Andrzej Małkiewicz

27 kwietnia 2022

Trolle

W intencjach kierownictwa rosyjskiego wojna w 2022 r. miała mieć charakter hybrydowy, tj łączyć tradycyjne medody walki z nowatorskimi, przede wszystkim w obszarze Internetu.

Działania tradycyjne, mimo wyraźnej przewagi liczebnej, nie udały się Rosji. Do działań w sferze informacyjnej przygotowała się, jak sądził Putin, bardzo solidnie, a działania podjęto z dużym wyprzedzeniem. Szczególną rolę odegrali dwaj ludzie: Jewgienij Prigożyn (Евгений Пригожин) i Jewgienij Kasperski (Евгений Касперский).

Ten pierwszy wyspecjalizował się w realizowaniu zamówień publicznych rosyjskiego Ministerstwa Obrony, organizowaniu grup najemników wojskowych, określanych ogólnie jako „grupy Wagnera" i właściciel tzw. „fabryki trolli" w Petersburgu, która oficjalnie nazywa się Agencja Badań Internetowych (Агентство интернет-исследований).

Zajmuje się nie tyle badaniami, ile infekowaniem sieci.

Jest zaangażowana w interesie Rosji w operacje polegające na wywieraniu wpływu w Internecie. Jej zadaniem jest m.in. rozprzestrzenianie fałszywych informacji, wywoływanie skrajnie prawicowych postaw społecznych i politycznych oraz dezinformowanie zagranicznej opinii publicznej, przede wszystkim poprzez kwestionowanie demokratycznej legitymacji Unii Europejskiej i podejmowanie innych tematów „podgrzewających nastroje" i wywołujących konflikty. Dysponuje miesięcznym budżetem w wysokości ok. 1 mln euro i zatrudnia rotacyjnie ok. 80 osób. Szczególną formą działania jest sporządzanie postów i komentarzy pod wiadomościami na stronach internetowych. Zatrudnia też setki płatnych blogerów i komentatorów, piszących w duchu wygodnym dla Kremla, a czyniących wrażenie, że reprezentują opinię publiczną poszczególnych krajów. Ich zadania to krytyka opozycji rosyjskiej, polityki wewnętrznej i zagranicznej Ukrainy i Stanów Zjednoczonych.

Rozpowszechniali teorie spiskowe na temat sieci 5G, a po wybuchu pandemii regularnie przekazywali fake newsy na temat COVID-19, zamieszczali treści otwarcie podważające sensowność noszenia maseczek, zarzucali lekarzom kłamstwa i przekonywali, że pandemia nie istnieje, lub podawali w wątpliwość skuteczność szczepień – choć nadawali z różnych miejsc świata (w internecie to przecież nie problem). Nie udało się rosyjskim manipulantom sprawić śmierci na Covid-19 zbyt

wielu chorych poza granicami, ale rzeczywiście, liczba zaszczepionych wśród Ukraińców była niewielka, coś więc uzyskali.

21-22 lutego (a więc tuż przed rozpoczęciem rosyjskiej agresji) gwałtownie zmienili zainteresowania: zaczęli aktywnie promować treści prokremlowskie, antyukraińskie i antyuchodźcze. Motywami przewodnimi pojawiającymi się w postach stało się podjudzanie nastrojów poprzez nazywanie Ukraińców „banderowcami" lub „upowcami", obrażanie prezydenta Zełenskiego lub po prostu dokładne przekazywanie treści propagandowych Kremla. Niekiedy wręcz negowali istnienie narodu ukraińskiego, który „wymyślili" masoni (domyślamy się – by wyrządzić krzywdę Rosji, pozbawiając ją części narodu). Później m.in. otwarcie negowali bombardowania Ukrainy i zbrodnie na cywilach.

Decyzją z dnia 23 lutego 2022 r., a więc podjętą w przeddzień agresji, Rada Unii Europejskiej nałożyła na Agencję Badań Internetowych sankcje ze względu na prowadzenie kampanii dezinformacyjnych skierowanych przeciwko Ukrainie.

Kasperski to absolwent Wydziału Matematyki Wyższej Szkoły KGB, przekształconego później w Instytut Kryptografii, Telekomunikacji i Informatyki Akademii Federalnej Służby Bezpieczeństwa. W 1997 r. założył Kaspersky Lab (Лаборатория Касперского), dziś jest to międzynarodowa korporacja będąca jednym z największych światowych dostawców oprogramowania antywirusowego, zarejestrowana w Wielkiej Brytanii, ale z centralą w Moskwie. Antywirusowe oprogramowanie Kasperskiego otwierało jednocześnie dostęp do komputerów hakerom i agentom rosyjskiego wywiadu. Od 2017 r. oprogramowanie Kaspersky Lab jest zakazane w systemach federalnych USA. Aktualnie ostrzeżenia przed zagrożeniem stwarzanym przez produkty Kaspersky Lab zostały wydane również przez organy cyberbezpieczeństwa USA, Unii Europejskiej, Wielkiej Brytanii, Niemiec, Włoch, Holandii i Litwy. 26 kwietnia objęły firmę sankcje w Polsce.

24 lutego rosyjskie media zaczęły publikować i rozsyłać w różnych językach informacje o poddaniu się wojsk ukraińskich bez walki i ucieczce przywódców państwowych z kraju.

Podobnie jak na poziomie ataków lądowych i morskich służby ukraińskie nie zostały zaskoczone, podjęły skuteczne przeciwdziałanie. W ciągu dwóch miesięcy wojny zneutralizowały ponad 250 dużych cyberataków, wykryto kilkanaście farm botów i zablokowano 50 tys. kont, przy pomocy których w socialmediach publikowano treści korzystne dla najeźdźców. Chodzi m.in. o sieć anonimowych kanałów komunikatora Telegram i działające w portalach społecznościowych grupy wzywające do fizycznego zniszczenia narodu ukraińskiego.

Agresorzy sądzili, że „panują" nad Internetem, tymczasem okazało się, że sami mogą zostać zaatakowani. Międzynarodowa sieć hakerów Anonymous dokonywała włamań do kolejnych rosyjskich instytucji i firm, wykradając miliony maili i różnego

typu wrażliwych danych. Początkowo wydawało się, że będzie to druzgocące dla interesów Moskwy, jednak – jak przypuszczam – ilość pozyskanych informacji przerosła możliwości ich analizowania, a z samego faktu wykradzenia i udostępnienia chętnym na razie niewiele wynikło. Dopiero w przyszłości mogą być poważne konsekwencje.

W połowie kwietnia w Rosji wreszcie zrozumiano, jaką rolę w wojnie odgrywa komunikacja za pomocą udostępnionej Ukrainie przez Elona Muska sieci satelitów Starlink, zapewniająca dostęp do internetu. Korzystają z tej łączności głównie ukraińskie siły zbrojne oraz instytucje obsługujące elementy infrastruktury krytycznej. Podjęto próby zagłuszania sygnału. Akcja poniekąd się udała, w niektórych częściach kraju łączność została zagłuszona, ale tylko na kilka dni. Programiści SpaceX wkrótce opracowali skuteczną tarczę ochronną przeciwko rosyjskim działaniom elektromagnetycznym.

Sojusz Północnoatlantycki już dawno zdał sobie sprawę z potencjalnych zagrożeń i podjął przeciwdziałanie rosyjskiej dywersji w Internecie. Za jednego ze światowych liderów w dziedzinie cyberbezpieczeństwa i ochrony infrastruktury krytycznej przed cyberatakami uznawana jest Estonia. Już w 2007 r. padła ona ofiarą cyberataku. Unieruchomiono strony internetowe parlamentu, ministerstw obrony i sprawiedliwości, partii politycznych, policji i szkół. 9 maja, gdy Rosjanie świętują Dzień Zwycięstwa, hakerzy zaatakowali też przedsiębiorstwa prywatne, a dwa największe banki, Hansapank i SEB Ühispank, musiały zawiesić usługi on-line i wstrzymać transakcje zagraniczne. Liderzy estońscy, w porozumieniu z kierownictwem NATO, podjęli energiczne środki, by zabezpieczyć się na przyszłość przed podobnymi atakami.

W 2008 r. w Tallinie utworzono Centrum Doskonalenia Cyberobrony NATO (NATO Cooperative Cyber Defense Centre of Excellence). Jego misją jest zwiększenie zdolności do współpracy i wymiany informacji pomiędzy państwami członkowskimi Sojuszu i partnerami w dziedzinie cyberobrony. Centrum prowadzi m.in. analizę strategiczną trendów w zakresie cyberobrony oraz odpowiada za szkolenie kadr sił zbrojnych państw Sojuszu w tej dziedzinie. Jego partnerami są też kraje nienależące do NATO: Austria, Finlandia i Szwecja. W 2017 r. dołączyła Norwegia, a w 2018 r. Japonia. W samej Estonii utworzono Ligę Obrony Cybernetycznej, złożoną z ochotników z sektora prywatnego, którzy w razie zagrożenia bezpieczeństwa państwa mają bezpośrednio podlegać dowództwu wojskowemu.

19 kwietnia 2022 r. w Tallinie rozpoczęły się gry wojenne Locked Shields – największe na świecie międzynarodowe ćwiczenia obrony cybernetycznej w czasie rzeczywistym zorganizowane przez to Centrum.