Instytut Europy Środkowej

Komentarze IEŚ

Redakcja: Beata Surmacz (dyrektor IEŚ), Tomasz Stępniewski (z-ca dyrektora IEŚ), Agnieszka Zajdel (sekretarz redakcji), Aleksandra Kuczyńska-Zonik, Jakub Olchowski, Konrad Pawłowski, Agata Tatarenko

Nr 553 (65/2022) | 09.03.2022

ISSN 2657-6996

Piotr Borkowski*

Operacje w cyberprzestrzeni – informacja, dezinformacja, działania ofensywne

Zarówno tuż przed działaniami wojennymi prowadzonymi przez Rosję na terytorium Ukrainy, jak i równolegle do nich rozpoczęła się bardzo szeroka operacja w cyberprzestrzeni. Łączy ona w sobie działania dezinformacyjne, propagandę, działania dywersyjne oraz operacje ofensywne. Jej skala i złożoność powodują, że duża część środowiska ekspertów, komentatorów i dziennikarzy mylnie interpretuje sytuację, wychwytując „najłatwiejsze" elementy i powielając informacje o nich, czym *de facto* hiperbolizuje efekty wskazanej operacji.

Powody. Skala operacji jest znacząca w związku nie tylko z bardzo szerokim wykorzystaniem różnych technik, ale również zaangażowaniem olbrzymich zasobów oraz globalnym teatrem działań. O ile działania militarne są skoncentrowane na terytorium Ukrainy, o tyle operacje w cyberprzestrzeni są prowadzone w wielu krajach, m.in. w Rosji, Ukrainie, Polsce, ale także w Stanach Zjednoczonych czy innych państwach należących do NATO. Należy zwrócić uwagę na różnice w celach, które inicjatorzy chcą osiągnąć w zależności od kraju. W Rosji dąży się do osiągnięcia pełnej kontroli nad przepływem informacji, tak aby społeczeństwo nie miało możliwości uzyskania wiarygodnych wiadomości na temat tego, co się dzieje na świecie. W Ukrainie jednym z celów operacji jest obniżenie morale żołnierzy ukraińskich oraz degradacja – i tak już nadwyrężonej przez toczącą się wojnę – odwagi ludności cywilnej (Ukraina również prowadzi intensywne działania informacyjne, aby temu przeciwdziałać). Analizując natomiast sytuację w Polsce, należy zauważyć, że tu powodem działań dezinformacyjnych jest destabilizacja wewnętrzna (społeczna) kraju jako frontowego NATO oraz najbardziej zaangażowanego w pomoc Ukrainie, a celem – obniżenie tak oceny działań Polski na arenie międzynarodowej, jak i motywacji (na poziomie społecznym i politycznym) do niesienia pomocy Ukrainie. Analogicznie jak np. w USA, działania w sferze dezinformacyjnej koncentrują się na hiperbolizacji niechęci opinii publicznej do niesienia pomocy Ukrainie.

Przykłady działań. Na wstępie należy zaznaczyć, że pomimo tego, że Federacja Rosyjska w zdecydowanej mierze przewodzi większości operacji o charakterze dezinformacyjnym i propagandowym, to jednak nie jest jedynym państwem, które te techniki stosuje – inne kraje stosują je niejako w reakcji/odpowiedzi. To dodatkowo komplikuje możliwość oceny dostarczanych informacji. Nawet środowisko ekspertów zajmujących się tą problematyką ma niekiedy wątpliwości co do faktycznej oceny niektórych przekazów, a to świadczy o skuteczności i jednocześnie skali „szumu" informacyjnego, z jakim mamy do czynienia. Poniżej przedstawionych zostanie kilka przykładów takich działań wraz z ich następstwami.

Rasizm na granicy polsko-ukraińskiej: na początku kampanii dezinformacyjnej publikowano informacje o niechęci polskiej Straży Granicznej do uchodźców o innym pochodzeniu etnicznym niż Ukraińcy (złe traktowanie oraz problem z wpuszczaniem do kraju). To działanie miało prawdopodobnie wywrzeć presję polityczno-społeczną na funkcjonariuszach, aby z mniejszą starannością weryfikowali dokumenty przyjezdnych. Kolejnym etapem była kampania informacyjna na temat tego, że uchodźcy o innym pochodzeniu etnicznym niż Ukraińcy dopuszczają się szeregu przestępstw w przygranicznych miejscowościach i terroryzują społeczeństwo. Do tego doszła inspirowana „ustawka" tzw. „kiboli", którzy dopuścili się niezgodnych z prawem działań, dzięki czemu kolejna próba dezinformacji nabrała rozpędu. Celem obu tych akcji była degradacja opinii o Polsce w oczach środowiska międzynarodowego oraz skłócenie społeczeństwa w Polsce. Ten drugi cel udało się na jakiś czas osiągnąć, co było dodatkowo podsycane przez dziennikarzy i polityków wielu opcji, czym niejako przyczynili się oni do hiperbolizacji wpływu na stan społeczny w Polsce. Po kilku dniach ukazała się informacja o ujęciu

w Przemyślu przez ABW osoby mającej być oficerem GRU, co też pokazuje, że działania informacyjne i dezinformacyjne mogą mieć bezpośrednie przełożenie na fizyczną dywersję i „inspirację" niektórych środowisk.

„Antyszczepionkowiec" = „ruski troll": jedna z prywatnych firm zajmujących się mediami przekazała informację, że wiele kont, z których płynie dezinformacja, to konta wcześniej upowszechniające wątpliwości dotyczące szczepień na COVID-19. O ile intencja (potencjalnie) była dobra, o tyle zestawienie tych dwóch informacji w danym momencie nie miało żadnej wartości analitycznej i doprowadziło do dużych tarć na portalach społecznościowych. W późniejszym dyskursie wiele osób używało określeń typu „ruski troll" lub „ruska onuca" wobec zwykłych ludzi, aby podbić emocjonalny przekaz. Wielu dziennikarzy i polityków bardzo szybko zaczęło powielać te stereotypy, czym – po raz kolejny – przyczyniło się do częściowego sukcesu kampanii, której celem była próba destabilizacji społeczeństwa. Dodatkowo należy wspomnieć, że takie operacje mają na celu wielowektorowy przekaz i zazwyczaj konta budowane na ich potrzeby prezentują skrajnie przeciwstawne poglądy. W przypadku COVID-19 część kont przedstawiała tzw. skrajne poglądy „antyszczepionkowe", a część – skrajne opinie wzmacniające strach związany z obowiązującym stanem pandemii, co służyło moderowaniu i podsycaniu społecznej polaryzacji.

Brak paliwa oraz gotówki: jedna z pierwszych akcji przeprowadzona w polskiej sieci. Wprowadzono do obiegu informacje, które wskazywały, że w Polsce zabraknie paliwa, a także gotówki w bankach, co (chwilowo) było również powielane przez duże portale informacyjne i doprowadziło do spirali paniki w społeczeństwie. Operacja okazała się skuteczna, choć na szczęście na krótko (na ok. dwa dni).

Cyberataki w Ukrainie: w Ukrainie przeprowadzono wiele operacji ofensywnych w cyberprzestrzeni. Rozpoczęły się one przed wejściem wojsk Federacji Rosyjskiej na jej terytorium. Jedna z wykorzystywanych metod to tzw. DDoS (Distributed Denial of Service), której celem było wykreowanie braku dostępności do wybranych usług, jak dostęp do stron rządowych czy usług bankowych (te drugie najdłużej były niedostępne przez ok. 4 godziny, później zaś powróciły do normalnego funkcjonowania). Podobna taktyka została wykorzystana w przypadku działań mających na celu aneksję Krymu w 2014 roku, a także przed militarną napaścią Federacji Rosyjskiej na Gruzję w roku 2008. Poza wskazanymi atakami DDoS uaktywniono również złośliwe oprogramowanie „HermeticWiper", którego głównym celem jest czyszczenie danych z zainfekowanych urządzeń. Pojawił się też „HermeticRansom", czyli malware, którego zadaniem jest szyfrowanie dysków zainfekowanych maszyn.

Chwilowy brak usług w Polsce: w ostatnim czasie odnotowano kilka ataków typu DDoS na niektóre banki, jednak były one bardzo szybko odpierane i nie powodowały zakłóceń w realizacji usług. 28 lutego br. opublikowano informację o problemach w dostępności usług niektórych dostawców usług telefonicznych oraz Internetu. Bardzo szybko podchwyciły to media społecznościowe – przekazywano coraz szerzej informację o tym, że Polska może być właśnie atakowana. Informację co prawda zdementowano, ale stała się jednak podstawą „histerycznej" reakcji użytkowników.

Działania niezależne: w związku z wojną w Ukrainie swoje zaangażowanie zadeklarowało m.in. Anonymous, jednoczące ludzi z całego świata, jak i znane grupy świata „cyber". Rozpoczęły się działania mające na celu pomoc Ukrainie. Zainicjowano ataki (blokowanie dostępności usług, kradzież danych itp.) przeciwko wybranym systemom w Federacji Rosyjskiej (strony rządowe, strony informacyjne, telewizje, Roskosmos itp.). Zaobserwować można również kontrofensywę grup wspierających Kreml. Działania tego typu niosą jednak ze sobą pewne ryzyko, ponieważ nie są skoordynowane, a celami ataków mogą być również krytyczne zasoby krajów, co może potencjalnie doprowadzić do niezamierzonych, negatywnych następstw. W sieci pojawiały się też informacje dla użytkowników niebędących specjalistami od cyberbezpieczeństwa, w których przekazywano im do zainstalowania „narzędzia" umożliwiające stanie się aktywnym elementem ofensywy przeciwko Rosji. Należy jednak pamiętać, że część tych informacji również może być działaniem dywersyjnym, którego twórcami mogą być ugrupowania prorosyjskie.

Konkluzje. Prowadzone aktualnie operacje w cyberprzestrzeni są wielowektorowe i zakrojone na globalną skalę. O ile działania ofensywne (cyberataki) skoncentrowane są głównie w Federacji Rosyjskiej oraz Ukrainie (gdzie dochodziło do chwilowo skutecznych ataków), o tyle należy pamiętać, że mamy do czynienia również

z operacjami ofensywnymi w innych krajach, aczkolwiek tam nie odnotowano ich znaczącego wpływu na funkcjonowanie instytucji publicznych i prywatnych.

Dużo większą skuteczność można zaobserwować w sferze wojny informacyjnej, gdzie przekazywanie informacji zarówno nieprawdziwych, jak i prawdziwych (jednak skonstruowanych w formie emocjonalnej) powoduje czasowe niepokoje społeczne, które w niektórych przypadkach przekładają się na świat realny. Szum informacyjny jest tak duży, że osoby niezajmujące się zawodowo tym zjawiskiem nie posiadają skutecznej metody weryfikacji otrzymywanych przekazów. Prowadzi to do konkluzji, że należy zachować wstrzemięźliwość w powielaniu informacji z niesprawdzonych źródeł, gdyż może się to przyczynić do hiperbolizacji operacji informacyjnej w Polsce. Wszelkie przejawy skrajnych opinii, nacechowanych emocjonalnie i ukazujących wycinek sytuacji mającej związek z agresją Rosji, można wstępnie traktować jako potencjalną próbę oddziaływania na społeczeństwo – intencjonalną lub powieloną.

Opinie wyrażone w publikacji prezentują wyłącznie poglądy autora i nie mogą być utożsamiane ze stanowiskiem Instytutu Europy Środkowej.

---

[*] **Piotr Borkowski** – autor komentarza gościnnego. Dyrektor ds. operacji Red Team oraz testów cyberbezpieczeństwa w jednym z międzynarodowych banków, były funkcjonariusz ABW w Rządowym Zespole Reagowania na Incydenty Komputerowe CERT.GOV.PL, wykładowca przedmiotów związanych z cyberbezpieczeństwem, m.in. na Uniwersytecie Warszawskim.