Cyberdefence 24

aut. Jacek Raubo 18.02.2016

HYBRYDOWE TROLLE I CYBERWOJNA PRZECIWKO ŁOTWIE

O hybrydowych trollach zrobiło się głośno w związku aneksją Krymu przez Rosję i wybuchem konfliktu na wschodniej Ukrainie. NATO Strategic Communications Centre of Excellence przyjrzało się szczegółowo skali problemu koncentrując się głównie na działaniach prowadzonych wobec Łotwy.

Carl von Clausewitz twierdził, że wojna jest kontynuacją polityki, tylko prowadzoną innymi środkami. W drugiej dekadzie XXI w. do słów klasyka śmiało można byłoby dodać, że działania w cyberprzestrzeni to kontynuacja zarówno polityki jak i wojny, tylko prowadzonych innymi metodami. Twitter, Facebook, fora wymiany opinii w Internecie itp. stały się bowiem centrum aktywności, która nosi znamiona polityki i wojny. Liczące się w rozgrywkach globalnych i regionalnych kraje w ostatnich latach rozpoczęły internetowy wyścig zbrojeń, ale na tym proces się nie zatrzymał. To, co obserwujemy od 2014 r., wygląda wręcz na otwarcie kolejnego frontu nieustannie prowadzonej walki pomiędzy państwami.

Trolle współczesnymi żołnierzami wojen hybrydowych

Cennym punktem wyjścia do dyskusji na temat Internetu jako współczesnego pola walki jest raport z 26 stycznia 2016 r., przedstawiony przez NATO, a zatytułowany „Internetowy trolling jako narzędzie wojen hybrydowych: casus Łotwy". Za jego przygotowanie odpowiadało bezpośrednio NATO Strategic Communications Centre of Excellence (NATO StratCom CoE), we współpracy z lokalnymi partnerami naukowymi. Należy podkreślić, że NATO StratCom (CoE) rozpoczęło swoje działania w 2014 r., a na jego lokalizację została wybrana łotewska Ryga.

Wspomniane studium jest znacznie szersze, gdyż zajmuje się nie tylko Łotwą, choć temu krajowi rzeczywiście poświęcono najwięcej miejsca. Punktem wyjścia dla analizy było stwierdzenie, że media społecznościowe są i będą coraz częściej używane do wspierania operacji militarnych. Szczególnie, gdy oddziaływanie niebojowe na społeczeństwa jest równie ważne, jak sama walka. To właśnie poprzez umiejętne wykorzystanie tego rodzaju środków przekazu zróżnicowanych treści można wygrać walkę o rząd dusz obywateli danego państwa. W tym kontekście można mówić o swoistej militaryzacji internetowych mediów.

Oczywiście sama aktywność trolli czy też zdefiniowana na nowo działalność propagandowa państw, nawet ta zakamuflowana w mediach społecznościowych, są ściśle powiązane z rozwojem takich pojęć jak m.in. „wojna hybrydowa", „wojna informacyjna" czy klasyczną już „wojna psychologiczna". Jesteśmy świadkami gwałtownego przekształcania się mediów sieciowych w narzędzia walki. Odbiorcy przekazu pomimo tego często mają problem z odczytaniem konkretnego źródła ataków. Autorzy raportu podkreślają, że działania uderzające w niemal całe społeczeństwo korzystające z Internetu są relatywnie tanie.

Służby specjalne i wojsko nie pozostają bierne wobec zmian zachodzących w Internecie

Powołując się na Thomasa Elkjera Nissena, stwierdzono, że gama możliwości wykorzystania tego rodzaju komunikacji w celach wywiadowczych czy wojskowych znacząco wzrosła. Służby specjalne od dawna wykorzystują media społecznościowe do pozyskiwania i gromadzenia danych wywiadowczych o poszczególnych osobach. Social media są sta ły się cennym narzędziem określania i profilowania celów rozpracowań operacyjnych. Współczesne siły zbrojne nie pozostają w tyle za służbami specjalnymi testując możliwości sieci społecznościowych, np. w zakresie wojnie psychologicznej. Nie należy też zapominać o działaniach ofensywnych i defensywnych w cyberprzestrzeni, a także operacjach wymierzonycgh w systemy dowodzenia i kontroli (C2).

Do bogatego już arsenału narzędzi walki, używanych przez państwa i organizacje niepaństwowe, włączane są operacje z udziałem tzw. trolli. Ich działania były znane od dawna czytelnikom internetowych forów i komentarzy pod artykułami prasowymi. Jednak od pewnego czasu pojawiła się nowa kategoria hybrydowych trolli łamiących zasady etykiety i prowadzących skoordynowane działania, które mogą być sterowane przez instytucje państwowe bądź organizacje. Widoczna jest ich korelacja z aktywnością wybranych państw czy organizacji w sferze politycznej, militarnej i gospodarczej. Znamienne jest, że emocjonalność, jaka zazwyczaj towarzyszy działaniom klasycznych trolli, zastąpiły racjonalny ogląd i planowa realizacja wyznaczonych celów.

Rosja wyznacza kierunki w używaniu hybrydowych trolli

Według NATO StratCom (CoE), państwem o największym zinstytucjonalizowanym i profesjonalnie zarządzanym potencjale hybrydowych trolli jest Rosja. Co więcej, nowoczesne podejście Moskwy do działań w mediach społecznościowych zostało zintegrowane z jej doktrynami i strategiami państwa obejmującymi aktywność różnych instytucji. Dotyczy ono takich aspektów bezpieczeństwa państwa jak walka z ekstremizmem czy też działania sił zbrojnych. Cytowana w omawianym raporcie Jolanta Darczewska z Ośrodka Studiów Wschodnich miała wręcz stwierdzić, iż żadne inne państwo nie podchodzi do wojny informacyjnej w sposób tak systematyczny jak Rosja. Podkreśliła ona, że Rosja wyprzedziła inne państwa pod względem skali, poziomu inwestycji, finansowania czy kompetencji organizacyjnych w tej sferze.

Jednak należy podkreślić, że dla władz rosyjskich działania hybrydowych trolli są rozpisane w ramach długofalowej strategii. Kreml godzi się więc na to, że tego rodzaju aktywność nie przekłada się na natychmiastowe odniesienie zwycięstwa. Celem jest budowanie w perspektywie długookresowej w społeczeństwa przeciwnika różnych odczuć, które mogą być użyteczne z punktu widzenia rosyjskiej polityki. Taka zdolność osiągania celów w sposób zawoalowany ma wynikać w głównej mierze z dotychczasowych, tradycyjnych doświadczeń służb specjalnych Moskwy, które dezinformację i manipulowanie przekazem uczyniły nad wyraz skutecznym orężem m.in. w okresie zimnej wojny.

Autorzy przywołanego studium wzięli pod lupę przede wszystkim okres wzmożonej aktywności hybrydowych trolli w okresie aneksji Krymu i po wybuchu konfliktu na wschodniej Ukrainie. Analiza nie ogranicza się jedynie do casusu Ukrainy, ale dotyczy też Finlandii, Polski, a nawet USA. Analitycy NATO StratCom (CoE) zauważyli, że zorganizowana i nasilona aktywność trolli była od początku ukierunkowana na dwa typy zadań: obronny przed podobną aktywnością przeciwników oraz ofensywny, uderzający bezpośrednio w interesy państw i instytucji uznanych za wrogie.

Co najbardziej interesuje hybrydowe trolle

Casus Łotwy jest szczególnie ważny z racji specyfiki jej położenia geograficznego, przynależności do NATO, a także istnienia znacznej mniejszości rosyjskiej w tym państwie. Na wstępie autorzy wskazali, że działania hybrydowych trolli w analizowanym ujęciu, choć istotnie widoczne i skomasowane, nie były w sensie całościowym aż tak groźne jak można było domniemywać. Hybrydowe trolle wykazywały największą aktywność wobec tamtejszych mediów w kontekście tematów dotyczących

m.in. rozwoju sytuacji na Ukrainie, międzynarodowych reakcji na kryzys ukraiński, w tym sankcji nałożonych na Moskwę, relacji łotewsko-rosyjskich, eksplozji samolotu MH-17 czy też embarga na import żywności do Rosji.

Hybrydowe trolle częściej brały udział w operacjach nakierowanych na media rosyjskojęzyczne działające na Łotwie. Jednak różnica w stosunku do mediów łotewskojęzycznych nie była aż tak znacząca. Autorzy analizy zwrócili większą uwagę na szczególną aktywność kilku internautów podejrzanych o występowanie w charakterze hybrydowych trolli, analizując ich wpisy, używane numery IP, etc. Zauważyli też, że większość pojawiających się wpisów, nawet pomimo reakcji ze strony innych internautów, nie była rozwijana. Co więcej ok. 60-70 proc. wpisów noszących znamiona hybrydowego czy klasycznego trollingu było usuwanych przez specjalne narzędzia do moderowania komentarzy i administratorów stron. Badając casus Łotwy analitycy NATO ocenili, że wpływ hybrydowych trolli był ograniczony w badanym okresie, a ich średni udział w całości komentarzy nie przekraczał nawet 4 proc., chociaż w przypadku najbardziej nośnych tematów np. dotyczących Ukrainy, był większy.

Skuteczna obrona przed zagrożeniem ze strony hybrydowych trolli

Okazuje się, że media społecznościowe są w stanie bronić się poprzez obecność innych komentatorów, aktywność własnych użytkowników, moderatorów, a także dzięki wykorzystaniu oprogramowania antyspamowego. Stąd też w przypadku Łotwy nie określono hybrydowych trolli jako jednego z ważniejszych zagrożeń. Jednak autorzy raportu NATO StratCom (CoE) są dalecy od wykluczania możliwości odegrania większej roli przez działania hybrydowych trolli w kolejnych latach. Szczególnie, że wśród samych trolli następuje znaczne zróżnicowanie w zakresie schematów i narzędzi działania, skierowanych do różnych odbiorców lub uczestników dyskusji. W omawianym raporcie wyróżniono i scharakteryzowano takie rodzaje trolli jak: „obwiniaj Stany Zjednoczone”, trolle teorii konspiracyjnych, trolle bikini, trolle agresywne, trolle Wikipedii, trolle „z załącznikiem”.

Eksperci z NATO StratCom (CoE) i ich partnerzy badający problematykę hybrydowych trolli przygotowali również przewodnik jak rozpoznać tego rodzaju aktywność w sieci. Do jego elementów należą identyfikacja zjawiska w określonym przypadku, sprawdzenie, czy mamy do czynienia z hybrydowym trollem, oznaczenie jego aktywności i - co najbardziej istotne - ignorowanie tego rodzaju działań.

Rekomendacje ze strony NATO StratCom (CoE)

Pojawiły się również rekomendacje dla mediów, które mogą być potencjalnym celem działania hybrydowych trolli. Stwierdzono, że muszą one przykładać jeszcze większą uwagę do publikowanych informacji, tak aby nie stać się tubą służącą do realizacji kampanii dezinformacyjnych. Położono też nacisk na zwiększenie umiejętności ogólnego korzystania z mediów przez społeczeństwo. Nadal wymagane jest także inwestowanie w rozwój oprogramowania do filtracji komentarzy i przekazów tworzonych przez hybrydowe trolle. Dla instytucji rządowych kluczowe są zdolności identyfikowania źródeł kampanii realizowanych z udziałem hybrydowych trolli i uwzględnianie mediów społecznościowych we własnej polityce medialnej.

Należy również zwrócić uwagę na zunifikowane i spójne strategie narracji wykorzystywanej do opisu kontrowersyjnych wydarzeń. Chodzi o to, by skutecznie zapobiegać wykorzystaniu potencjalnych niespójności do działań dezinformacyjnych. Trzeba także odpowiednio wyczulić społeczeństwa na krytyczny odbiór niektórych rodzajów internetowych treści. Warto tu wykorzystać doświadczenia takich państw jak Łotwa i inne kraje nadbałtyckie, Finlandia czy Polska. Najważniejsze jednak pozostaje zachowanie postawy niekonfrontacyjnej przez władze, które zgodnie z zasadą „robić żarty, a nie dyskutować na poważnie” nie powinny podejmowanymi działaniami pozycjonować aktywności

hybrydowych trolli na równi z oficjalnymi przekazami.

Trolle stałym elementem działań ofensywnych i defensywnych w cyberprzestrzeni

Po opublikowaniu raportu NATO StratCom (CoE) pojawiły się także głosy ze strony innych podmiotów, które miały styczność z problemem cybertrolli w swej codziennej działalności w Internecie. Interesujące wnioski przedstawił w imieniu The Intersection Project Ernest Wyciszkiewicz. Podkreślił on dualność w uderzeniach zarówno na pojedyncze osoby zaangażowane w działania instytucji, jak i w samą The Intersection Project czy Polsko-Rosyjskie Centrum Dialogu i Porozumienia. Autor wskazał, iż działania obejmowały nie tylko ataki wprost przy użyciu fałszywych informacji i kalumnii, ale również operacje pod obcą flagą, w których praktykowane jest podszywanie się pod inny kraj czy organizację, w tym wypadku proukraińskich internautów. Według Wyciszkiewicza, najlepszą obroną dla organizacji i osób stanowiących cele ataków hybrydowych jest transparentność działań, personaliów i sposobu finansowania.

Cybertrolle na stałe wpisały się w krajobraz Internetu jako narzędzie, które ma pomóc państwom i innego rodzaju organizacjom zwiększyć efektywność ich polityki. Nie należy zapominać, że chociaż rosyjskie trolle hybrydowe są najbardziej rozpoznawalne, szczególnie w dobie konfliktu na Ukrainie, trudno przypuszczać, aby inni nie stosowali podobnych metod. Społeczeństwa, instytucje państwowe i zwykli użytkownicy Internetu, m.in. mediów społecznościowych, muszą być więc przygotowani na tego rodzaju zagrożenia. Szczególnie, że model rozchodzenia się informacji w dobie Internetu sprzyja operacjom dezinformacji w ramach wojen informacyjnych czy działań nacechowanych hybrydyzacją sił i środków stosowanych m.in. w ramach operacji wojskowych.

Dotychczas hybrydowe trolle nie były w stanie doprowadzić do błyskotliwego i szybkiego zwycięstwa w walce o serca i umysły internautów, ale nie należy nie doceniać zbieranych obecnie przez ich mocodawców doświadczeń. Z pewnością najnowszy wyścig zbrojeń w cyberprzestrzeni nie obędzie się bez takich narzędzi jak cybertrolle.