji (GIG – Global Information Grid), pojęcie zastępowane obecnie przez sformułowanie Sieci Informacyjne Departamentu Obrony: DODIN – Department of Defense Information Networks, obejmujące sieci wykorzystywane przez i do działań Departamentu Obrony USA.

- przewaga w cyberprzestrzeni – stopień dominacji jednej siły w cyberprzestrzeni, który zapewnia bezpieczne, niezakłócone prowadzenie operacji przez tę siłę i powiązane z nią siły lądowe, morskie, powietrzne i operujące w przestrzeni kosmicznej bez efektywnego sprzeciwu przeciwnika;
- działania cyber-wojenne (cyber warfare) – konflikt zbrojny prowadzony w całości lub części w cyebrprzestrzeni; operacje militarne prowadzone w celu uniemożliwienia przeciwnikowi efektywnego wykorzystania systemów i broni w cyberprzestrzeni; obejmuje cyberataki, cyberobronę i operacje cyber-wsparcia;
- działania wczesnej fazy ataku: operacja, która poprzedza główny wysiłek w danym obszarze w celu przegotowania głównego ataku przez prowadzenie takich działań, jak rozpoznanie, przejęcie pozycji wsparcia, z włączeniem kluczowych węzłów lub systemów, wczesne rozmieszczenie lub usunięcie broni – jak rozminowanie, bombardowanie, wysadzanie podwodnych przeszkód, rozmieszczanie cyber punktów dostępu lub broni oraz operacje powietrzne;
- atak na sieci komputerowe (CNA – Computer Network Attack)[8] – kategoria ataków używanych do celów ofensywnych poprzez użycie sieci komputerowych w celu zakłócenia, odmowy dostępu, pogorszenia jakości, manipulowania lub zniszczenia informacji pozostających w systemach komputerowych będących celem ataku lub samych systemów komputerowych; ostatecznym oczekiwanym skutkiem nie musi być wywarcie wpływu na sam system, ale wsparcie większych operacji, na przykład operacji informacyjnych lub kontrterrorystycznych (zmiana lub umieszczanie fałszywych informacji w komunikacji przeciwnika albo zdobycie dostępu do kanałów komunikacyjnych i logistycznych przeciwnika);
- cyberatak – wrogie działanie z użyciem komputerowych lub innych pokrewnych sieci albo systemów w celu zakłócenia działania i/lub zniszczenia krytycznych cyber- systemów, zasobów lub funkcji przeciwnika; oczekiwane

[8] Zastępuje pojęcie: „wykorzystanie sieci komputerowych" (CNE – Computer Network Exploitation) – wsparcie zdolności operacyjnych oraz gromadzenia informacji poprzez użycie sieci komputerowych to zbierania danych na temat celu lub zautomatyzowanych systemów informacyjnych przeciwnika; obrona sieci komputerowych; operacje w sieciach komputerowych.

efekty mogą nie być ograniczone do samych systemów komputerowych lub danych – na przykład ataki komputerowych mogą służyć do pogorszenia sposobu funkcjonowania lub zniszczenia zdolności dowodzenia i kontroli sił przeciwnika; cyberatak może wykorzystywać metody bezpośredniego wprowadzania kodu, jak urządzenia peryferyjne, transmisje elektroniczne, kod wbudowany lub operatorów-ludzi; aktywacja lub efekt cyberataku może być znacząco oddalona czasowo lub geograficznie od jego przeprowadzenia.

Jak łatwo zauważyć, rozumienie ofensywnych zdolności i operacji w cyberprzestrzeni powiązane jest nierozerwalnie ze wsparciem działań kinetycznych. **Wynika to z faktu, że obok stanowienia piątego pola walki, cyberprzestrzeń stanowi współcześnie komponent dowodzenia i kontroli w każdej innej przestrzeni prowadzenia działań bojowych.**

Wykorzystanie zdolności ofensywnych w cyberprzestrzeni

Argumentem na rzecz wykorzystania cyberprzestrzeni w kontekście realizacji założonych celów strategicznych i taktycznych wydaje się efektywność prowadzonych na tej płaszczyźnie operacji. Efekt skali, który występuje w tym środowisku walki jest bowiem nie do przecenienia – pojedynczy kod teoretycznie może wyłączyć z działań całą klasę systemów bojowych przeciwnika, a operacje w cyberprzestrzeni realizowane są z prędkością, która jest niedostępna z punktu widzenia tradycyjnych środków prowadzenia konfliktów[9].

Różnorodność działań, które mogą być podejmowane z wykorzystaniem cyber-broni także nie ma sobie równych. Służyć mogą zarówno działaniom zaczepnym, jak i działaniom bojowym w pełnej skali. Z drugiej strony, efekty operacji w cyberprzestrzeni mogą być odwracalne oraz służyć wszystkim fazom konfliktu – od zniszczenia do odbudowy.

Jeśli działanie określonej cyber-broni zostanie skierowane przeciwko konkretnemu systemowi przeciwnika, może służyć do atakowania go w różnych punktach w czasie – od momentu jego powstawania / rozwijania (powodując problemy

[9] Maren Leed, Offensive Cyber Capabilities at the Operational Level. The Way Ahead, CSIS & Georgia Tech, September 2013, źródło: http://csis.org/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf, s. 1.

z niezawodnością działania), aż do decyzji o jego użyciu (udane unieruchomienie choćby jednego urządzenia danej klasy powoduje wątpliwości co do wiarygodności całej klasy w sposób, jaki nie jest możliwy w wypadku ataków kinetycznych), aż do przeciwdziałania efektom działania danej broni już po tym, kiedy rozpoczął się atak z jej użyciem[10].

Badania dotyczące ofensywnego użycia zdolności państwa w cyberprzestrzeni skupiają się między innymi nad rozróżnieniem cyber-działań w zależności od poziomu ich wykorzystania – strategicznego, operacyjnego lub taktycznego.[11] Na wszystkich tych poziomach cyberataki ukierunkowane są na odmowę dostępu, przerwanie lub pogorszenie zdolności przeciwnika, pośrednio (przez dezinformację) lub bezpośrednio.

Na poziomie strategicznym dowódcy będą bardziej skłonni do zainteresowania dużymi węzłami informacyjnymi – lub tymi, które są postrzegane jako niewspółmiernie ważne przez przeciwnika. Czasowe przerwanie ich działania może wystarczyć do zakłócenia sposobu działania przeciwnika – choć całkowite zniszczenie części sieci również może być celem działania. Niemal z definicji cele takich działań wybierane są wcześniej, często z kilkuletnim wyprzedzeniem. Ich charakterystyka obejmuje nie tylko wielkość, ale także ilość połączeń z innymi węzłami i sieciami – pojęcie strategicznego celu w cyberprzestrzeni dotyczyć może zatem sieci dowodzenia i kontroli wrogiego dowództwa i wspierającej je infrastruktury. Cele te będą w znacznej większości statyczne i dobrze chronione nie tylko w cyberprzestrzeni, ale także fizycznie.

Dowódcy na poziomie taktycznym będą z drugiej strony bardziej skłonni do przeprowadzania cyber-ataków na lokalną skalę, w celu wsparcia działań prowadzonych na kontrolowanym przez nich teatrze działań. Może się to łączyć także z większą skłonnością do atakowania celów wybieranych ad hoc, wraz z ich pojawieniem się w zasięgu, na przykład w sieciach bezprzewodowych.

Inne będzie podejście także do zabezpieczenia informacyjnego operacji w cyberprzestrzeni w zależności od poziomu, na którym są prowadzone. Z punktu widzenia dowództwa na poziomie strategicznym, szczególnie premiowana może być dyskrecja przeprowadzenia ataku – tak ze względu na konsekwencje polityczne, jak ze względu na korzyści, które mogą zostać utracone w przyszłości, jeśli atak zostanie

[10] Ibidem, s. 1.
[11] Ibidem, s. 3.

wykryty w trakcie jego trwania. Odmiennie, dowódcy na poziomie taktycznym / operacyjnym, większą wagę mogą przykładać do szybkości przeprowadzenia ataku, niż do jego dyskrecji[12].

Warto zauważyć, że z punktu widzenia politycznych i psychologicznych efektów, cyber-broń posiada immanentne ograniczenia (niemożność zastraszania przeciwnika lub podnoszenia autorytetu państwa w wyniku prezentowania posiadanych zasobów ofensywnych przy jednoczesnym poważnym zagrożeniu w postaci poderwania autorytetu państwa i zaufania do niego). Co więcej, efektywne użycie cyber-broni wiąże się w wypadku dobrze zabezpieczonych systemów w koniecznością użycia komponentu ludzkiego[13].

Wojna sieciocentryczna (wojna epoki wysokich technologii komunikacyjnych)

Analizując różnorodne aspekty oddziaływania przez cyberprzestrzeń na pojęcie współczesnego bezpieczeństwa – nie tylko w kontekście jego definiowania, ale także w kontekście jego praktyki, nie można pominąć roli, jaką rozwój wysokich technologii komunikacji i przetwarzania danych odgrywa w odniesieniu do współczesnego pola walki, skutkujących powstaniem pojęcia wojny sieciocentrycznej.

Wojna sieciocentryczna to „[…] nowa teoria wojny w epoce informacji. To także koncepcja, która – na najwyższym poziomie – stanowi militarną odpowiedź na epokę informacji. Termin ‘wojna sieciocentryczna’ (netcentric warfare) szeroko opisuje kombinację strategii, nowych taktyk, technik i procedur, a także rozwiązań organizacyjnych, które częściowo usieciowione siły zbrojne mogą zastosować, aby stworzyć decydującą przewagę pola walki.”[14]

Przystosowanie sił zbrojnych współczesnego państwa do nowego sposobu prowadzenia wojny nie jest zależne od znalezienia odpowiednich rozwiązań dla dylematów technologicznych – choć z pewnością bez nich nowe pole walki nigdy by nie zaistniało. Istotą zmiany jest bowiem kwestia behawioralna – zachowania zarówno pojedynczych jednostek, jak i organizacji działających w środowisku usieciowionym.

---

[12] Ibidem, s. 4.
[13] Thomas Rid, Cyberwar and Peace. Hacking Can Reduce Real-World Violence, źródło: http://csis.org/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf.
[14] The Implementation of Network-Centric Warfare, op.cit , s. 3.

Istotnym aspektem nowego pola walki jest przewaga wynikająca z uwspólnionej świadomości sytuacyjnej. Jest ona bez wątpienia jest argumentem na rzecz maksymalnego wykorzystania cech usieciowionego pola walki, jednak transformacja prowadząca do osiągnięcia takich zdolności jest ogromnym wyzwaniem.

Bezpośrednim efektem osiągania usieciowienia oddziałów jest przyspieszanie cyklu „obserwacji – orientacji – decyzji – akcji”[15]. Jest to abstrakcyjny konstrukt, opisujący sekwencję zdarzeń, która musi dojść do skutku w każdym militarnym starciu. Aktor w konflikcie musi dokonać obserwacji sytuacji na polu walki, dokonać właściwego procesu orientacji w stosunku do sytuacji taktycznej, podjąć decyzję i działać. Jest to proces fundamentalny z punktu widzenia działań militarnych, obowiązujący nie tylko na poziomie taktycznym, ale także na poziomie strategicznym. Warto zauważyć, że jest to proces, który zachodzi w każdej relacji drapieżnik – ofiara.

Możliwość przyspieszenia tempa tego procesu jest kluczowa z punktu widzenia uzyskiwania przewagi nad przeciwnikiem i utrzymywania do w pozycji defensywnej, wytrąconego z równowagi. Szybka obserwacja i orientacja nie tylko ułatwiają proces decyzyjny. Przetwarzanie informacji w czasie rzeczywistym na polu walki ma kluczowe znaczenie także dla modyfikacji przyjętego toku postępowania także w trakcie starcia – możliwość dostosowania do zmieniającej się sytuacji w środowisku bojowym zmienia bojowym.

Wzrost zależności tempa i sposobu prowadzenia operacji bezpieczeństwa w środowisku sieciowym ma jednak jednocześnie wiele negatywnych aspektów. Wśród najważniejszych warunków brzegowych, które muszą być zrealizowane, aby możliwe było wykorzystanie potencjału systemów bezpieczeństwa w otoczeniu sieciowym, można zidentyfikować następujące[16]:

1. bezpieczeństwo transmisji danych: ze względu na to, że znaczenie SIGINTU i prawidłowego zabezpieczenia kryptograficznego transmisji jest zrozumiałe dla wszystkich uczestników konfliktu, należy zakładać, że każda ze stron wkłada maksymalny wysiłek w rozpoznanie, podsłuch i dekryptaż na każdym etapie operacji; tym samym nie tylko treść transmisji, ale sam fakt jej

[15] Carlo Kopp, Understanding Network Centric Warfare, op.cit.
[16] Ibidem.

dokonywania mogą stanowić sygnał, który – jeśli zostanie przechwycony – może stanowić o porażce operacji;

2. trwałość sygnału transmisji: nie tylko celowe działanie przeciwnika, polegające na zakłócaniu transmisji, ale nawet zdarzenia naturalne, o charakterze losowym, mogą zagrozić bezpieczeństwu realizacji misji – rozbłysk słoneczny czy po prostu zła pogoda mogą uniemożliwić transmisję w kluczowym momencie realizacji operacji;
3. przepustowość kanałów transmisyjnych: w dobie licznych źródeł informacji, w tym tych, które obejmują cyfrową transmisję obrazów w wysokiej rozdzielczości, zapisów wideo i innych wielkich pakietów danych, a które jednocześnie muszą być dokładnie zabezpieczone przed infiltracją lub zakłóceniem (co również pochłania część wydajności łączy) przepustowość zapewniająca płynność transmisji jest czynnikiem krytycznym;
4. zdolność do właściwego ukierunkowania wiadomości i transmisji: przekazywanie danych i poleceń w sieci o zmiennej topologii, w płynnym środowisku operacyjnym wymaga nakładów na zapewnienie wiarygodniej transmisji danych bezpośrednio do adresata;
5. kompatybilność sygnałów i protokołów: jednym z najistotniejszych czynników jest interoperacyjna zbieżność formatów komunikacyjnych – udział w działaniach różnych platform i systemów wymaga zapewnienia, że rozbieżności w modulowaniu sygnałów i protokołach cyfrowych nie przeszkodzą w osiągnięciu efektywnego komunikowania w warunkach bojowych.

Organizacje wieku informacji: potrzeba (r)ewolucji

Epoka informacji wymaga zmian nie tylko w sposobie działania, ale także w sposobie organizowania się – wymaga ewolucji starych lub powstania nowych struktur, które efektywnie będą mogły odpowiadać na wyzwania współczesnego środowiska bezpieczeństwa.

Dostosowanie struktur organizacji bezpieczeństwa do wymogów usieciowionego środowiska bezpieczeństwa to wyzwanie szczególne. Działanie w środowisku sieciocentrycznym wymaga budowy organizacji, które swoje cele osiągają poprzez

elastyczność ról i działania oraz szybkość dowodzenia[17]. Organizacje takie, wykorzystując w zaawansowanym stopniu technologie informacyjne, polegają w swoich działaniach przede wszystkim na innowacyjnych strukturach dowodzenia dążąc do jak najszybszego odcięcia przeciwnika od możliwości podejmowania nowych działań. Co więcej, charakterystyczną cechą sposobu ich działania jest podejmowanie równoległych przedsięwzięć, które za pomocą zmasowanego efektu uzyskują dodaną wartość w zaskoczeniu przeciwnika.

Organizacja taka, aby w pełni efektywnie funkcjonować w usieciowionym środowisku, musi posiadać cechy samo-projektowania w trybie ciągłego dostosowywania się do nowych warunków. Teoria organizacji zawiera w sobie dwie koncepcje, które posłużyć mogą jako baza rozważań nad powstaniem tego rodzaju organizacji w strukturach wojskowych[18]:

1. koncepcja modyfikowanych form organizacyjnych, opartych na technologiach informacyjnych,
2. koncepcja organizacji zdolnych do gwałtownej zmiany i innowacji.

Koncepcja modyfikowanych form organizacyjnych obejmuje takie podejścia, jak organizacje wirtualne, alianse strategiczne, partnerstwa i organizacje usieciowione. Szczególnie istotne w kontekście rozważań o wojnie sieciocentryczne wydaje się podejście związane z organizacjami wirtualnymi. Mogą one obejmować zarówno zgromadzoną ad hoc grupę jednostek, często pochodzących z więcej niż jednej instytucji, o różnorodnych polach specjalizacji, powołane do realizacji pojedynczego projektu.

Choć elastyczność i wielozadaniowość wirtualnej organizacji, jaką mogą być połączone siły zadaniowe, mają liczne zalety, nie można pominąć problemów, jakie mogą się wiązać z ich użyciem. Wśród najważniejszych wymienić można zależność efektywności wykonywanych działań od skutecznej komunikacji, która w organizacji nieprzetestowanej pod względem koordynacji może zawieść w kluczowym momencie. Problemy z określeniem statusu, autorytetu i zakresu kompetencji poszczególnych komponentów również mogą stanowić przeszkodę skutecznego działania. Odpowiedzią na te wyzwania może stać się dopracowana i szczegółowa doktryna działania, jednak i

---

[17] Kishore Sengupta and Carl R. Jones, *Creating Structures for Network-Centric Warfare: Perspectives from Organization Theory*, Naval Postgraduate School, Monterey 1999, źródło: http://www.dtic.mil/dtic/tr/fulltext/u2/a458996.pdf, s. 1.

[18] Ibidem, s. 3.

ona musiałaby być przez pewien czas wdrażana – aż do momentu wzajemnego rozpoznania się elementów takiego systemu[19]. Koncepcja organizacji zdolnych do innowacji i gwałtownej zmiany dla efektywnego dostosowania do nowych wyzwań oparta jest o założenie, że takie organizacje zmieniają się w trybie ciągłym, co jest warunkowane trudnymi warunkami (zasada „dostosowania się, aby przetrwać").

NAJWAŻNIEJSZE REKOMENDACJE NA RZECZ DŁUGOFALOWEGO ROZWOJU SYSTEMÓW CYBERBEZPIECZEŃSTWA I ZDOLNOŚCI DZIAŁANIA

[19] Ibidem, s. 5.

W CYBERPRZESTRZENI

1. Postrzeganie zobowiązania do realizacji zadań w cyberprzestrzeni w taki sam sposób, jak w innych istotnych obszarów zapewniających bezpieczeństwo narodowe.
2. Przygotowanie mapy drogowej barier w obszarze cyberbezpieczeństwa, ze szczególnym uwzględnieniem transsektorowości cyberbezpieczeństwa oraz potrzeby realizacji działań w tym zakresie na płaszczyźnie współpracy i koordynacji w wymiarze międzyresortowym, wraz z planem eliminacji tych barier, harmonogramem i prognozami finansowymi.
3. Opracowanie i wdrożenie algorytmów działania, określających dobre praktyki i zasady współpracy międzyresortowej oraz z podmiotami sektora prywatnego, zwłaszcza operatorami teleinformatycznej infrastruktury krytycznej, oraz w sytuacjach realizacji międzyresortowych działań w obszarze cyberbezpieczeństwa. Powinny one być wdrożone jako obowiązkowy element szkolenia w przygotowaniu do działań antykryzysowych.
4. Ułatwianie wymiany informacji w zakresie zagrożeń cyberbezpieczeństwa oraz działań na rzecz przeciwdziałania im (szczególnie istotna jest wymiana informacji pomiędzy organami administracji centralnej, właściwymi służbami, agendami rządowymi i instytucjami oraz administracją samorządową), także w wymiarze międzynarodowym.
5. Prowadzenie polityki, w ramach której fundusze są wykorzystywane na tworzenie systemowych rozwiązań, zapewniających podtrzymywanie nie tylko bieżącego poziomu bezpieczeństwa zdolności działania w cyberprzestrzeni, ale także monitorowanie rozwoju nowych technologii ofensywnych i defensywnych oraz ich implementowanie do krajowego systemy cyberbezpieczeństwa.
6. Aktywne angażowanie organizacji przedstawicielskich sektora prywatnego i społeczeństwa obywatelskiego w proces tworzenia wewnętrznych wytycznych i polityk szkoleniowych, a także w ewaluacji i zbieraniu dobrych praktyk oraz identyfikacji wyzwań i zagrożeń.

7. Ekonomiczne wspieranie inicjatyw związanych z cyberbezpieczeństwem w indywidualnych organizacjach (inicjatywy te, o charakterze publiczno-prywatnym, powinny zawierać nagrody za szybkie reagowanie na problemy cyberbezpieczeństwa i kary za nieadekwatne do skali problemu podejście (np. ulgi podatkowe lub ubezpieczenia na preferencyjnych warunkach).
8. Zwiększony nacisk na dobre projektowanie systemów, realizowany z wykorzystaniem roli rządu jako kluczowego odbiorcy cybertechnologii.
9. Wspieranie badań interdyscyplinarnych badań naukowych z zakresu cyberbezpieczeństwa.

Podsumowanie

Choć społeczeństwo (i państwo) 2.0, uzależnione od Sieci i jej ciągłego wykorzystania, na każdej niemal płaszczyźnie swojego funkcjonowania stało się rzeczywistością, sporo jeszcze brakuje do realnego dostosowania struktur odpowiedzialnych za bezpieczeństwo do wymogów tego nowego środowiska.

Jest to szczególnie prawdziwe dla struktur bezpieczeństwa. Ze względu na tradycyjnie podejście do organizowania się oraz przywiązanie – także pod względem kultury organizacyjnej – do sztywnych, hierarchicznych struktur, ewolucja do postaci elastycznej, sieciowej organizacji może okazać się wyzwaniem nie na poziomie technologicznym, a na poziomie możliwości mentalnego i psychicznego przystosowania zarówno dowodzących, jak i dowodzonych.

Ich transformacja jest konieczna, aby w pełni odpowiedzieć na wyzwania hybrydowego – jednocześnie materialnego i cyfrowego – pola walki. Próba sprowadzenia „konfliktu przyszłości" do jednego z tym dwóch obszarów wydaje się bowiem błędem. Właściwą formą konfliktu przyszłości będzie bowiem najprawdopodobniej konflikt równoległy, odbywający się na wielu poziomach rzeczywistości materialnej i cyfrowej. Niezależnie jednak od przeszkód, obiektywnych i subiektywnych, jakie ta ewolucja może napotkać, wydaje się ona nieunikniona, a przygotowanie na nią jest zobowiązaniem wobec teraźniejszości i przyszłości państwa.

Autorzy: Paulina Piasecka, dr Krzysztof Liedel

Redakcja serii: Anna Radwan

Tłumaczenie: Aleksandra Żebrowska

Konrad Adenauer Stiftung

Publikacja wydana we współpracy z Fundacją Konrada Adenauera w Polsce.