Od 2016 roku cyberprzestrzeń, po lądzie, morzu, przestrzeni powietrznej i kosmosie, jest oficjalnie uznaną przez Sojusz Północnoatlantycki (NATO) piątą domeną operacyjną. Pojęcie cyberwojny nie zostało dotąd zdefiniowane w jednoznaczny sposób. Jason Andress i Steve Winterfeld wskazują na problem z ustaleniem definicji cyberwojny, która wciąż jest przedmiotem debaty naukowej. Pomimo trudności badacze tego obszaru podejmują próby naukowego opisu tego zjawiska.

Punktem wyjścia dla poniższej analizy jest definicja autorstwa James A. Green'a, zgodnie z którą „cyberwojna stanowi kontynuację polityki poprzez działania inicjowane w cyberprzestrzeni zarówno przez podmioty państwowe, jak i niepaństwowe, stanowiące zagrożenie dla bezpieczeństwa innych podmiotów lub działanie odpowiadające na zagrożenie dla bezpieczeństwa państwa (rzeczywiste lub postrzegane)".

Przyjętą w analizie definicją cyberataku jest propozycja zespołu badaczy Uniwersytetu Warszawskiego, zgodnie z którą cyberatak to „nielegalne działanie prowadzone w przestrzeni wirtualnej, którego celem jest przejęcie kontroli nad stronami internetowymi, zawartością skrzynek pocztowych lub baz danych instytucji, firmy, grupy itp.; często akt cyberterroryzmu".

Szybka i wiarygodna identyfikacja agresora w cyberprzestrzeni jest zadaniem trudnym, anonimowość działań w tym obszarze jest cechą atrakcyjną dla wszelkich działań o prowokacyjnym i dezinformacyjnym charakterze. Wobec trudności z ustaleniem źródeł ataków w cyberprzestrzeni agresor ostatecznie nie ponosi odpowiedzialności.

Cyberataki poprzedzające rosyjskie działania militarne

Rosyjskie działania militarne rozpoczęte 24 lutego zostały poprzedzone cyberatakami o ograniczonym zasięgu wymierzonymi w Ukrainę, przede wszystkim skierowanymi w serwisy internetowe administracji publicznej (tzw. ataki DDoS – ang. distributed denial of service, rozproszona odmowa usługi) oraz rozmieszczaniem złośliwego oprogramowania niszczącego dane (tzw. wiper). Pierwszy atak, do którego doszło 14 stycznia, wymierzony został w oficjalne serwisy administracji publicznej, portal Ministerstwa Oświaty, Ministerstwa Spraw Zagranicznych, Ministerstwa Energetyki, strony rządowe, w tym aplikacji „Dija" oraz Państwowej Służby ds. Sytuacji Nadzwyczajnych. W wyniku przeprowadzonego ataku nie uległa zmianie zawartość stron internetowych, nie doszło również do

ujawnienia danych osobowych, pokłosiem ataku były prowokacyjne komunikaty wyświetlane na głównych stronach atakowanych witryn.

W połowie lutego doszło do kolejnego rosyjskiego ataku na ukraińskie podmioty działające w kluczowych sektorach, m.in. energetycznym, telekomunikacyjnym i transportowym. Ataki DDoS skierowane zostały przeciwko ukraińskiemu Ministerstwu Obrony Narodowej i bankom państwowym, w jego wyniku zakłóceniu uległy witryny internetowe Ministerstwa Obrony oraz Sił Zbrojnych Ukrainy, zablokowano także usługi mobilne banków państwowych, PrivatBanku, Oszczadbanku i Sbierbanku. Wstrzymano również wypłaty gotówki z bankomatów.

Atak przeprowadzony 15 lutego służby Ukrainy określiły jako największy w historii tego kraju. Za inicjatorów obu cyberataków Ukraina uznała Federację Rosyjską. Przypuszczenia te potwierdziły ustalenia amerykańskich analityków twierdzących, że głównym celem przeprowadzonych ataków cybernetycznych była destabilizacja ukraińskiego społeczeństwa. Podczas konferencji prasowej Białego Domu 18 lutego doradczyni prezydenta Joe Bidena ds. cyberbezpieczeństwa nowych technologii, Anne Neuberger poinformowała o wiarygodnych dowodach potwierdzających informacje, zgodnie w którymi za ataki wymierzone w ukraińskie Ministerstwo Obrony Narodowej i państwowe banki odpowiedzialność ponosi Kreml. Na podstawie obserwacji infrastruktury Głównego Zarządu Wywiadowczego (GRU), transmitującej znaczne ilości danych do adresów IP zlokalizowanych w Ukrainie, wskazano na tę organizację jako autora obu ataków. Neuberger oceniła, że atak DDoS, którego celem było przeciążenie i zablokowanie usług online ukraińskich instytucji nie spowodował zamierzonych, rozległych szkód, co było wynikiem szybkiej reakcji Ukrainy i wsparcia udzielonego przez USA.

Kolejny incydent cybernetyczny związany z atakiem DDoS miał miejsce w przeddzień inwazji rosyjskiej, 23 lutego. Rosja zaatakowała ukraińskie portale internetowe, w tym wiele stron państwowych oraz internetowych serwisów ukraińskich instytucji państwowych. Wydarzenia ta bezpośrednio poprzedzały działania militarne.

Cyberataki jako element działań wojennych

Od początku działań zbrojnych podjętych w Ukrainie cyberprzestrzeń stała się istotną domeną działań wojennych. Zgodnie z informacjami przekazanymi przez izraelską firmę Checkpoint w okresie 24-27 lutego 2022 roku liczba cyberataków wymierzonych w ukraińskie instytucje polityczne i wojskowe wzrosło o 196 procent.

Obszarami najbardziej narażonymi na ataki hakerskie jest sektor publiczny, finansowy oraz infrastruktura krytyczna. Kluczowym celem rosyjskich działań ofensywnych prowadzonych w cyberprzestrzeni jest doprowadzenie do sparaliżowanie funkcjonowania zaatakowanej infrastruktury teleinformatycznej.

Na początku marca celem rosyjskiego ataku była firma telekomunikacyjna Triolan. Doszło w niej do włamania, w wyniku którego zresetowano niektóre systemy wewnętrzne, czego konsekwencją była utrata dostępu przez niektórych lokalnych abonentów. Na początku kwietnia Microsoft poinformował, że w ostatnich dniach udało mu się powstrzymać cyberatak prowadzony przez rosyjskich hakerów, który był wymierzony przeciwko celom w Ukrainie, dokładnie grupy o nazwie APT28, wspieranej finansowo przez rosyjski rządu i powiązanej z grupą wywiadowczą GRU. Wśród celów ataku znajdowały się serwery powiązane z ukraińskimi instytucjami rządowymi oraz mediami. Powstrzymanie ataku rosyjskich hakerów było możliwe dzięki przejęciu siedmiu domen internetowych, które były wykorzystywane do przeprowadzania cyberataków. Zostały one skierowane do centrów obsługi Microsoftu, co doprowadziło do znacznego ograniczenia pola manewru w kontekście prowadzonej ofensywy.

Według oficjalnych danych od 15 lutego Ukraina była celem około 2,8 tysięcy cyberataków. 6 marca odnotowano rekordową liczbę 271 ataków DDoS. Rosjanie wykorzystują szeroki wachlarz matod, aby sparaliżować funkcjonowanie kluczowych instytucji dla funkcjonowania państwa ukraińskiego, zwłaszcza w obszarze prowadzenia operacji obronnej przez Ukrainę. Za przykład może posłużyć próba kompromitacji przez rosyjskie służby aplikacji wykorzystywanych do sterowania ukraińską artylerią. Takie działanie można również wykorzystać do pozyskania współrzędnych położenia geograficznego i lokalizacji konkretnych obiektów, aby następnie je zbombardować.

Istotne z punktu widzenia eskalacji działań w cyberprzestrzeni mogą być skutki sankcji gospodarczych nałożonych na Federację Rosyjską. Hakerzy, zwłaszcza wyspecjalizowani w atakach ransomware, jak rosyjska grupa #Conti, mogą dążyć do finansowego odwetu na zachodnich podmiotach. Szczególnie niepokojące w tej perspektywie byłyby ataki APT (Advanced Persistent Threats) skierowane na infrastrukturę krytyczną oraz systemy automatyki przemysłowej. Równie groźnym scenariuszem byłyby ataki na globalną infrastrukturę cyfrową, w tym światłowody czy też protokoły typu BGP (Border Gateway Protocol) czy DNS (Domain Name System), które mogą wywołać bardzo poważne zakłócenia dla funkcjonowania Internetu. Zdolności do zaawansowanych ataków aplikacyjnych ma z pewnością

Rosja i Chiny, ale także sojusznicy Ukrainy, w tym zwłaszcza USA, które jako pierwsze w 2010 roku użyło zaawansowanej cyberbroni o nazwie Stuxnet przeciwko Iranowi, a później także rosyjskiej agencji dezinformacyjnej Internet Research Agency.

Powyższe przesłanki wskazują, że cyberataki użyte w wojnie rosyjsko-ukraińskiej mogą osiągnąć bezprecedensową skalę w historii, wspierając rosyjskie działania militarne. W konsekwencji cyberwojna może przyczynić się do przechylenia szali zwycięstwa na jedną ze stron konfliktu, ponieważ ataki cyfrowe mogą mieć bardzo konkretny wpływ na jej przebieg.

Szanse Ukrainy

W zakresie operacji informacyjnych prowadzonych w cyberprzestrzeni Federacja Rosyjska posiada przewagę nad Ukrainą. Wynika ona chociażby z doświadczenia Kremla w działaniach podejmowanych w tym obszarze, ponadto dysponuje niezbędną infrastrukturą. Moskwa posiada również jedne z bardziej zaawansowanych zdolności cyberofensywnych na świecie. W przeszłości Federacja Rosyjska przeprowadzała już działania tego typu, chociażby w 2007 roku przeciwko Estonii, w 2008 roku przeciwko Gruzji i Ukrainie w 2014 roku.

Szczególnie ważne są tu doświadczenia zebrane w walkach prowadzonych o Krym i Donbas. Federacja Rosyjska przeprowadziła w Ukrainie swoisty poligon, na którym testowała użycie ataków na obiekty infrastruktury krytycznej. W konsekwencji Ukraina doświadczyła m.in. kilkugodzinnego przerwania dostaw energii elektrycznej, a w 2017 roku była pierwszą ofiarą złośliwego oprogramowania NotPetya, jak dotąd najbardziej destrukcyjnego, rozległego i kosztownego cyberataku w historii świata, dotyczącego tysiąca firm i instytucji. W 2007 roku Federacja Rosyjska przeprowadziła atak cyfrowy na infrastrukturę w Estonii, w wyniku którego Sojusz Północnoatlantycki zainicjował zmiany, zarówno organizacyjne, jak i polityczne. W 2008 roku przyjęto pierwszą politykę NATO w dziedzinie cyberobrony. W 2014 roku podczas szczytu NATO w Walii zdecydowano, że zastosowanie artykułu 5 Traktatu Waszyngtońskiego dotyczy również przypadku poważnego cyberataku na jedno z państw sojuszniczych. Podczas Szczytu NATO w Warszawie w 2016 roku członkowie Sojuszu uznali przestrzeń cybernetyczną za obszar działań zbrojnych i w większym stopniu zobowiązali się do wzmacniania cyberobrony w odniesieniu do swoich krajowych sieci i infrastruktury oraz traktowania jej jako priorytet.

Ukraina nie jest bezbronna. Wyciągnęła nauczkę z zarówno z 2014 roku, jak i

kolejnych ataków z 2015 i 2016 roku na infrastrukturę energetyczną, ale przede wszystkim ze wspomnianej NotPetya z 2017 roku. Ponadto nie jest w swoich działaniach osamotniona. Po stronie Ukrainy opowiedzieli się haktywiści Anonymous oraz grupy hakerskie GNG (Georgian Hackers Society) i NB65 (Network Battalion 65). Hakerzy z grupy Anonymous dokonali ataku na szereg rosyjskich portali internetowych, m.in. rządowych, telewizji Russia Today oraz Gazpromu. Ponadto pozyskali poufne dane ministerstwa obrony Federacji Rosyjskiej oraz białoruskiej firmy Tetraedr, producenta uzbrojenia wspierającego Federację Rosyjską. W ciągu zaledwie tygodnia członkowie Anonymous pozyskali i upublicznili dane pracowników rosyjskiego Ministerstwa Obrony Narodowej, usunęli witryny strony większości ministerstw rządowych oraz instytucji państwowych, dokonali blokady białoruskich banków i doprowadzili do czasowego wstrzymania dostaw gazu ziemnego na terenie Federacji Rosyjskiej. Grupa zablokowała ogółem około 300 stron.

Skuteczne działania podejmowane przez grupę „Anonymous” mogą mieć znaczenie propagandowe, jednak analitycy z grupy IT Herpig poddają w wątpliwość, czy rosyjscy decydenci będą pod wrażeniem podejmowanych działań. Jednocześnie zwracają uwagę, że aktywność hakerów stanowi również źródło potencjalnych niebezpieczeństw, polegających chociażby na wyprzedzającym ostrzeganiu Federacji Rosyjskiej przed istniejącymi lukami w systemie zabezpieczeń internetowych, które dostrzeżone zostały przez zachodni lub ukraiński wywiad.

W zakresie zabezpieczeń w obszarze cyberataków Ukraina dodała do swych zasobów prowadzoną przez rząd IT Army, złożoną z ukraińskich firm technologicznych oraz cyberspecjalistów. Celem działania instytucji ma być odciążenie ukraińskich służb, poprzez niesienie pomocy w ochronie infrastruktury krytycznej oraz przeprowadzaniu misji cyberszpiegowskich przeciwko rosyjskim wojskom. Taka aktywność ukraińska jest bezprecedensowa. Według analityczki francuskiej firmy Sekoia, Livii Tibirny, ukraińska IT Armia zrekrutowała do swoich szeregów prawie 260 000 osób. Eksperci ostrzegają jednak, że aktywność taka mogą mieć również negatywne skutki. Podejmowane działania mogą doprowadzić do uszkodzenia infrastruktury ważnych instytucji państwowych lub sprowokować kontratak strony przeciwnej. Ponadto może dochodzić do aktów łamania prawa.

W działania na rzecz pomocy dla Ukrainy w obszarze cyber zaangażowały się również zagraniczne podmioty. Elon Musk na prośbę władz w Kijowie udostępnił usługi łączności satelitarnej dla Ukrainy, zabezpieczając obywateli przed niebezpieczeństwem utraty kontaktu ze światem. Prywatne firmy wykonują i dostarczają do Kijowa zdjęcia satelitarne wojsk rosyjskich, pozwalających szybciej i

dokładniej zlokalizować umiejscowienie wojsk rosyjskich. Ministerstwo Cyfryzacji Ukrainy pozyskało również dotacje w kryptowalucie w ramach programu crowdfundingu w wysokości około 8 milionów dolarów.

I choć należy podkreślić, że cyberataki charakteryzuje ograniczenie w obszarze fizycznych konsekwencji, jednak mogą one w sposób wymierny wpłynąć na ostateczny wynik wojny. Należy więc dążyć do wzmacniania zdolności obronnych Kijowa w tym zakresie.

Wnioski

Tocząca się obecnie wojna rosyjsko-ukraińska zapisze się w historii jako konflikt, który zmienił architekturę bezpieczeństwa współczesnego świata. Będzie również pierwszą wojną z tak kluczowym znaczeniem wymiaru cyfrowego. Rozszerzenie teatru wojny na domenę cyberprzestrzeni, geopolityczne znaczenie użytych w niej technologii cyfrowych oraz rosnące znaczenie firm technologicznych są dostrzegalne w wielu jej aspektach.

Sytuacja w cyberprzestrzeni eskaluje. Nie jest to wyłącznie wynikiem aktywności kolejnych grup hakerskich, opowiadających się po przeciwnych stronach konfliktu, jak chociażby odpowiedzialna za przeprowadzenie ataków ransomware rosyjska grupa #Conti oraz grupa hackerska Anonymous, która wypowiedziała wojnę cyfrową reżimowi Putina i konsekwentnie atakuje rosyjskie strony internetowe i bazy danych rosyjskich instytucji państwowych.

Platformy wykorzystywane do dezinformacji znajdują się przede wszystkim w posiadaniu korporacji technologicznych, co w obecnej sytuacji wymaga od nich zdecydowanej reakcji na agresywne działania inicjowane przez reżim Władimira Putina. Rozwiązania technologiczne zachodnich firm stały się arsenałem w ramach pakietu zachodnich sankcji, które mają powstrzymać Federację Rosyjską przed eskalacją działań wojennych i pogrzebać jej możliwość rozwoju w erze cyfrowej.

Dalsze ataki, podejmowane zarówno przez służby rosyjskie, jak również pośredników działających z polecenia Moskwy (proxies) oraz prawdopodobieństwo ich niekontrolowanej proliferacji z Ukrainy na inne regiony są niewykluczone i w perspektywie krótkoterminowej przyczyniać się mogą do dalszej destabilizacji sytuacji międzynarodowej.

Źródła:

Źródła:

Army of Cyber Hackers Rise Up to Back Ukraine; https://www.securityweek.com/army-cyber-hackers-rise-back-ukraine.

Cyber Attack Trends In The Midst of Warfare – The numbers behind the first days of the conflict; https://blog.checkpoint.com/2022/02/27/196-increase-in-cyber-attacks-on-ukraines-government-and-military-sector/.

Cyber Warfare: A multidisciplinary analysis, ed. J. Green, Routledge Taylor & Francis Group, London, New York 2015. Gengler B., Super-hacker Kevin Mit.

https://directionsblog.eu/ukraine-cyber-operations-and-digital-technologies/.

Izabela Albrycht, Rozpoczyna się globalna cyberwojna; https://cyfrowa.rp.pl/opinie-i-komentarze/art35773131-rozpoczyna-sie-globalna-cyberwojna.

Press Briefing by Press Secretary Jen Psaki, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, and Deputy National Security Advisor for International Economics and Deputy NEC Director Daleep Singh, February 18, 2022; https://www.whitehouse.gov/briefing-room/press-briefings/2022/02/18/press-briefing-by-press-secretary-jen-psaki-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-and-deputy-national-security-advisor-for-international-economics-and-dep/.

S. Herpig, Ukraine cyber operations and digital technologies; https://directionsblog.eu/ukraine-cyber-operations-and-digital-technologies/

Thomas Brewster, As Russia Invaded, Hackers Broke Into A Ukrainian Internet Provider. Then Did It Again As Bombs Rained Down; https://www.forbes.com/sites/thomasbrewster/ 2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/

Winterfeld S., Andress J., The Basics of Cyber Warfare, Elsevier, Amsterdam, Boston,

Heidelberg, London, New York, Oxford, Paris, San Diego, San Francisco, Singapore, Sydney, Tokyo 2013.

Materiał pobrany ze strony Instytutu Sobieskiego, sobieski.org.pl, autor: dr Agnieszka Rogozińska.