Wojciech Jakóbik: Front, którego geopolityka się nie ima

Nowe zjawiska łączące wirtualną rzeczywistość z codziennością pokazują, że obie sfery będą się ze sobą wiązać coraz mocniej, dlatego też aparat państwowy musi reagować na symptomy internetowej rewolucji - czytamy na stronie OMP

Zapraszamy na www.usa-ue.pl – stronę Ośrodka Myśli Politycznej o stosunkach międzynarodowych.

W debacie publicznej w Stanach Zjednoczonych i rozmowach prowadzonych w gabinetach państw zachodnich coraz więcej uwagi poświęca się dyskusji o roli cyberprzestrzeni na arenie międzynarodowej. W świetle pojawiających się doniesień o nowych zjawiskach w tym obszarze o skali światowej, ustalenie roli tej sfery w polityce państwa staje się kluczowe.

Signum Tempori

Nowe zjawiska łączące wirtualną rzeczywistość z codziennością pokazują, że obie sfery będą się ze sobą wiązać coraz mocniej, dlatego też aparat państwowy musi reagować na symptomy internetowej rewolucji i dostosować do nowych warunków swoje instrumentarium. Jest to konieczne, jeżeli przywódca państwa chce uniknąć ataków informatycznych przeprowadzanych przez inne państwo, bądź aktorów niepaństwowych. Od nowej rzeczywistości nie ma odwrotu, a ten kto adekwatnie na nią nie zareaguje, przegra walkę o własne bezpieczeństwo.

Zaciemnienie sieci

Odcięcie od Internetu całego Egiptu w obliczu niepokojów społecznych, jakie ogarnęły ten kraj pokazało siłę narzędzia, jakim dysponuje państwo, w celu kontroli działań swoich obywateli. Z punktu widzenia bezpieczeństwa kraju, w celu ograniczenia wymiany informacji między własnymi obywatelami, wystarczy zmusić dostawców internetowych do zablokowania transferu. Autorytarny prezydent Egiptu Mosni Mubarak zdołał przeprowadzić taką akcję w jeden dzień, odcinając 27 stycznia cały kraj od Internetu. Protestujący przeciwko jego władzy (abstrahując od inspiracji tych protestów) skrzykiwali się na manifestacje za pomocą popularnych serwisów społecznościowych, jak Twitter, czy Facebook. Mubarak znalazł na to remedium – odciął Internet na przestrzeni całego kraju. Było to możliwe, ponieważ infrastruktura egipskiego Internetu jest słabo rozwinięta, a dostawców na rynku jest kilku. Owa sieć jest tak wątła, że w 2008 roku wystarczyła usterka kabli łączących kraj faraonów z resztą świata, by Egipcjanie stracili dostęp do Internetu.

Opisujący sprawę dziennikarze Reutersa stwierdzili, że w USA nie byłoby to możliwe, jako, że amerykańska infrastruktura zapewnia pełną dywersyfikację źródeł sygnału internetowego i jest lepiej skomunikowana z resztą świata, jak przystało na kolebkę World Wide Web. Jest jednak kwestią czasu, aż rządy demokratycznych potęg wejdą w posiadanie narzędzi pozwalających powtórzyć egipskie ,,zaciemnienie'', ponieważ z punktu widzenia bezpieczeństwa

informatycznego państwa, lepiej posiadać sposób na przeprowadzenie takiego procederu, niż stać się jego ofiarą i wtedy zastanawiać, w jaki sposób było to możliwe.

Podobne zaciemnienie miały miejsce w chińskiej prowincji Xinjiang, w której doszło do niepokojów na tle etnicznym w 2009 roku. Pekin wprowadził również obejmującą cały kraj sieć oddzieloną od reszty świata, w której zabrakło miejsca dla popularnych w wolnym świecie serwisów, jak Youtube, czy Myspace, ów chiński Internet jest też przedmiotem stałej inwigilacji przez służby informatyczne państwa. Restrykcje odnośnie sieci wprowadziły również Iran, Tunezja i Syria w obliczu rosnącego niezadowolenia społecznego mającego ujście w komunikatorach internetowych. Cyberprzestrzeń ma coraz większy wpływ na życie codzienne obywateli, a także na kondycję państwa, czego przypadek egipski jest tylko najbardziej namacalnym przykładem.

Cybernetyczne szpiegostwo

Na łamach pisma The Examiner specjalista Heritage Foundation do spraw bezpieczeństwa narodowego James Jay Carafano opisuje nowe narzędzie cybernetyczne, za pomocą którego państwa mogą prowadzić szpiegostwo międzynarodowe. Dzięki niemu obwarowane granice, przeszkody geograficzne i wszelkie stosowane przez państwo tradycyjne środki zabezpieczania informacji tracą moc, ponieważ frontem, na którym działa owa broń jest nieskończona i niemierzalna rzeczywistość wirtualna.

Naukowcy z Uniwersytetu w Toronto po miesiącach badań sieci używanej przez tybetańskich dysydentów ustalili, że wycieki informacji zauważone przez mnichów, mają miejsce, ponieważ ich infrastruktura internetowa, a razem z nią sieci ponad 100 państw świata, są zainfekowane złośliwym oprogramowaniem (malicious software – malware), nazwanym przez Kanadyjczyków GhostNet. Program kradnie dane, wysyłając je bez wiedzy użytkownika do z góry ustalonego źródła. Cały proceder pozostaje w ukryciu, a cywilne sposoby ochrony danych nie są w stanie go zablokować.

Carafano nie odpowiada jednoznacznie na pytanie, czy GhostNet powstał w Chinach. Wskazuje jednak na przykłady działalności chińskich informatyków państwowych, która nie byłaby możliwa, bez użycia narzędzia, takiego jak to złośliwe oprogramowanie. W swoim

artykule podaje on też ciekawe informacje, na temat informatycznej potęgi, którą Pekin buduje z rodzimych informatyków, którymi często są zdolni studenci, którym oferuje się ,,wprowadzanie sprawiedliwości online'' na pół etatu, w zamian za dostęp do powszechnie zablokowanych domen internetowych. W Chinach działa również Red Hacker Alliance – usankcjonowana przez władzę organizacja rzekomo strzegąca sieci.

Według informacji wywiadu USA liczba jej członków i opłacanej kadry wynosi 300 tys. osób, wśród których wielu jest uniwersyteckimi geniuszami informatycznymi. Misją RHA jest ,,patriotyczny'' cyberhacking i realizacja sponsorowanych przez rząd projektów.

Ekspert HF podkreśla, że oficjalna doktryna Państwa Środka forsuje sprawdzanie możliwości cybernetycznych Państwa Środka w praktyce. To istotne, ponieważ zdaniem Carafano Chiny są głównym zagrożeniem dla bezpieczeństwa amerykańskiej sieci. Specjalista przyznaje jednak, że w USA nie została jeszcze sformułowana polityka względem cyberprzestrzeni, ponieważ w Pentagonie wciąż silne jest lobby sceptyczne wobec potencjału tego frontu. Carafano nawołuje jednak do głębokiej refleksji nad tym zagadnieniem, ponieważ Pekin już teraz wyprzedził Waszyngton w wyścigu cybernetycznym, a wobec bierności amerykańskich oficjeli może poczynić dalsze postępy.

Jak wiadomo, w globalnej rywalizacji ten, kto pozostaje w miejscu – cofa się. W zagadnieniach związanych z bezpieczeństwem informatycznym państwa nie ma miejsca na bierność, ponieważ wyścig wirtualnych zbrojeń ma dużo szybsze tempo, niż wyścig konwencjonalny. Najsilniejsze państwa świata tworzą już narzędzia służące do obrony własnej sieci, a co za tym idzie informacji, ale i takie, służące do przeprowadzania ataków cybernetycznych. W dziedzinie rywalizacji międzynarodowej otwiera się nowy front, na który siłą rzeczy władze każdego państwa będą musiały wkroczyć. Lepiej dla tej władzy, jeśli będzie na ten moment odpowiednio przygotowane.

Wirus, który związał ręce państwu

Szeroko komentowana w mediach sprawa wirusa Stuxnet, który doprowadził do zatrzymania irańskiego programu atomowego, pokazuje potencjał wpływania na rzeczywistość, drzemiący w narzędziach cybernetycznych. Program, o którego stworzenie posądza się głównie Tel Awiw, lub Waszyngton, zablokował działanie urządzeń używanych do badań atomowych przez Teheran. Spowodowało to czasowe zatrzymanie irańskich prac nad programem atomowym, którego obawia się Zachód.

Ten wyczyn wskazuje na fakt, że informatycy są dziś zdolni za pomocą metaforycznych klawiatury i monitora wpływać na losy całych państw. Jedynie odpowiedź państwa, w postaci silnej służby informatycznej, będącej w stanie bronić infrastruktury sieciowej swoich obywateli i organów władzy może dać odpór takiemu zagrożeniu. W chwili obecnej większość państw odsłania wirtualne podbrzusze, mogące stać się celem ataku bardziej zaangażowanych wirtualnie państw, bądź podmiotów pozapaństwowych.

Kodeks cybernetyczny

Na łamach portalu think tanku Heritage Foundation Paul Rosenzweig wylicza dziesięć zasad walki w cyberprzestrzeni, którymi powinny się kierować władze pragnące zapewnić bezpieczeństwo w tym sektorze.

Po pierwsze, cyberataki są niebezpośrednie. Wpływają na infrastrukturę sieci, zmieniają informacje, kasują je, lub kradną, ale rzadko mają przełożenie na fizyczną rzeczywistość. To założenie może ulec zmianie, na co wskazuje sam autor wyliczenia, wymieniając Stuxnet, jako przykład działania w sieci, które oddziałuje na rzeczywistość materialną.

Po drugie – cyberprzestrzeń jest wszędzie. Każde obsługujące na świecie systemy finansowe, energetyczne, obronne, telekomunikacyjne, a nawet rolnictwo, są kontrolowane za pomocą komputerów. Ponadto, praktycznie każdy podmiot obecnej wymiany informacji, prowadzi ją za pomocą Internetu.

Po trzecie, sieć nie ma granic. Rosenzweig podaje przykład pocisku międzykontynalnego, który potrzebuje 33 minut, by osiągnąć cel. Odległość pomiędzy dwoma punktami w sieci informatycznej mierzone są w mocy przesyłowej, a nie w kilometrach. Autor wskazuje na kraje takie, jak Rosja, czy Ukraina, które stały się bezpieczną przystanią dla przestępców cybernetycznych, dla których oddalenie Waszyngtonu nie ma znaczenia. Specjalista jednak stwierdza jasno, że tworzenie wewnętrznych sieci, takich jak chińska nie jest realnym zabezpieczeniem wobec tego zagrożenia, ponieważ jednocześnie odcina ono obywateli od zalet Internetu.

Po czwarte – anonimowość jest funkcją, a nie błędem sieci. Problemy tybetańskich mnichów z ustaleniem źródła ataku za pomocą GhostNet, pokazują jak trudno jest je zidentyfikować w warunkach cyberprzestrzeni. Jednak anonimowość, jest zdaniem autora wyliczenia, częścią natury Internetu, który przez swój minimalizm funkcjonalny warunkuje wolność słowa ale i bezkarność przestępców w ramach wirtualnej rzeczywistości.

Po piąte – pasywna defensywa na długą metę nie działa. Zdaniem Rosenzweiga inwestowanie rozrastające się systemy firewall nie ma sensu w skali długofalowej, ponieważ w cyberprzestrzeni ofensywa ma przewagę nad defensywą. Kluczem do zabezpieczenia danych w sieci jest aktywna obrona wykraczająca poza własny system informatyczny. Mowa tu o narzędziach cybernetycznej kontroli systemów przeciwnika.

Po szóste, większość rządowego ruchu w Internecie odbywa się za pomocą pozarządowej infrastruktury. Autor przywołuje dane dla USA – 85-90 procent danych istotnych dla amerykańskiego rządu podróżuje kablami prywatnymi. Rosenzweig stawia tu tezę z pozycji

konserwatywnej, zakładając, że jeżeli wymiana informacji pomiędzy organami rządu wymaga użycia sieci pozarządowej, to rząd powinien rozciągnąć aktywną obronę, również nad sektorem prywatnym sieci.

Po siódme – działania rządu w celu obrony Internetu i jego użytkowników mają pełną legitymację. Na nic narzekania lewicowych wolnościowców, których możemy się spodziewać w razie ingerencji władzy w sieć – jedynie rząd jest w stanie stworzyć aktywną obronę cyberprzestrzenną, zatem jego obowiązkiem jest, zdaniem autora kodeksu, jej stworzenie i kontrolowanie sieci za jej pomocą.

Po ósme, ,,wojskowi zrobią to lepiej, niż cywile. Autor wskazuje na różnice w kulturze pracy oraz możliwościach sektora militarnego i cywilnego, które zdecydowanie przeważają na korzyść tego pierwszego. Wojsko ma dostęp do nowszej technologii, większe i bardziej zdyscyplinowane zasoby ludzkie oraz szersze kompetencje pozwalające na skuteczną obronę sieci.

Po dziewiąte – żadna obrona nie będzie w stu procentach doskonała. Jedyną pewnością w cyberprzestrzeni jest niepewność, co do skuteczności zabezpieczeń stosowanych w systemach cybernetycznych.

Obrona w sieci działa, dopóki nowy rodzaj ataku jej nie zakwestionuje. Rozwój technologii internetowej jest niepowstrzymywalny i szybszy, niż rozwój technologii innego rodzaju, dlatego też nie ma pewnych środków do obrony informacji w sieci. Są jedynie narzędzia, które do tej pory działały, albo takie, których skuteczność została już poddana próbie.

Wreszcie, po dziesiąte – ataki typu hardware (na sprzęt komputerowy) są trudniejsze do powstrzymania niż ataki software (na oprogramowanie). Większość krzemowych układów, które składają się na urządzenia komputerowe, produkowane jest poza granicami państw, w których funkcjonują. Nie ma czegoś takiego jak narodowy przemysł informatyczny, poza wąskim sektorem, który nie jest w stanie zabezpieczyć danych wrażliwych w stopniu wystarczającym. Autor pisze o USA, inne kraje są w gorszej sytuacji, jako, że Stany Zjednoczone posiadają jeden z najsilniej rozwiniętych przemysłów IT. Taki stan rzeczy sprawia, że system cybernetyczny jest rozproszony, także pod względem źródeł technologii, zatem problem walki cybernetycznej u gruntu ma charakter międzynarodowy.

Rządy muszą działać

W dalszej części artykułu zawierającego wskazania legislacyjne dla Stanów Zjednoczonych, Paul Rosenzweig koncentruje się na specyfice amerykańskiej, która nie przystaje do ogólnego opisu zjawiska rywalizacji cybernetycznej. Pewnym jest, że nowy front w dziedzinie bezpieczeństwa został na dobre otwarty, a rolą państwa jest jego zabezpieczenie.

Państwo potrzebuje dobrze wykształconej i rozbudowanej grupy informatyków – specjalistów do spraw bezpieczeństwa w sieci, innowacji w dziedzinie cybernetyki oraz odpowiednich regulacji prawnych, pozwalających na wdrożenie skutecznej aktywnej obrony w sieci. Ten kto nie idzie naprzód – cofa się. W wymiarze cyberprzestrzeni to powiedzenie sprawdza się w pełni.

Wojciech Jakóbik

Linki: http://www.cnbc.com/id/41311587

http://www.washingtontimes.com/news/2011/jan/31/report-warns-iran-nuclear-disaster/?page=2

http://www.heritage.org/Research/Commentary/2011/01/Obama-Needs-to-Address-Our-Cyber-Warfare-Gap-with-China

http://www.heritage.org/Research/Reports/2011/01/10-Conservative-Principles-for-Cybersecurity-Policy#_ftn1