PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 172 (2793), 21 LISTOPADA 2023 © PISM

BIULETYN

Rosyjskie cyberzagrożenia dla państw NATO

Anna Maria Dyner

W ostatnich latach Rosja zwiększała intensywność wrogich operacji prowadzonych w cyberprzestrzeni przeciw państwom NATO oraz Ukrainie. Ta aktywność będzie utrzymana, o czym świadczą prace nad koncepcją strategii cyberbezpieczeństwa. Po stronie Sojuszu i państw członkowskich rośnie zatem konieczność dalszego rozbudowywania zdolności do prowadzenia działań defensywnych w tej domenie, w tym aktywnej obrony, oraz poszerzania współpracy z partnerami.

Od rosyjskiej agresji na Ukrainę w 2022 r. państwa NATO, zwłaszcza te, które wspierają Ukrainę, stały się głównym celem rosyjskich cyberataków. Raport Microsoft z października br. wskazuje, że 36% zidentyfikowanych przez tę firmę wrogich rosyjskich działań było wymierzonych w członków Sojuszu (dla porównania 48% w Ukrainę), a 13 spośród 15 najczęściej atakowanych państw to członkowie NATO i oczekująca na przyjęcie Szwecja. Wyłączając Ukrainę, Rosja atakowała cele zlokalizowane w USA (21% wszystkich wrogich aktywności), Polsce (10%) oraz Wielkiej Brytanii (9%), koncentrując się na infrastrukturze rządowej (27%). Dane polskich Wojsk Obrony Cyberprzestrzeni wskazują z kolei, że pięciokrotnie wzrosła liczba ataków przeprowadzonych od lutego 2022 r. do października 2023 r. przez prorosyjskie środowiska cyberprzestępcze i grupy hakerskie na infrastrukturę wojskową (będącą w kompetencji szefa CSIRT MON). Rosja podejmowała głównie próby kradzieży danych, paraliżowania systemów kluczowych dla funkcjonowania państwa czy podszywania się pod instytucje państwowe, m.in. w celu siania dezinformacji lub uzyskiwania dostępu do danych.

Rosyjskie podejście do cyberprzestrzeni. Rosja przywiązuje dużą wagę do cyberprzestrzeni jako domeny operacyjnej, w której może prowadzić skuteczne operacje ofensywne, będące elementem szerszych działań hybrydowych przeciwko adwersarzom. Cyberataki angażują stosunkowo małe środki, a mogą spowodować duże koszty po stronie państwa zaatakowanego. Rosja zwiększa zakres aktywności w cyberprzestrzeni od lat 2015–2016, co zbiegło się z przyjęciem przez to państwo doktryny bezpieczeństwa informacyjnego. W dokumencie jako najważniejsze zagrożenia zidentyfikowane zostały wpływanie na infrastrukturę informacyjną w celach wojennych, rozpoznanie technologiczne, prowadzenie operacji informacyjno-psychologicznych nakierowanych na destabilizację sytuacji wewnątrzpolitycznej oraz skoordynowane cyberataki na informatyczną infrastrukturę krytyczną. Obecnie w Rosji trwają prace nad koncepcją strategii cyberbezpieczeństwa, której projekt został umieszczony na stronie Rady Federacji. Dokument wskazuje, że Rosja będzie dążyła do zwiększenia zakresu działań podejmowanych w cyberprzestrzeni, tłumacząc to koniecznością ochrony infrastruktury państwowej, biznesu oraz edukacji społeczeństwa. Należy założyć, że w tych obszarach Rosjanie będą rozwijać zdolności ofensywne przeciwko NATO i jego partnerom.

W Rosji za działania w cyberprzestrzeni odpowiadają Zarząd Wywiadowczy rosyjskiego Sztabu Generalnego (G.U.), Wojska Technologii Informacyjnych, Federalna Służba Bezpieczeństwa oraz Służba Wywiadu Zagranicznego. Oficjalnie mają one zabezpieczać funkcjonowanie krytycznej infrastruktury informatycznej i chronić ją przed wrogimi działaniami. W praktyce prowadzą operacje ofensywne w cyberprzestrzeni, wymierzone głównie w Ukrainę i państwa NATO. W publikowanych po rosyjskiej agresji na Ukrainę raportach dotyczących cyberbezpieczeństwa, opracowanych przez główne zachodnie firmy z branży internetowej, wskazywane są liczne przykłady ich bezpośredniego zaangażowania oraz działań prowadzonych

przez powiązane z nimi grupy hakerskie. Najczęściej wymieniane są grupa Killnet oraz wiązane bezpośrednio z G.U. i siłami zbrojnymi FR Fancy Bear (APT28), Cozy Bear (APT29) i Sandworm (będące jednostką G.U. 74455).

Oprócz nasilenia skali ofensywnych działań w cyberprzestrzeni Rosja dąży do zwiększenia kontroli nad kształtowaniem międzynarodowego systemu prawnego dotyczącego cyberbezpieczeństwa. W tym celu aktywnie działa w ONZ, gdzie trwają prace nad traktatem o cyberprzestępczości, którego Rosja była główną inicjatorką. Na forum ONZ wspiera ją część państw, z którymi po 2020 r. podpisała dwustronne umowy o współpracy w zapewnieniu bezpieczeństwa informacyjnego, m.in. Azerbejdżan, Białoruś, Chiny, Indie, Indonezja, Nikaragua, Republika Południowej Afryki, Uzbekistan i Wietnam. Część z nich domaga się m.in. legalizacji inwigilacji poza granicami, co może oznaczać dodatkowe prześladowania dysydentów czy niezależnych mediów piszących o sytuacji w państwach niedemokratycznych. Takiemu podejściu przeciwstawiają się głównie państwa NATO i UE.

Zagrożenia i wyzwania dla NATO. Ataki w cyberprzestrzeni są elementem działań hybrydowych Rosji, które mogą prowadzić do destabilizacji w państwach NATO i osłabiać spójność polityczną Sojuszu. Tworzą też stałą presję na systemy informacyjne sojuszników i demonstrują posiadane przez Rosję zdolności. Wojna na Ukrainie pokazała jednocześnie, że rosyjskie cyberataki mogą być integralnym elementem operacji militarnej, gdyż pełnoskalowa agresja została poprzedzona próbą zdestabilizowania m.in. ukraińskiego systemu energetycznego i bankowego. Tym samym skuteczne eliminowanie tego zagrożenia może opóźnić rozpoczęcie pełnoskalowej agresji Rosji na państwa NATO.

Dostrzegając coraz większe znaczenie działań w cyberprzestrzeni, NATO na szczycie w Warszawie w 2016 r. uznało ją za piątą domenę operacyjną. Na szczycie w Brukseli w 2021 r. zatwierdzona została kompleksowa polityka cyberobrony, a sojusznicy zobowiązali się do wykorzystywania zdolności do aktywnego odstraszania, obrony i przeciwdziałania cyberzagrożeniom, w tym poprzez zbiorową odpowiedź. Od 2008 r. działa utworzone w Tallinnie NATO Cooperative Cyber Defence Centre of Excellence, które prowadzi badania, szkolenia i ćwiczenia w zakresie cyberobrony, obejmujące obszary technologii, strategii, operacji i prawa. W 2018 r. utworzono Centrum Operacyjne Cyberprzestrzeni, a w rezultacie szczytu w Wilnie zainaugurowane zostało Virtual Cyber Incident Support Capability. NATO prowadzi też regularne ćwiczenia, takie jak organizowane corocznie Cyber Coalition Exercise. Sojusz współpracuje też z partnerami międzynarodowymi, szczególnie z UE.

Najważniejszym problemem w walce z rosyjskimi cyberzagrożeniami jest jednak defensywna doktryna Sojuszu, która – choć NATO uznaje, że cyberataki mogą spowodować reakcję z art. 5. – może osłabiać wiarygodność polityki obrony i odstraszania w tej domenie. Jest to tym ważniejsze, że do cyberprzestrzeni, w której wrogie działania trwają nieustannie, nie da się odnieść pojęcia pokoju czy wojny ani wskazać początku konfliktu, który w innych domenach operacyjnych łatwo zdefiniować jako fizyczną agresję przeciwnika. Oznacza to, że państwa członkowskie powinny zredefiniować podejście do zagrożeń w cyberprzestrzeni i zacząć rozwijać koncepcję aktywnej obrony, czyli użycia środków ofensywnych w celach defensywnych. Polega ona na przechwytywaniu, zakłócaniu lub powstrzymywaniu ataku lub przygotowań do niego i z wyprzedzeniem, i w samoobronie. W przypadku groźby agresji militarnej NATO powinno mieć możliwość podjęcia działań wyprzedzających w cyberprzestrzeni, aby zminimalizować skutki ataku.

Wnioski. Biorąc pod uwagę podejście Rosji do działań w cyberprzestrzeni, można spodziewać się kontynuacji lub nasilenia cyberataków przeciwko państwom NATO. Ich celem będzie infrastruktura kluczowa dla funkcjonowania państwa, w tym wojskowa. Można też oczekiwać wzmocnienia antyzachodniej cyberkoalicji Rosji z takimi państwami, jak Chiny, Białoruś czy Iran, które w cyberprzestrzeni będą podejmowały wrogie aktywności wymierzone w państwa Sojuszu.

Rosyjskie działania będą zatem wymagały od państw NATO rozbudowy sił przeznaczonych do operowania w cyberprzestrzeni, a ze względu na odmienny charakter zagrożeń w tej domenie Sojusz będzie musiał rozwijać koncepcję aktywnej obrony. Kluczowe będą tu zdolności i zasoby państw członkowskich do prowadzenia rozpoznania oraz sposoby zapobiegania wrogiej aktywności. Dlatego istotne będą działania takich państw jak Polska, które już zgłaszają chęć rozwoju zdolności ofensywnych i przekazania ich na potrzeby Sojuszu. Im więcej państw złoży takie deklaracje, tym wyższa będzie wiarygodność sojuszniczego odstraszania i obrony.

Rosnąca liczba i skala zagrożeń będą również wymagały zwiększenia międzysojuszniczej współpracy kontrwywiadowczej. Ważna pozostanie współpraca z takimi partnerami jak UE, w tym dalszy rozwój zespołów reagowania cybernetycznego i kooperacji w obszarach obejmujących szkolenia, badania i ćwiczenia. Istotne będzie też utrzymywanie współpracy z największymi firmami technologicznymi, które aktywnie wspierają NATO i państwa członkowskie w walce z cyberzagrożeniami.