aut. Adam Lelonek 09.03.2018

ANDRIEJ SOŁDATOW: DZIENNIKARZE ŚLEDCZY CZASEM MOGĄ ZROBIĆ WIĘCEJ NIŻ SŁUŻBY [WYWIAD]

O nieskuteczności rosyjskiej cenzury internetu, ciekawości Zachodu ze strony Rosjan, problemach z ustaleniami atrybucji służb odpowiedzialnych za ataki wobec państw zachodnich, o niemożliwości odmawiania współpracy z rosyjskimi organami bezpieczeństwa przez tamtejsze firmy z branży IT, ale i „totalitarnej inwigilacji" z wykorzystaniem rosyjskiej technologii mówił w rozmowie z CyberDefence24.pl Andriej Sołdatow, rosyjski dziennikarz śledczy specjalizujący się w tematyce służb specjalnych. Rozmowa odbyła się 27 lutego br. w Microsoft Innovation Center w Brukseli w kuluarach konferencji CYBERSEC – Brussels Leaders' Foresight, zorganizowanej przez Instytut Kościuszki.

dr Adam Lelonek: Wszyscy skupiają się na jednym wektorze oddziaływań informacyjnych – Rosji wobec państw zachodnich. W tym samym jednak czasie Kreml uszczelnia swoją przestrzeń informacyjną, realizuje koncepcję „suwerenności cyfrowej", wymusza na firmach magazynowanie danych na swoim terytorium, co daje jednocześnie rosyjskim służbom szerokie możliwości inwigilacji. Jakie są więc obecnie możliwości wpływania przez Zachód na społeczeństwo rosyjskie?

Andriej Sołdatow: Myślę, że w pierwszej kolejności powinniśmy pamiętać o lekcjach z okresu zimnej wojny. Scentralizowane wysiłki propagandowe ukierunkowane są na porażkę. Nieważne czy będzie chodziło o pozytywny czy negatywny przekaz. Ludzie prędzej czy później zaczną je dostrzegać.

To, co było wtedy ważne, to fakt, że zagraniczne media czy rozrywki były niezwykle atrakcyjne dla mieszkańców ZSRR. Podobnie jest i dzisiaj dla obywateli Federacji Rosyjskiej. Czasem to, co zyskuje popularność, może zaskakiwać. Na przykład mamy teraz ten międzynarodowy skandal z rosyjskimi sportowcami i stosowaniem dopingu. Kremlowskie media przedstawiają całą sprawę jako wielki spisek – raz jako spisek CIA, raz kogoś innego, aby tylko uderzyć w Rosję. Bardzo wielu Rosjan przejęło ten punkt widzenia. Nagle jednak Netflix, który jest dostępny w Rosji, wyemitował niezwykle dobry film dokumentalny „Ikar" [ang. Icarus – przyp. red.]. To zmieniło wszystko. A to nie jest propaganda, to prawdziwe dziennikarstwo. Ponieważ zostało to zrobione tak profesjonalnie, ludzie zaczęli to oglądać i kwestionować oficjalny przekaz. Także takie działania okazują się już wystarczające.

Dostęp do zachodnich mediów jest ważnym elementem. Ludzie w Rosji bardzo chętnie z nich korzystają, jeżeli chodzi o pozyskiwanie informacji. Są więc różne projekty, które tłumaczą publikacje na temat Rosji i z Rosji z zachodnich mediów na język rosyjski. Niestety Kreml zdaje sobie z tego sprawę. Próbują w związku z tym kontrolować ten przepływ informacji.

W jaki sposób?

Jedną z takich prób jest inoSMI.ru [ros. ИноСМИ – przyp. red.]. Strona ta dostarcza tłumaczeń z bardzo

wielu mediów z Zachodu na temat Rosji. To odzwierciedla jednak ogólny trend – Rosjanie chcą wiedzieć, co pisze się o ich kraju zagranicą. Prawdziwą barierą, swojego rodzaju ścianą pozostają jednak języki obce.

Więc rekomendowałby Pan oddziaływanie przez popularyzację treści w języku rosyjskim?

Można zacząć od czegoś podstawowego. Nie chodzi nawet o fizyczne robienie wszystkich tłumaczeń. Warto byłoby zastanowić się nad wprowadzaniem rozwiązań, które ułatwiałyby takie tłumaczenia automatycznie lub wspierać samych tłumaczy. Gdyby ludzie w Rosji mieli możliwość czytania każdego dnia np. The New York Times, którego publikacje byłyby automatycznie tłumaczone na rosyjski, nawet niektóre komentarze czy opinie, mowa byłaby o zupełnie nowym audytorium, nie tylko trollach. Czytelnikami staliby się „zwykli Rosjanie", którzy naprawdę są zainteresowani w tym, co się dzieje.

Ale jak to się ma do zmian prawnych, cenzurowania internetu, ograniczania możliwości działania zachodnim podmiotom, nie tylko mediom? Blokada rosyjskiej przestrzeni informacyjnej może być aż tak nieskuteczna?

To nie działało wcześniej, za Związku Radzieckiego, kiedy mieliśmy bardzo wiele różnych ograniczeń i pod znacznie większą kontrolą KGB. To nie działa i dzisiaj. Dwa tygodnie temu Roskomnadzor [Rosyjska Federalna Służba Nadzoru w sferze łączności, technologii informatycznych i środków masowego przekazu – przyp. red.], tj. agencja odpowiadająca za cenzurę internetu przyznała wprost, że jej działania z blokowaniem serwisów VPN [Virtual Private Network – przyp. red.] są nieskuteczne.

Czytaj więcej: Rosja ogranicza dostęp do sieci VPN

Czyli przyznała się do porażki.

Tak, oczywiście. Na szczęście, kiedy ma się do czynienia z państwami autorytarnymi, to najczęściej przegrywają one z technologią. Innymi słowy postęp technologiczny jest szybszy niż machina biurokratyczna. Tak jak było to w okresie zimnej wojny, tak samo jest i teraz.

Prywatne sieci są więc wciąż popularne w Rosji, mimo zakazu?

Jeżeli ktoś w Rosji jest zainteresowany jakimiś informacjami może w łatwy sposób zdobyć dostęp nawet do zakazanych stron internetowych. System filtrowania ruchu w sieci jest bardzo dziurawy i nie jest zbyt zaawansowany na poziomie technicznym.

To jest chyba pewien proces, może się to zmienić.

Ja osobiście w to nie wierzę. Rosja to nie Chiny. W Chińskiej Republice Ludowej pewne elementy filtracji i ograniczeń zostały zainstalowane na poziomie fundamentów całej infrastruktury internetu. Rosja rozwijała swój internet na zasadach swobody i braku państwowej kontroli przez ponad 20 lat. Pewne negatywne zmiany zaczęły się pojawiać od 2012 roku, jednak było już trochę za późno dla Kremla. Jest tu jednak pewna nadzieja.

Najważniejsze pytanie, które wszyscy na całym świecie sobie zadają, a nikt nie jest w stanie udzielić odpowiedzi, to jak działają rosyjskie służby specjalne w obszarze wojny informacyjnej. Jak wyglądają procesy decyzyjne, planowanie, przygotowywanie strategii i zarządzanie operacjami informacyjnymi?

Nie jest to takie proste czy, powiedziałbym – „tradycyjne". Na część z tych zagadnień staraliśmy się odpowiedzieć w naszej książce [„The Red Web: The Kremlin's Wars on the Internet" – przyp. red.], jak chociażby struktura dowodzenia czy centralizacja. Na Zachodzie jest takie przekonanie, że hakerzy,

którzy używają narzędzi z repertuaru służb specjalnych, to z automatu oznacza to, że są to służby specjalne. To absolutnie błędne rozumowanie. Bardzo często jest wręcz przeciwnie. Mamy aktorów niepaństwowych pracujących dla Kremla, jednak w żaden sposób z nim nie powiązanych. Taka strategia „outsourcingowa" okazuje się być niezwykle skuteczna. Z jednej bowiem strony mamy ludzi, którzy są znacznie bardziej elastyczni, ale i „odważniejsi", ponieważ nie są elementem biurokracji. Od ich działań oficjalne struktury państwa zawsze mogą się odciąć i powiedzieć, że „to nie my". Na tym polega cała sztuczka. Moim zdaniem niezwykle ważne jest wprowadzanie odpowiedzialności karnej wobec farm trolli. Ich funkcjonowanie pokazuje bowiem jak pewne procesy są zorganizowane na poziomie wewnętrznym.

Działania tych „aktorów niepaństwowych" muszą być jednak jakoś koordynowane i zarządzane.

Oczywiście. Chodzi o to, że są one bliżej do Kremla niż służby specjalne. Te ostatnie, podobnie jak i w każdym kraju na świecie, są elementem całego aparatu biurokracji. Mówiąc wprost, jeżeli ktoś chce przeprowadzić jakąś operację, musi iść do swojego przełożonego, on do swojego i tak do samej góry. Obok tego jest stos roboty papierkowej. To zbyt wolny proces. Poza tym osoby pracujące dla służb wcale nie czują się wcale zbyt komfortowo, kiedy chodzi o realizowanie jakiegoś „śmiałego", ryzykownego zadania. Aby podać jeden przykład. Mamy Internet Research Agency. Struktura w pełni rozwinięta, która posiada nawet swoich ludzi w zagranicznych placówkach dyplomatycznych. To jest coś „śmiałego", co może „wkurzyć" wielu ludzi. Jeżeli ktoś chce się zdecydować na takie działania, musi liczyć się z konsekwencjami, jak na przykład wydaleniem z terytorium danego kraju. Taka ekspozycja to jednak spory koszt. Jeżeli jednak są ludzie, którzy działają w sposób całkowicie nieformalny, jak agencje PR-owe, pojedyncze jednostki lub grupy ludzi, którzy są wyłącznie szczęśliwi, że mogą pomóc własnemu państwu i dają się sterować przez Kreml, koszt wtedy jest bardzo niewielki. No chyba, że ktoś zidentyfikuje wydających polecenia imiennie. Ale sami ci ludzie wykonujący pracę nie są jednak żadną instytucją.

Na Zachodzie w gronie ekspertów często są spory odnośnie zakwalifikowania działań takich grup. Jedni mówią, że kimś zarządza wywiad wojskowy, inni że cywilny.

Niestety są to bardzo trudne kwestie. W wielu wypadkach mamy do czynienia z pokrętną logiką. Kryminalistyka cyfrowa dostarcza najwięcej dowodów na podstawie których dokonywana jest atrybucja sprawców, ale i wiązanie danych podmiotów atakujących z określonymi strukturami służb specjalnych. Problem polega jednak na tym, że ta kryminalistyka ma swoje limity. Możemy na przykład określić dokładnie kraj, z którego miał miejsce atak, nie możemy jednak pójść dalej i dokładnie przyporządkować odpowiedzialną za niego agencję rządową. Wtedy więc mówi się, że ponieważ kilka lat temu, czy to będzie pięć czy siedem, była tendencja do atakowania przez daną grupę, powiedzmy – celów wojskowych, to obecnie „wierzymy", że stoi za nią wywiad wojskowy. Takie rozumowanie ma jednak wątpliwą jakość, zwłaszcza jeżeli chodzi o Rosję. Mamy służby cywilne atakujące cele wojskowe i wojskowe atakujące cele cywilne. Dlatego też dosyć dziwnie się czuje, kiedy ktoś jednoznacznie stwierdza, że na pewno za coś odpowiada Służba Wywiadu Zagranicznego, a za coś innego na pewno Federalna Służba Bezpieczeństwa.

Czytaj więcej: Holenderski wywiad zhakował Rosjan

Wszyscy mają problem z takimi narracjami. Wystarczy spojrzeć na ostatni raport Holendrów. Twierdzą oni dwie rzeczy, które mogą być faktycznie prawdziwe. Z jednej strony, od lat pracowali razem ze Stanami Zjednoczonymi przy identyfikacji działań grupy Cozy Bear. Z drugiej strony mówią teraz, że ich zdaniem za wspomniana grupa to operacja, za którą odpowiada Służba Wywiadu Zagranicznego FR. Natomiast strona amerykańska twierdziła, że to operacja FSB. Mamy do czynienia z takimi sytuacjami, kiedy jest zbyt mało narzędzi mogących pomóc przy atrybucji.

Czytaj więcej: Zhakowanie Rosjan potwierdza wysoką klasę holenderskiego wywiadu SIGINT

Innymi słowy nawet Pan, specjalista zajmujący się od lat tematyką rosyjskich służb, ma problem z identyfikacją takich działań.

Oczywiście. Próbujemy czasem podejmować próby atrybucji, na podstawie różnych przesłanek. Część z nich zawarliśmy w książce. Mamy jednak pewne problemy z tym, jak jest to postrzegane na Zachodzie, tym bardziej, że i tam są różne niespójności czy kontrowersje.

Musimy więc polegać na spekulacji i scenariuszach teoretycznych.

Nie. Trzeba brać zawsze pod uwagę, że najlepsze śledztwa, w tym chociażby na temat farm trolli, pochodzą jednak z samej Rosji. Jeszcze raz podkreślę, że nie możemy zapominać nawet na chwilę o zimnej wojnie, ponieważ tutaj są największe różnice. W tamtym czasie, mieliśmy prawdziwy mur między Rosją a Zachodem. Za nim, po stronie Paktu Warszawskiego, występowało KGB czy Stasi, ogólnie jakieś litery. To nie był zbyt szczegółowy obraz. Dziś żyjemy w zglobalizowanym świecie. Wiemy dziś znacznie więcej. Można zdobyć bardzo rozległą wiedzę na temat rosyjskich operacji, m.in. od rosyjskich dziennikarzy śledczych, którzy pozostają na terytorium Federacji Rosyjskiej i wykonują swoją pracę. Podobnie jest z zachodnimi dziennikarzami, którzy przebywają w Moskwie.

Są więc sposoby na zgłębianie pewnych tematów. To jest jedna z otwartych opcji. Dla mnie osobiście jest ona bardziej atrakcyjna niż lata raportów służb specjalnych, które są po prostu komunikatami, nie popartymi żadnymi istotnymi dowodami. Po działaniach Edwarda Snowdena i Juliana Assange'a nikt już zresztą za bardzo w nie nie wierzy. Dzisiaj nie wystarczy już powiedzieć, że „bardzo wierzymy, że coś było rosyjską agresją". Trzeba przedstawić dowody.

Zapewne nie zawsze można to zrobić.

Oczywiście rozumiem, że często są powody dla których służby nie upubliczniają pewnych faktów. Problem jest z tym jednak taki, że jeżeli chce się przekonać do czegoś opinię publiczną, trzeba jednak przedstawiać pewne dowody. To nie musi być wcale praca dla wywiadów. To jest w zasadzie praca dla dziennikarzy śledczych.

Gdyby jednak pokusić się o namalowanie najprostszego obrazu sytuacji w Rosji na odcinku prowadzenia wojny informacyjnej i psychologicznej, to jakby on wyglądał? Powiedział Pan, że mamy służby, Kreml i podmioty prywatne.

Mamy trzy elementy. Kreml i administracja państwowa podejmują decyzję. Mamy służby specjalne – cywilne i wojskowe. Ale mamy też hakerów i cały sektor IT, którzy pomagają i stanowią wsparcie dla działań władz. To ostatnie to najważniejsza część całego problemu, zwłaszcza po aneksji Krymu. W 2014 roku Kreml zrobił wszystko, aby zabezpieczyć sobie lojalność wielu prywatnych firm, które działają w branży IT. Teraz, jeżeli ktoś ze struktur państwowych przychodzi do takiej firmy i prosi o pomoc w jakiejkolwiek sprawie, nie mówiąc już o tych najbardziej poufnych czy ważnych, nikt nie jest w pozycji, żeby móc odmówić. Pomagają wszyscy. Głównie ze strachu. To bardzo skomplikowana sytuacja.

No to w takiej sytuacji nie mogę nie dopytać – co w takim razie z firmą Kaspersky?

Myślę, że częściowo on i jego firma są ofiarami obecnego kryzysu. Przed 2016 rokiem Jewgienij Kaspierski był bardzo szczęśliwy i dumnie deklarował, że on i jego firma współpracują z rosyjskimi służbami specjalnymi. Wierzył w swoim idealistycznym podejściu, że Rosja jest w zasadzie taka sama jak Stany Zjednoczone. Do tej pory zresztą udaje, że FSB jest agencją porządku publicznego, jak taka sama służba w innych zachodnich państwach. To nie jest jednak do końca prawda, ponieważ FSB nie

jest t y l k o agencją odpowiadającą za bezpieczeństwo w państwie, to także agencja wywiadowcza. On zdawał się ten fakt całkowicie odrzucać.

Proszę jednak pamiętać, że do 2016 roku nawet i FSB cieszyło się dosyć dobrą reputacją na Zachodzie. Powiedziałbym nawet, że zadziwiająco dobrą reputacją. Jej szef był nawet zapraszany do Waszyngtonu. A to było przecież po aneksji Krymu.

Dlaczego tak było?

Może podam teraz zbyt wiele szczegółów, ale po zamachu w Bostonie w 2013 r. wypłynęły historie, że FSB próbowało ostrzec FBI i CIA. Pozwoliło to bardzo mocno wzmocnić wiarygodność FSB w państwach zachodnich. Dlatego też Kaspierski przez wiele lat mógł nie widzieć niczego złego we współpracy z tą służbą – miała pozytywną ocenę na Zachodzie. W 2016 r. wszystko się zmieniło. On nie był na to gotowy. I chyba dalej nie rozumie istoty problemu. W dzisiejszym świecie, kiedy stoimy przed problemem tak dużego braku zaufania trzeba odbudować zaufanie klientów. On tego nie rozumie. Na szczęście działalność jego i jego firmy musi być coraz bardziej transparentna jeżeli chodzi o współpracę ze służbami czy organami odpowiadającymi za bezpieczeństwo publiczne.

Wielokrotnie rozmawiałem z wykładowcami uczelni technicznych oraz ekspertami z obszaru IT czy cyberbezpieczeństwa z Ukrainy. Są oni przekonani, że wiele urządzeń rosyjskiego pochodzenia, jak nawet domofony w blokach mieszkalnych, ale i routery, telefony komórkowe, czy inny sprzęt codziennego użytku stanowi realne zagrożenie. Mimo to rosyjska technika, czy tzw. „rosyjski chińczyk", wciąż wykorzystywana jest nawet we Lwowie, mimo tego, że są polskie czy zachodnie zamienniki. Często chodzi tu bowiem o cenę. Czy biorąc pod uwagę to, co Pan powiedział o konieczności współpracy rosyjskiego sektora IT z rosyjskimi służbami, zgodzi się Pan z tezami ukraińskich ekspertów, że instalacja komponentów umożliwiających przejęcie danego urządzenia lub szpiegowanie użytkowników może być zlecana masowo i eksportowana do innych państw?

Problem jest nawet większy, jeśli mam być szczery. Prowadzonych jest wiele śledztw na takie tematy. Tutaj nie chodzi o eksport pewnej technologii do krajów o ustroju autorytarnym czy totalitarnym. Nie chodzi też o to, że, powiedzmy, jakaś brytyjska technika trafi do Egiptu, czy Rosyjska na Ukrainę. Prawdziwe sedno problemu polega na tym, że wiele spośród państw byłego ZSRR, w tym właśnie Ukraina, niestety, ale nie zdołały zreformować swojego systemu prawnego. Chodzi mi o to, że jeżeli prowadzi się jakiś biznes, potrzebne są licencje. Jednym z elementów składowych całego procesu jest m.in. to, że można dodawać pewne komponenty lub wprowadzać określone modyfikacje produktów tak, aby ułatwiać pracę organów bezpieczeństwa. Kluczowe będą tu standardy, w ramach których realizowane są działania z tym związane. Można przyjąć np. europejskie, można amerykańskie. Można jednak robić to „po rosyjsku". Znowu, niestety, ale wiele państw poradzieckich wybrało najłatwiejszą drogę i zgodziło się na rosyjskie kierownictwo w ustanawianiu pewnych norm i reguł. Za tym podążają jednak konsekwencje. Do dzisiaj znacznie łatwiej jest w państwach byłego ZSRR kupować wiele rzeczy z Rosji, ponieważ spełniają one określone normy, dane komponenty czy części są bardziej znane. Rosyjskie firmy również znacznie łatwiej potrafią się poruszać w takich środowiskach prawnych i wiedzą jak zdobyć określone uprawnienia czy spełnić dane wymagania.

Osobiście jestem bardzo zdziwiony, że nawet po 2014 r. ukraińskie organy odpowiedzialne za bezpieczeństwo kraju dalej pozostały przy tych starych normach i regulacjach. Mało tego, często nie zmieniono nawet osób na kierowniczych stanowiskach w instytucjach państwowych pracujących na tym odcinku. Innymi słowy faktycznie nie podjęto tutaj procesu reform. Nie chcę powiedzieć, że to źle tylko dlatego, że Ukraina kontynuuje import towarów z Rosji, ponieważ trwa rosyjsko-ukraiński konflikt. To źle przede wszystkim dlatego, że rosyjskie podejście do inwigilacji jest po prostu totalitarne. Naprawdę totalitarne. Nieważne przy tym kto zasiada na Kremlu. Po prostu to, jak się w

Rosji do tego podchodzi, co zostało skopiowane w wielu innych byłych krajach związkowych, zostało wymyślone jeszcze w latach 80. XX wieku przez KGB. Wtedy nikt jeszcze nie myślał o takim poziomie kontrolowania społeczeństw w rozwiniętych demokracjach. Te metody były systematycznie aktualizowane i dostosowywane do postępu technologicznego. W praktyce mamy więc do czynienia z koncepcją inwigilacji i nadzoru autorstwa KGB. Podejmowanie próby budowania państwa demokratycznego, co jest procesem bardzo delikatnym, kiedy wciąż w podejściu do technologii obecne jest podejście wypracowane przez KGB, uważam za bardzo poważny błąd.

Innymi słowy potwierdza Pan obawy ukraińskich ekspertów.

Tak. Wszystko wskazuje na to, że mają oni rację.