Komentarz KBN

Nr 1 (104) / 2023 19 stycznia 2023 r.

Rola cyberprzestrzeni w konfliktach międzynarodowych. Wstępne wnioski z rosyjskich działań podczas wojny z Ukrainą[1]

Błażej Sajduk

Wojna Rosji z Ukrainą w swojej „gorącej" fazie trwa już od 2014 roku. Nie ulega wątpliwości, że ten krwawy konflikt stanowi źródło wniosków na temat przebiegu militarnej rywalizacji w następnych dekadach XXI wieku. Pierwsza odsłona tej wojny sprowokowała wiele obserwacji związanych z tzw. hybrydowym sposobem prowadzenia działań militarnych, a także potwierdziła rolę, jaką systemy bezzałogowe będą pełnić w siłach zbrojnych. Aktualna faza konfliktu, trwająca od 24 lutego 2022 roku, pozwala sformułować kolejne wnioski istotne dla przyszłości działań wojennych, w tym zwłaszcza roli cyberprzestrzeni.

Analitycy i komentatorzy wiele miejsca poświęcili kontekstowi geopolitycznemu oraz działaniom konwencjonalnym, przesuwając na dalszy plan uwagi dotyczące znaczenia działań w cyberprzestrzeni. W poniższym tekście autor chciałby się skupić na roli cyberprzestrzeni w aktualnej fazie tego konfliktu, zwłaszcza że rywalizacja dotyczy podmiotów o bardzo rozwiniętych zdolnościach w tej domenie. Warto w tym miejscu przypomnieć, że według *National Cyber Power Index 2022*

[1] Publikacja powstała w ramach realizacji grantu „Rola działań w cyberprzestrzeni dla państw porozumienia Pięciorga Oczu w świetle konfliktu rosyjsko-ukraińskiego" finansowanego przez Wydział Studiów Międzynarodowych i Politycznych UJ na rozwój trwałej interdyscyplinarnej współpracy badawczej, realizowanego w ramach Działania nr 3 (R2R – współpraca badawcza) w ramach programu strategicznego Inicjatywa Doskonałości w Uniwersytecie Jagiellońskim.

Ukraina została sklasyfikowana na drugim miejscu pod względem zdolności cyberobrony, podczas gdy Rosję uznano za drugi kraj o największych możliwościach ofensywnych w domenie cyber.

Na wstępnie należy poczynić dwa zastrzeżenia. Po pierwsze, parafrazując Clausewitza, „mgła wojny" jest szczególnie „gęsta" gdy obejmuje informacje dostępne na temat działań w cyberprzestrzeni. Działania dezinformacyjne prowadzone przez strony zaangażowane w konflikt utrudniają ustalenie stanu faktycznego, ponadto prywatne podmioty zajmujące się cyberbezpieczeństwem realizują własną agendę, która często może wpływać na wybór zagadnień przedostających się do sfery publicznej. Mając świadomość tych ograniczeń, poniżej formułowane spostrzeżenia opierają się na jawnych informacjach pojawiających się w domenie publicznej. Po drugie, ponieważ wojna toczy się pomiędzy dwoma podmiotami państwowymi, wnioski formułowane na podstawie jej przebiegu mogą się odnosić zarówno do rosyjskiego sposobu prowadzenia działań wojennych w cyberprzestrzeni, jak też mogą dawać asumpt do sformułowania wniosków o bardziej ogólnym charakterze.

Rosyjski sposób wykorzystania cyberprzestrzeni w trakcie działań wojennych

Charakteryzując strategiczne uwarunkowania rosyjskich działań w cyberprzestrzeni, należy wskazać, iż Rosja wciąż nie utworzyła jednego centralnego cyberdowództwa, struktury która koordynowałoby cyberoperacje realizowane przez Federalna Służbę Bezpieczeństwa (FSB), Służbę Wywiadu Zagranicznego (SWR), Główny Zarząd Wywiadu (GRU) oraz podmioty prywatne. Zdaniem wielu ekspertów, jest to jeden z powodów mało spektakularnych działań ofensywnych w cyberprzestrzeni towarzyszących inwazji sił lądowych.

Ponadto w oficjalnych dokumentach dotyczących międzynarodowego bezpieczeństwa informacyjnego oraz w doktrynie bezpieczeństwa informacyjnego Federacja Rosyjska kładzie szczególny nacisk na dominację informacyjną oraz działania psychologiczne. Mniej akcentowana jest rola działań ofensywnych w cyberprzestrzeni, które charakteryzowano głównie jako element tzw. „aktywnej obrony", czyli katalogu działań poniżej progu wojny. Przykładami mogą być np. przypisywane rosyjskim podmiotom operacje informacyjne, w tym m.in. ingerowanie w wybory prezydenckie w USA w 2016 roku czy brytyjską kampanię dotyczącą opuszczenia Unii Europejskiej. Innym przykładem zaawansowanej cyberoperacji o charakterze wywiadowczym było zainfekowanie w 2020 roku oprogramowania tworzonego przez firmę SolarWinds, w rezultacie czego poważnie naruszono bezpieczeństwo kilku amerykańskich agencji federalnych oraz kilkunastu tysięcy największych przedsiębiorstw na świecie. Wznowienie „gorącej" fazy wojny z Ukrainą przełożyło się również na działania Rosji w cyberprzestrzeni.

24 lutego 2022 roku, w dniu, w którym Władimir Putin publicznie poinformował o rozpoczęciu tzw. wojskowej „operacji specjalnej" przeciwko Ukrainie, przeprowadzono cyberatak na infrastrukturę dostawcy łączności internetowej amerykańskiej firmy Viasat, z której usług korzystała ukraińska armia. Był to przykład ofensywnego wykorzystania cyberprzestrzeni do osłabienia zdolności przeciwnika. Doniesienia medialne wskazują, iż łączność specjalna sił zbrojnych Ukrainy została ograniczona na kilka lub kilkanaście dni (efektem ataku było również odcięcie łączności niemieckiej firmy Enercon z jej farmami wiatrowymi na Bałtyku). Należy jednak podkreślić, iż

atak ten jest jak dotąd jedynym poważnym i potwierdzonym działaniem w cyberprzestrzeni, które stanowi ekwiwalent ataku kinetycznego – z poziomu sieci Internet udało się, za pośrednictwem szkodliwej aktualizacji oprogramowania, wpłynąć na funkcjonowanie infrastruktury w świecie fizycznym. Z tego powodu wielu ekspertów wyraża rozczarowanie, a wręcz kwestionuje zasadność uznania cyberprzestrzeni za piątą domenę prowadzenia działań wojennych. Tym niemniej Rosja w trakcie działań w czterech klasycznych domenach uzupełniała je operacjami w cyberprzestrzeni, dostosowując wykorzystywaną taktykę do realiów „gorącego konfliktu".

Zmianę wywołaną przejściem w tryb wojenny bardzo dobrze widać na przykładzie cyberataków przeprowadzanych przez GRU (grup znanych jako UNC2589 i APT29). O ile uprzednio koncentrowano się na działaniach wywiadowczych i pozyskiwaniu informacji, to wraz z rozpoczęciem inwazji dominującą wrogą aktywnością stało się wykorzystywanie wiperów (szkodliwego oprogramowania, którego celem jest uszkadzanie lub wymazywanie danych w zainfekowanych systemach). Przez około cztery miesiące od rozpoczęcia inwazji systemy teleinformatyczne ukraińskich agencji rządowych oraz przedsiębiorstw zostały zaatakowane przez osiem rodzin szkodliwego oprogramowania. Biorąc pod uwagę fakt, iż między 2012 a 2020 rokiem wykryto łącznie osiem rodzin tego typu oprogramowania, to ilość użytych przez Rosjan środków jest znacząca – połowa ze znanych wiperów została wykorzystanego podczas czterech miesięcy tzw. „operacji specjalnej". By podtrzymać inicjatywę Rosjanie zwielokrotnili tempo i agresywność cyberataków, nieustannie ponawiając je na wybrane cele (głównie instytucje rządowe). Próby wykorzystania nieuprawnionego dostępu do systemu ofiary następowały dużo szybciej, niż miało to miejsce przed 24 lutego, zamiast miesięcy były to dni lub tygodnie. Do przeprowadzania wrogich działań wykorzystywano te same odmiany wiperów, jednak by zachować skuteczność działań za cel zaczęto obierać wszystkie dostępne urządzenia znajdujące się na krawędzi sieci (firewalle, routery i serwery), a nie jak wcześniej starannie wyselekcjonowane urządzenia, za pomocą których infiltrowano sieć ofiary. Struktura kodu wspominanego szkodliwego oprogramowania wskazuje, że było one kompilowane niedługo przed rozpoczęciem inwazji. Sugeruje to chęć osiągnięcia możliwie dużej skali ataków, pozostawiając poziom ich zaawansowania na dalszym miejscu. Po pierwszej, intensywnej fazie cyberataków nastąpiło ich znaczne ograniczenie oraz zmiana jakościowa (wzrost liczby znacznie mniej wysublimowanych ataków phishingowych i DDoS). Brak też informacji o nowych odmianach szkodliwego oprogramowania. Najprawdopodobniej to wynik tego, iż obrońcy nauczyli się skutecznie przeciwdziałać rosyjskim cyberatakom oraz faktu, iż Rosja wyczerpała swój potencjał cyberofensywny (sugeruje to ponowne wykorzystywanie domen użytych już wcześniej do zdalnej kontroli szkodliwego oprogramowania).

Kwestią budzącą największe wątpliwości pozostaje poziom koordynacji rosyjskich działań we wszystkich domenach. Pewne jest natomiast to, że nawet jeśli byłyby one wysoce skoordynowane, to dla ogólnego przebiegu wojny rola działań w cyberprzestrzeni była do tej pory ograniczona.

Wojna w Ukrainie potwierdza, że efekty ofensywnych działań w cyberprzestrzeni można z nie mniejszą skutecznością osiągać środkami konwencjonalnymi, w tym zwłaszcza bronią dalekiego zasięgu. W trakcie „gorących" działań wojennych aterytorialność, problematyczność przypisania odpowiedzialności oraz zdolność do dezorganizowania zhackowanych systemów, czyli więk-

szość cech przypisywanych specyfice działań w cyberprzestrzeni, tracą na znaczeniu. Aterytorialność łączona z działaniami w cyberprzestrzeni bez problemu jest osiągana przez broń rakietową – całe terytorium Ukrainy jest ofiarą rosyjskich ataków rakietowych. Rosjanie rażą cele na terytorium całej Ukrainy. W samej tylko pierwszej fazie operacji (między lutym a końcem czerwca 2022 r.) Rosja przeprowadziła w przybliżeniu 3654 ataki rakietowe oraz około 796 ataków cybernetycznych, przy czym efekty tych pierwszych dużo łatwiej potwierdzić. Utrudniona atrybucja straciła znaczenie w chwili, kiedy obie strony nie kryją już wrogich wobec siebie zamiarów, a zdolność do dezorganizowania i wywoływania paniki dużo efektywniej osiągnięto za pomocą broni konwencjonalnej dalekiego zasięgu (np. atakując infrastrukturę elektroenergetyczną lub cywilną).

Wnioski dla przyszłej roli cyberprzestrzeni w konflikcie zbrojnym

Dotychczas upubliczniane informacje jednoznacznie wskazują, że w trakcie działań wojennych poważne rosyjskie ataki informatyczne były nieliczne. W przeważającej liczbie nie stanowiły ekwiwalentu ataku kinetycznego (np. uszkadzając infrastrukturę), nie ma również jednoznacznych dowód potwierdzających ich skoordynowanie z działaniami konwencjonalnymi. W chwili obecnej bez odpowiedzi pozostaje pytanie, czy gdyby siły zbrojne Federacji Rosyjskiej posiadały dowództwo koordynujące działania ofensywne w cyberprzestrzeni dotychczasowy obraz wojny uległby zmianie.

Dynamika rosyjskich cyberataków oraz spadek ich jakości wskazują, że siły zbrojne rozbudowujące komponent cybernetyczny muszą poważnie przemyśleć decyzje o rozwijanym potencjale. Intensywna cyberwojna jest nie mniej wyczerpująca od działań konwencjonalnych i tak samo wymaga odnawiania zdolności do przeprowadzania ataków. Wydaje się to szczególnie aktualne w kontekście państw średnich, takich jak Polska, która buduje własny potencjał Wojsk Obrony Cyberprzestrzeni. Przebieg działań w Ukrainie pokazuje, iż w sytuacji, w której zasoby są ograniczone priorytet powinny mieć zdolności defensywne i wywiadowcze.