Pułaski Policy Papers
Komentarz Międzynarodowy Pułaskiego
ISSN 2080-8852 Warszawa, 17.05.2016 r.

Autor: Andrzej Kozłowski

Cyfrowe zagrożenia dla szczytu NATO

Zbliżający się szczyt Organizacji Sojuszu Północnoatlantyckiego w Warszawie wzbudza obawy o bezpieczeństwo całego wydarzenia. Media coraz częściej donoszą o możliwości ataków terrorystycznych, a służby przeprowadzają liczne ćwiczenia sprawdzające sposób postępowania w przypadku wystąpienia zagrożenia. Mniej miejsca poświęca się jednak potencjalnemu atakowi w cyberprzestrzeni.

Potencjalni sprawcy

Analizując aktorów państwowych jak i niepaństwowych potencjalnie zainteresowanych uderzeniem w szczyt NATO, na pierwszy plan wysuwa się Rosja posiadająca zarówno możliwości jak i intencje dokonania cyberataku. Państwo to dysponuje rozbudowanymi strukturami cyberjednostek ulokowanych w siłach zbrojnych jak i służbach specjalnych (Federalna Służba Bezpieczeństwa (FSB) czy Główny Zarząd Wywiadowczy (GRU)). Ponadto funkcjonuje w nim jedno z najbardziej rozbudowanych podziemi cyberprzestępców, którzy mają powiązania z siłami bezpieczeństwa i w przeszłości wielokrotnie wykonywali już operacje ofensywne na zlecenie Kremla. Trzecią grupą wykorzystywaną przez Rosję w środowisku wirtualnym są tzw. „patriotyczni hakerzy". Mogą oni przeprowadzić ataki typu Distributed Denial of Service (DDoS), jak również zaangażować się w działalność propagandową w mediach społecznościowych, czy na stronach internetowych. Jak już wspomniano, Rosja wykorzystywała swoje zdolności i siły w cyberprzestrzeni wielokrotnie. Najbardziej znanymi przypadkami był atak na Estonię w 2007 r. oraz połączenie działań cyfrowych i konwencjonalnych w 2008 r. podczas agresji

> *Należy pamiętać, że sposób zorganizowania szczytu NATO będzie miał wpływ na wizerunek i odbiór Polski na arenie międzynarodowej. Sprawna i bezpieczna organizacja tego szczytu potwierdzi polską pozycję w Sojuszu, jako silnego państwa poważnie podchodzącego do kwestii bezpieczeństwa.*

na Gruzję i w 2014 r. na Ukrainę. Rosjanie nie tylko wykorzystali swój potencjał atakując inne kraje, ale również prowadząc zaawansowane kampanie cyberszpiegowskie wymierzone np. w przedsiębiorstwa sektora energetycznego. Prawdopodobnie stali oni również za jedynym udanym włamaniem do tajnych sieci amerykańskiego wojska, które miało miejsce w 2008 roku. Wtedy to podłączono do sieci jednej z amerykańskich baz na Bliskim Wschodzie urządzenie przenośne ze złośliwym oprogramowaniem. To wszystko powoduje, że uznawani są za przedstawicieli państwa posiadającego najbardziej zaawansowane, obok Stanów Zjednoczonych, zdolności działania w cyberprzestrzeni. Eksperci stawiają ich nawet przed Chinami, których kampanie cyberszpiegowskie zdominowały dyskurs medialny za oceanem.

Rosja ma również intencje, żeby zaszkodzić szczytowi NATO w Warszawie. Po pierwsze, Sojusz jest postrzegany na Kremlu jak wróg numer jeden i zagrożenie dla państwa. Pogląd ten podzielany jest w dużej mierze zarówno przez władze jak i rosyjskie społeczeństwo. Drugim powodem jest chęć skompromitowania państwa-gospodarza szczytu, czyli Polski, która od dawna głośno ostrzegała przez rosyjskim imperializmem i domagała się stałej obecności NATO na flance wschodniej. Niedawna wypowiedź Władimira Putina, że „Polska do tej pory nie wiedziała, co znaczy być na naszym celowniku" powoduje, iż ryzyko przeprowadzenia takich ataków wzrasta.

Rosja nie jest jednak jedynym podmiotem potencjalnie zainteresowanym uderzeniem w cyberprzestrzeni podczas szczytu NATO. Drugim z nich jest tzw. Państwo Islamskie, przeciwko któremu prowadzone są działania zbrojne. Wielokrotnie zapowiadało ono przeprowadzenie ataków na Zachodzie. Zdolności działania ISIS w środowisku wirtualnym są jednak zdecydowanie mniejsze i raczej ograniczają się do działań propagandowych i prostych cyberataków jak np. DDoS. Dlatego też z ich strony zagrożenie jest zdecydowanie mniejsze.

Ostatnią grupą podmiotów zainteresowanych uderzeniem w szczyt NATO są liczne grupy niezależnych hakerów o anarchistycznym nastawieniu, widzących w Sojuszu symbol amerykańskiej dominacji nad światem. Ich zdolności i możliwość są różne. Mogą oni przeprowadzić ataki typu DDoS, czy też wykraść wrażliwe dane i potem je opublikować w Internecie.

Widać wyraźnie, że potencjalnych chętnych do przeprowadzenia cyberataków nie brakuje i mogą tego dokonać zarówno aktorzy państwowi jak i niepaństwowi.

Hipotetyczne scenariusze

1) Działania propagandowe

Działania propagandowe z wykorzystaniem mediów społecznościowych takich jak Twitter, Facebook, Youtube, publikowanie antynatowskich artykułów czy zalew antynatowskich komentarzy pod artykułami o tematyce poświęconej Sojuszowi mają już miejsce i prawdopodobne jest, że w przeddzień szczytu nastąpi ich intensyfikacja. Nie stanowią one typowego cyberataku, ale pokazują jak istotne może być wykorzystanie Internetu w działaniach propagandowych. Ich szkodliwość jest znikoma, może tylko przekonać część społeczeństwa, że to NATO jest zagrożeniem a nie Rosja, a polski rząd jest jedynie marionetką w rękach Stanów Zjednoczonych. Działania te mogą być dokonywane przez opłaconych przez Rosjan trollów internetowych, działanie antyglobalistów, przedstawicieli grupy Anonymous, jak również wielu tzw. „pożytecznych idiotów" (ang. Useful idiots) zarówno Polaków jak i obcokrajowców.

Prawdopodobieństwo wystąpienia: Już występuje

Możliwe straty: Niewielkie

2) Ataki DDOS i Web Defacement

Obok legalnej propagandowej działalności wymienionej wyżej, możemy mieć też do czynienia z popularnymi i wykorzystywanymi na szeroką skalę atakami typu DDoS Celem takich działań mogą być zarówno strony polskiego MSZ informujące o szczycie NATO, czy też oficjalna strona Sojuszu. W przeszłości obie witryny doświadczyły podobnych operacji i mogą być one powtórzone w przyszłości. Podmioty zainteresowane zaszkodzeniem szczytowi NATO mają możliwość i doświadczenie w tego typu akcjach. Mogą je nawet przeprowadzić tzw. „patriotyczni hakerzy", dzięki coraz łatwiejszym i powszechniejszym w użytku narzędziom. Będzie to wizerunkowa porażka dla NATO i Polski jeśliby do nich doszło, a serwisy byłyby wyłączone przez dłuższy czas. Groźniejszą wersją tego scenariusza jest przejęcie przez hakerów stron i zamieszczenie własnej treści o wyraźnie antynatowskim charakterze.

Prawdopodobieństwo wystąpienia: Duże

Możliwe straty: Niewielkie

3) Kradzież i publikacja danych

Wydaje się, że ze wszystkich podmiotów zainteresowanych przeprowadzeniem takiej operacji, największe zagrożenie pochodzi ze strony hakerów rosyjskich zainteresowanych poufnymi dokumentami dotyczącymi szczytu NATO. Mogą to być szczegóły tajnych rozmów pomiędzy dyplomatami z różnych państw, strategie postępowania czy inne istotne informacje, zwłaszcza omawiające szczegóły rozlokowania sił NATO na wschodniej flance. Następnie korzystając ze źródeł uchodzących za neutralne, takich jak Wikileaks czy grupa Anonymous, dokumenty te zostałby opublikowane osłabiając wydźwięk szczytu lub kompromitując poszczególne państwa. Zależnie od swojej treści mogłyby również wpłynąć na agendę szczytu, zmarginalizować omawiane tematy lub nawet pomniejszyć znaczenie decyzji, które tam zapadały. Podobna sytuacja miała już miejsce, kiedy w przeddzień spotkania prezydentów Stanów Zjednoczonych i Chin opublikowano sensacyjne materiały dostarczone przez Edwarda Snowdena. Ze spotkania bardzo szybko zniknęły tematy związane ze szpiegostwem w Internecie. Podobna sytuacja może powtórzyć się w przypadku szczytu NATO. Biorąc pod uwagę doświadczenie i zdolności podmiotów zainteresowanych takim przeciekiem, nie można wykluczyć takiego scenariusza. Niestety liczne przypadki kradzieży olbrzymich ilości informacji czy to z przedsiębiorstw sektora prywatnego, czy instytucji państwowych pokazują, że jest to coraz częstsze zjawisko. Brak wyszkolenia z zakresu cyberbezpieczeństwa wśród personelu odpowiedzialnego za zabezpieczenie danych oraz luki w oprogramowaniu znacznie ułatwiają dokonywanie takich ataków.

Prawdopodobieństwo wystąpienia: Średnie

Możliwe straty: Zależne od treści dokumentów

4) Atak hybrydowy

Kolejnym scenariuszem, przed którym przestrzega się w wielu państwach na świecie i który wzbudza uzasadniony niepokój ekspertów jest połączenie konwencjonalnego ataku i operacji w cyberprzestrzeni. Przykładowo, mogłoby dojść do ataku terrorystycznego przy jednoczesnym zablokowaniu sieci telefonicznych i alarmowych, utrudniając tym samym sprawną interwencję służb bezpieczeństwa. Skuteczne ataki blokujące numery alarmowe były w przeszłości przeprowadzane. Biorąc jednak pod uwagę, że Warszawa w trakcie

szczytu NATO będzie bardzo dobrze chroniona, ryzyko konwencjonalnego ataku jest niewielkie, co jednocześnie minimalizuje możliwość zaistnienia takiego scenariusza.

Prawdopodobieństwo wystąpienia: Niewielkie

Możliwe straty: Duże

5) Ataki na infrastrukturę krytyczną

Biorąc pod uwagę stale zwiększającą się liczbę prób ataków na infrastrukturę krytyczną, które w niektórych przypadkach zakończyły się sukcesem, nie można wykluczyć, że podobne działania również zostaną przeprowadzone przeciwko Polsce. Przykładów kampanii zakończonych powodzeniem, które doprowadziły do powstania zniszczeń fizycznych nie brakuje. W latach 2008-2010 połączona amerykańsko-izraelska kampania prowadzona z wykorzystaniem robaka Stuxnet, wymierzona w irański ośrodek w Natanaz, doprowadziła do uszkodzenia wirówek wzbogacania uranu, będąc pierwszym przypadkiem zniszczeń fizycznych spowodowanych przez program komputerowy. Nie był to jednak odosobniony przypadek. W 2014 r. cyberatak skierowany przeciwko hucie stali w Niemczech również doprowadził do materialnych uszkodzeń. Z polskiej perspektywy najgroźniejszy jest jednak incydent, który miał miejsce na Ukrainie, gdzie atak cyfrowy skierowany przeciwko infrastrukturze energetycznej w regionie Iwano-Frankowska spowodował, że milion mieszkańców Ukrainy zostało czasowo pozbawionych prądu. Wydaje się oczywistym, że stała za tym Rosja, pokazując swoją zdolność do przeprowadzenia takiej operacji. Przeprowadzenie podobnych działań wymierzonych w elektrownie w Polsce i odcięcie Warszawy od prądu, mogłoby utrudnić organizacje i przeprowadzenie szczytu NATO. Podobnie jak ataki cyfrowe przeciwko systemowi zarządzania ruchem czy kanalizacją. W takich przypadkach, kiedy kamery wszystkich stacji telewizyjnych skierowane będą na Polskę, straty wizerunkowe byłyby poważne, a wiele osób zaczęłoby się zastanawiać czy jest sens obrony państwa niezdolnego do zabezpieczenia jednego wydarzenia. Na szczęście ryzyko takiego ataku jest niewielkie. Po pierwsze, tego rodzaju operacja wymaga zaangażowanie znacznych środków finansowych i zasobów ludzkich, długiego planowania oraz dostępu do informacji na temat używanego oprogramowania i luk w nim zawartych. W przypadku zaatakowania infrastruktury energetycznej na Ukrainie, Rosja nie miała większego problemu w pozyskaniu tych

informacji, biorąc pod uwagę podobieństwo technologii wykorzystywanych przez oba kraje. W Polsce byłoby to trudniejsze i dlatego scenariusz ten wydaje się mało prawdopodobny.

Prawdopodobieństwo wystąpienia: Niewielkie

Możliwe straty: Poważne

Wnioski i rekomendacje

1. Należy pamiętać, że sposób zorganizowania szczytu NATO będzie miał wpływ na wizerunek i odbiór Polski na arenie międzynarodowej. Sprawna i bezpieczna organizacja tego szczytu potwierdzi polską pozycję w Sojuszu, jako silnego państwa poważnie podchodzącego do kwestii bezpieczeństwa.

2. Stopień wykorzystania cyberprzestrzeni do realizacji celów politycznych stale wzrasta i dlatego wymienione wyżej scenariusze nie powinny zostać zlekceważone przez decydentów.

3. W ciągu kilkudziesięciu dni nie da się stworzyć efektywnego systemu cyberbezpieczeństwa, można jednak podjąć szereg czynności utrudniających potencjalne cyberataki takie jak zmiana haseł, czy uwrażliwienie pracowników administracji na bezpieczeństwo w sieci poprzez zwrócenie uwagi na nieotwieranie wiadomości niewiadomego pochodzenia itp. Pozwoli to na zwiększenie zabezpieczenia wrażliwych danych oraz systemów infrastruktury krytycznej.

4. Powinny zostać przeprowadzone ćwiczenia na wypadek zaistnienia różnego rodzaju cyberataków i sposobu radzenia sobie z nimi oraz ich neutralizacji.

5. Walka z propagandą powinna mieć miejsce poprzez rzetelną kampanią informującą o celach NATO oraz otaczającej nas sytuacji międzynarodowej.

6. Serwisy internetowe publikujące antynatowską propagandę powinny zostać poddane obserwacji kontrwywiadowczej.

Autor: *Andrzej Kozłowski, Research Fellow Fundacji im. Kazimierza Pułaskiego*

Fundacja im. Kazimierza Pułaskiego jest niezależnym think tankiem specjalizującym się w polityce zagranicznej i bezpieczeństwie międzynarodowym. Głównym obszarem aktywności Fundacji Pułaskiego jest dostarczanie analiz opisujących i wyjaśniających wydarzenia międzynarodowe, identyfikujących trendy w środowisku międzynarodowym oraz zawierających implementowalne rekomendacje i rozwiązania dla decydentów rządowych i sektora prywatnego.

Fundacja w swoich badaniach koncentruje się głównie na dwóch obszarach geograficznych: transatlantyckim oraz Rosji i przestrzeni postsowieckiej. Przedmiotem zainteresowania Fundacji są przede wszystkim bezpieczeństwo, zarówno w rozumieniu tradycyjnym jak i w jego pozamilitarnych wymiarach, a także przemiany polityczne oraz procesy ekonomiczne i społeczne mogące mieć konsekwencje dla Polski i Unii Europejskiej.

Fundacja Pułaskiego skupia ponad 40 ekspertów i jest wydawcą analiz w formatach: „Stanowiska Pułaskiego", „Komentarza Międzynarodowego Pułaskiego" oraz „Raportu Pułaskiego". Fundacja wydaje też „Informator Pułaskiego", będący zestawieniem nadchodzących konferencji i spotkań eksperckich dotyczących polityki międzynarodowej. Eksperci Fundacji regularnie współpracują z mediami.

Fundacja przyznaje nagrodę "Rycerz Wolności" dla wybitnych postaci, które przyczyniają się do promocji wartości przyświecających generałowi Kazimierzowi Pułaskiemu tj. wolności, sprawiedliwości oraz demokracji. Do dziś nagrodą uhonorowani zostali m.in.: profesor Władysław Bartoszewski, profesor Norman Davies, Aleksander Milinkiewicz, prezydent Lech Wałęsa, prezydent Aleksander Kwaśniewski, prezydent Valdas Adamkus, Javier Solana, Bernard Kouchner i Richard Lugar.

Fundacja Pułaskiego posiada status organizacji partnerskiej Rady Europy.

www.pulaski.pl