aut. Grzegorz Małecki 05.04.2019

WYZWANIA CYBERBEZPIECZEŃSTWA NA WSCHODNIEJ FLANCE NATO [ANALIZA]

Terytorium szczególnie narażonym na zagrożenia mające źródła w cyberprzestrzeni lub z nią powiązane jest tzw., wschodnia flanka NATO. Dominującym czynnikiem ryzyka na tym obszarze jest leżąca w jego bezpośrednim sąsiedztwie Rosja i jej niezwykle ekspansywna polityka zagraniczna, ukierunkowana w pierwszej kolejności na przejęcie kontroli nad państwami tego regionu, uznawanymi przez nią za jej naturalna strefę wpływów.

Cyberprzestrzeń jest jednym z głównych terenów działania rosyjskiego aparatu wywiadowczo – propagandowo – informacyjnego prowadzącego ofensywę wymierzoną w państwa i społeczeństwa wschodniej flanki NATO, której celem jest ich wewnętrzna dezintegracja i osłabienie zdolności obronnych, a jednocześnie doprowadzenie do rozpadu ich więzi w ramach Sojuszu oraz UE. Do najskuteczniejszy narzędzi w jego rękach należą udoskonalone, dzięki najnowszym technologiom cyfrowym, tradycyjne techniki dezinformacji, manipulacji i inspiracji, rozwinięte i stosowane z powodzeniem przez sowieckie służby specjalne w okresie zimnej wojny. Skuteczna kompilacja operacji wpływu, ataków hakerskich, penetracji zasobów informacyjnych oraz systemów informatycznych i infrastruktury krytycznej za pośrednictwem cyberprzestrzeni, z ofensywą propagandową w tradycyjnych mediach i niekiedy operacjami militarnymi, pozwala Rosji na prowadzenie niezwykle skutecznych i niebezpiecznych działań noszących miano wojny hybrydowej. Każde z państw regionu doświadczyło lub doświadcza, w większym lub mniejszym stopniu, tego typu aktywności ze strony Rosji.

Do istotnych czynników ryzyka na obszarze wschodniej flanki NATO należy także narastająca w ostatnich latach rywalizacja mocarstw światowych USA i Chin, dla której istotnym teatrem działań jest cyberprzestrzeń. Jak mogliśmy to zaobserwować w ostatnich miesiącach przy okazji ożywionej debaty na temat budowy sieci 5G to właśnie Europa Środkowo-Wschodnia jest jednym z obszarów, na którym i o który toczy się dzisiaj walka, także w cyberprzestrzeni, między Chinami USA, w której swoje cele stara się realizować także Rosja.

Wśród czynników mających swój wpływ na stan bezpieczeństwa w cyberprzestrzeni w naszym regionie należy wymienić także przeciągający się kryzys projektu integracyjnego Wspólnoty Europejskiej, powiązany z nim ściśle kryzys migracyjny, a także inne negatywne zjawiska społeczne i polityczne w Europie, takie jak narastająca radykalizacja społeczeństw i nasilanie się ekstremizmów, czy wzrost zagrożenia terrorystycznego, m.in. w efekcie negatywnej ewolucji sytuacji na Bliskim Wschodzie. Wszystkie te zjawiska i procesy, jakkolwiek toczą się w świecie realnym , to jednak szereg czynników determinujących ich dynamikę i kierunki ma swe źródła w sferze cyber.

Osobnym wyzwaniem dla cyberbezbieczeństwa, mającym kluczowe, choć nie zawsze dostrzegane, znaczenie jest postępująca w zawrotnym tempie rewolucja technologii cyfrowych. Zmieniają one nasz świat i nasze życie niepostrzeżenie, ale w sposób nieodwracalny i dużo poważniejszy i głębszy niż się powszechnie uważa. W konsekwencji gruntownym zmianom podlega także nasze otoczenie

strategiczne, w którym powstają nowe wyzwania, ale także w którym mamy do czynienia z nowymi szansami i możliwościami. Jednym ze skutków rewolucji cyfrowych jest także dezaktualizacja dotychczasowego konceptu cyberbezpieczeństwa, które w realiach Przemysłu 4.0, Internetu Rzeczy (IoT) czy sieci 5G będzie musiał objąć zagadnienia daleko wykraczające poza cyberprzestrzeń, czyli bezpieczeństwo systemów informacyjnych (jak ujmuje to uchwalona w 2018 roku ustawa o krajowym systemie cyberbezpieczeństwa). Zdaniem niektórych ekspertów już dzisiaj powinniśmy mówić o "bezpieczeństwie cyfrowym", stanowiącym nowe holistyczne podejście do zagadnienia bezpieczeństwa, łączące w sobie sferę fizyczną z wirtualną, czynnik ludzki z technicznym.

W tym kontekście nie ulega wątpliwości, że za jedno z najważniejszych wyzwań należy uznać zbliżający się wielkimi krokami nowy etap transformacji cyfrowej, związany z budową sieci 5G, wdrażaniem Przemysłu 4.0, implementacją IoT oraz IIoT, sztuczną Inteligencją (AI), uczeniem maszynowym itp.. Warunkami skutecznego stawienia czoła temu wyzwaniu jest wyciągnięcie wniosków z błędów popełnionych na wcześniejszych etapach, w tym przede wszystkim nadanie priorytetu kwestiom bezpieczeństwa od samego początku projektowania i wdrażania nowych technologii i systemów.

Omówione wyżej wyzwania i zagrożenia odnoszą się do każdego z państw wschodniej flanki NATO, stając się wyzwaniami dla całego regionu. Ścisła współpraca i skoordynowana odpowiedź na nie jest gwarancją skutecznego stawienia im czoła oraz wykorzystania szans, jakie się z nimi wiążą, przede wszystkim wzmocnienia odporności na zagrożenia oraz modernizacji państw i społeczeństw, dzięki transformacji cyfrowej. Dzięki zainicjowanym w ostatnich latach projektom współpracy regionalnej, na czele z inicjatywą Trójmorza oraz tzw. dziewiątką bukaresztańską, istnieją bardzo solidne fundamenty i świadomość wspólnoty celów. Konieczne jest jednak dynamiczne pogłębienie współpracy i przeniesienie jej na grunt konkretnych projektów i przedsięwzięć na różnych poziomach i obszarach. Ponadto konieczne jest wypracowanie nowych form współdziałania, uwzględniających szybkie zmiany otoczenia, w związku z przeobrażeniami środowiska cyfrowego. Priorytetowo należy potraktować innowacyjność i bezpieczeństwo.

Skuteczna koordynacja podejmowanych wysiłków, zapewniająca właściwą dynamikę i efektywność prac, wymaga instytucjonalizacji, zwłaszcza na etapie wykonawczym, oraz jednolitego przywództwa. Zdecydowane rozstrzygnięcia w tej materii nie mogą czekać, albowiem zaniedbania w tym względzie grożą utratą dynamiki, a jednocześnie przewagi, w stosunku do rywali i konkurentów. Równie ważną kwestią jest konsolidacja zasobów i aktywności, która gwarantuje efektywność i skuteczność, minimalizując koszty i ewentualne straty.

W tym kontekście szczególną uwagę warto zwrócić na praktyczne doświadczenia ostatnich lat na polu walki z cyberzagrożeniami, jakie stały się udziałem kilku państw bezpośrednio dotkniętych przez ataki cybernetyczne przeprowadzone z terytorium Rosji. Mowa to o Gruzji, Estonii i Ukrainie. Również Polska dysponuje interesująca wiedzą na temat rosyjskich ataków cybernetycznych, np. podejmowanych w stosunku do amerykańskich żołnierzy stacjonujących na naszym terytorium (próby hakowania telefonów). Oczywistym wnioskiem wydaje się konieczność tworzenia platform zapewniających wymianę doświadczeń tego rodzaju oraz bieżących informacji na temat wrogich działań w różnych newralgicznych sferach funkcjonowania państw, podejmowanych przez państwa trzecie wobec krajów regionu. Warto także rozważyć budowę efektywnych mechanizmów współpracy i koordynacji przy budowie a następnie praktycznym wykorzystaniu zdolności ofensywnych do operacji w cyberprzestrzeni, inaczej mówiąc wojsk obrony cybernetycznej. Świadomość wspólnoty celów i zagrożeń państw wschodniej flanki NATO nakazuje uzgadnianie podejmowanych w tej sferze aktywności od najwcześniejszych etapów tworzenia infrastruktury operacyjnej.

Las but not least, fundamentalnym warunkiem wszelkiej współpracy, a zwłaszcza w sferze bezpieczeństwa cyberprzestrzeni, jest budowa zaufania między jej użytkownikami, w tym przypadku

na poziomie państw i rządów. Bez wypracowania i implementacji wielopoziomowych i wszechstronnych rozwiązań, służących utrzymaniu i systematycznemu wzmacnianiu tego zaufania między wszystkimi użytkownikami cyberprzestrzeni w tych państwach, żadne inicjatywy nie zaowocują sukcesem w długiej perspektywie. Jednocześnie, wdrożenie skutecznych rozwiązań, skutkujących trwałym pogłębieniem zaufania między społeczeństwami regionu, dzięki cyberprzestrzeni, byłoby efektem o wyjątkowym, wręcz epokowym znaczeniu, stanowiącym fundament dla przyszłej architektury bezpieczeństwa całej wschodniej flanki NATO.

Autor: Grzegorz Małecki - prezes Fundacji Instytut Bezpieczenstwa i Strategii. Były Szef Agencji Wywiadu

Pełna wersja tekstu ukazała się na stronie Fundacji IBIS: Wyzwania Cyberbezpieczeństwa na Wschodniej Flance NATO