PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 191 (2610), 6 GRUDNIA 2022 © PISM

BIULETYN

Znaczenie ataków cybernetycznych w strategii Rosji

Aleksandra Kozioł

Aby destabilizować sytuację wewnętrzną państw demokratycznych wspierających Ukrainę, Rosja wykorzystuje ataki cybernetyczne na ich instytucje publiczne i infrastrukturę krytyczną. Wyraźnie wzmogła tę aktywność po dokonaniu pełnoskalowej agresji w lutym br., co wpisuje się w realizację jej strategii wojskowej. W tym kontekście korzyści przyniosłoby opracowanie w ramach UE i NATO wspólnych planów działania na wypadek przyszłych zagrożeń w cyberprzestrzeni.

Rosyjskie zdolności w cyberprzestrzeni. Rosja od lat wykorzystuje przestrzeń cyfrową do realizacji własnych interesów, często naruszając prawo międzynarodowe. Przy pomocy wyspecjalizowanych jednostek wywiadu wojskowego (GRU) i zagranicznego (SVR), służby bezpieczeństwa (FSB) i opłaconych grup hakerów atakuje instytucje publiczne i podmioty prywatne innych państw. Wykorzystuje takie ataki do kradzieży, szyfrowania lub niszczenia danych, a także do infekowania sieci komputerowych, które stają się następnie źródłem złośliwego oprogramowania rozprzestrzenianego na inne podmioty. Działania rosyjskich hakerów są przede wszystkim elementem działań hybrydowych – Rosja często koordynuje cyberataki z dezinformacją w sieci, co pozwala wzmocnić ich siłę oddziaływania na społeczeństwo. Tak szeroko zakrojone akcje Rosjanie prowadzili np. w 2016 r., podczas wyborów prezydenckich w USA i kampanii brexitowej w Wielkiej Brytanii, w obu przypadkach pośrednio wpływając na wynik. Rosja jest też m.in. odpowiedzialna za atak złośliwego oprogramowania NotPetya w 2017 r., uznany za najbardziej destrukcyjny w historii. Pierwotnie wymierzony był w Ukrainę, rozprzestrzenił się jednak w kilkudziesięciu państwach i przyczynił do strat szacowanych na 10 mld dol. Publikowane w ostatnich miesiącach raporty, np. Microsoftu i Agencji UE ds. Cyberbezpieczeństwa (ENISA) wskazują, że pełnoskalowa agresja na Ukrainę wywołała znaczny wzrost cyberagresji. Rosja opisana jest tam przede wszystkim jako źródło zagrożenia, chociaż coraz częściej staje się również obiektem ataków.

Cyberataki elementem agresji na Ukrainę. Rosja już od początku 2022 r. prowadziła nasilone działania w cyberprzestrzeni, przygotowując się do inwazji. Najpoważniejszy atak miał miejsce w połowie lutego, kiedy rosyjscy hakerzy doprowadzili do paraliżu kilku ukraińskich stron rządowych, w tym ministerstw spraw zagranicznych i obrony, a także dwóch największych państwowych banków. Na godzinę przed rozpoczęciem inwazji, by osiągnąć efekt zaskoczenia i spowolnić odpowiedź, Rosja przeprowadziła też cyberatak na działającą w Europie i na obszarze Morza Śródziemnego sieć satelitarną KA-SAT. W ten sposób sparaliżowała komunikację między kilkoma tysiącami użytkowników publicznych i prywatnych na Ukrainie, a także zerwała łączność z szerokopasmowym internetem dziesiątkom tysięcy odbiorców w kilku państwach członkowskich UE. W kolejnych miesiącach ofiarami zmasowanej rosyjskiej ofensywy w cyberprzestrzeni padały m.in. ukraińskie władze, media i infrastruktura krytyczna. Hakerzy, wykorzystując głównie kampanie wyłudzające dane i luki systemowe, wykradali potrzebne Rosji informacje, niszczyli kluczowe dane strony ukraińskiej lub prowadzili akcje inwigilacyjne. Cyberataki skorelowane były więc z innymi działaniami Rosji, a w kilku przypadkach bezpośrednio poprzedzały wydarzenia na froncie, np. ofensywę na miasto Sumy, ostrzał wieży telewizyjnej w Kijowie czy zajęcie zaporoskiej elektrowni jądrowej.

Rosja nasiliła ponadto działania w cyberprzestrzeni wymierzone m.in. w instytucje publiczne, organizacje humanitarne oraz think tanki w ponad 40 państwach

zaangażowanych w pomoc Ukrainie. Najważniejszym celem rosyjskich operacji są USA, postrzegane jako główny przeciwnik na arenie międzynarodowej. Najczęściej atakowanym państwem w Europie jest natomiast Polska, m.in. ze względu na fakt, że przez jej terytorium odbywa się większość transportów z pomocą wojskową i humanitarną dla Ukrainy. Obiektami ataków są ponadto inne państwa członkowskie NATO, a także Finlandia i Szwecja. Zagrożenie ze strony Rosji jest poważne, gdyż posiada ona możliwości nie tylko przełamywania zachodnich zabezpieczeń (według szacunków udaje się to w ok. 1/3 przypadków), ale także prowadzenia w cyberprzestrzeni długotrwałej inwigilacji. Podobnie jak wobec Ukrainy, niektóre działania wymierzone w państwa zachodnie pozostają skorelowane z wydarzeniami o charakterze politycznym, np. 23 listopada br. Parlament Europejski został zaatakowany przez hakerów, gdy uznał Rosję za sponsora terroryzmu.

Reakcja na rosyjskie zagrożenie w cyberprzestrzeni. Pełnoskalowa agresja Rosji zwiększyła udział państw zachodnich w budowie ukraińskich zdolności cyberobrony. Jeszcze w lutym UE po raz pierwszy uruchomiła Zespół Szybkiego Reagowania w Cyberprzestrzeni w ramach PESCO, delegując do pomocy stronie ukraińskiej ekspertów z państw członkowskich. W marcu Ukraina dołączyła ponadto do współpracy w ramach Centrum Doskonalenia Cyberobrony NATO (CCDCOE). W obliczu pełnoskalowej agresji ukraińskie władze potrzebowały jednak szybko zwiększyć zdolności ofensywne w przestrzeni cyfrowej, dlatego już 26 lutego wicepremier i minister transformacji cyfrowej Mychajło Fedorow ogłosił powstanie Armii IT Ukrainy. Jej głównym zadaniem są ataki na rosyjskie podmioty publiczne i prywatne, polegające m.in. na blokowaniu stron administracji i mediów rządowych, rozprzestrzenianiu prawdziwych informacji o wojnie, a także uzyskiwaniu dostępu do danych. Chociaż jest inspirowana i faktycznie zarządzana przez ukraińskie władze, organizacja ta pozostaje strukturą nieoficjalną, skupioną wokół kanału na komunikatorze Telegram. Działania na rzecz Ukrainy podejmują także inne grupy hakerskie, np. Anonymus i Białoruscy Cyberpartyzanci, nie są one jednak powiązane z ukraińskimi władzami, a ich działalność jest motywowana ideologicznie. Grupie Anonymus przypisuje się np. emisję w marcu prawdziwych informacji na temat wojny na Ukrainie na antenach głównych rosyjskich kanałów telewizyjnych, takich jak Pierwyj Kanał i Rossija 24. Bezprecedensowe jest także stanowisko prywatnych firm, np. Microsoftu i Google'a, które podjęły współpracę z ukraińskimi władzami, wspierając je w wykrywaniu i zwalczaniu rosyjskich ataków.

Wnioski. Rosyjskie władze posługują się cyberatakami, by zwiększyć efektywność swoich działań na arenie międzynarodowej. Wzmożenie ofensywy Rosji w przestrzeni cyfrowej jest wymierzone w stabilność państw demokratycznych, co m.in. ma zniechęcić je do wspierania Ukrainy. Rosyjscy hakerzy uderzają jednak przede wszystkim w cele ukraińskie (według szacunków to dwa–trzy poważniejsze ataki tygodniowo), jako że największe znaczenie ma sytuacja na froncie. Wymuszając na Ukrainie ciągłą obronę swoich zasobów, Rosja stosuje taktykę dążenia do wyczerpania przeciwnika, jednocześnie starając się zdobyć przewagę informacyjną i obniżyć zaufanie Ukraińców do władz. W bardziej wybiórczy sposób prowadzone są natomiast ataki na państwa demokratyczne, stanowiąc przeważnie element sygnalizowania politycznego stanowiska Rosji. Rosyjskie władze chętnie i coraz bardziej otwarcie stosują taką taktykę, ponieważ cyberataki – traktowane jako działania poniżej progu wojny – rzadko spotykają się z odpowiedzią publicznego lub prywatnego podmiotu, który stał się ofiarą. Powodem są nie tylko trudności w zidentyfikowaniu źródeł, ale także ograniczone możliwości wyciągania konsekwencji wobec sprawców. UE np. przyjęła pierwsze w historii sankcje za cyberataki (m.in. NotPetya) w 2020 r., obejmując nimi trzy podmioty i sześć osób.

Znaczny wzrost liczby rosyjskich cyberataków na Ukrainę stanowi poważne zagrożenie także dla państw zachodnich, trudno bowiem ocenić, czy obecna koncentracja terytorialna tych działań jest podyktowana charakterem operacji lub decyzjami władz Rosji. Potencjalne użycie złośliwego oprogramowania może doprowadzić do poważnych skutków, jeśli dojdzie do jego niektontrolowanego rozlania, tak jak stało się w przypadku NotPetya. Ponadto nawet jeśli rosyjskie wojska zostaną wyparte z Ukrainy, Rosja zachowa zdolności do cyberagresji. W tym kontekście warto, by Polska inicjowała pogłębianie współpracy państw UE i NATO, a także jej rozszerzanie na Ukrainę i innych partnerów, np. Mołdawię i Gruzję. Kluczowe będą nie tylko poprawa wymiany informacji i wzmacnianie cyberzabezpieczeń, ale także przygotowywanie planów działania na wypadek ataków. Rosnące zaangażowanie międzynarodowych korporacji funkcjonujących w przestrzeni cyfrowej będzie wymagało również pogłębiania współpracy publiczno-prywatnej, co staje się kwestią szczególnie pilną dla najbardziej zagrożonych państw w Europie, w tym Polski. Dotychczasowe przykłady wskazują, że dywersyfikacja dostawców usług wzmacnia odporność na ewentualne skutki cyberataków, dlatego m.in. znaczenie ma dostęp do internetu z alternatywnych źródeł, takich jak sieć Starlink, a także przechowywanie danych dzięki rozwiązaniom chmurowym.