USA – wirtualne mocarstwo

1 czerwca 2009

Wojna w okopach to już przeszłość, a w kosmosie – to ciągle przyszłość. Dzisiaj najgroźniejsze wojny toczą się w cyberprzestrzeni.

Internet sprzyja prowadzeniu wojen. Wojny w sieci są bardziej demokratyczne: sprzęt – choć drogi, kosztuje i tak mniej niż wyposażenie nowoczesnej armii. Zresztą sam sprzęt nie decyduje o zwycięstwie, a najzdolniejsi informatycy i programiści nie rodzą się tylko w Stanach Zjednoczonych. Ba, nie rodzą się tylko w krajach demokratycznych.

Takie państwa, wysyłając najzdolniejszych studentów na zachodnie uniwersytety, zyskują szeroki dostęp do wiedzy, nie dzieląc się własną.

Internet to także znakomity kanał propagandowy, wykorzystywany zarówno wobec własnych obywateli, jak i zagranicy.

To przede wszystkim jednak źródło informacji. Informacji ważnych, ale niekoniecznie ukrytych – często zawieruszonych gdzieś w czeluściach cyberprzestrzeni i czekających na odkrycie. Część z nich to zwykłe informacyjne śmieci, chociaż paparazzi – grzebiąc w śmieciach celebrytów, często zyskują w ten sposób sensacyjne i słono opłacane historie okładkowe.

Groźna dla narodowego bezpieczeństwa jest więc nie tylko internetowa partyzantka, ale też zbieracze złomu, z którego można złożyć całkiem groźny internetowy czołg.

Najważniejszą jednak zaletą sieci w kontekście prowadzenia wojen, jest brak powszechnych norm prawnych, a często nawet – brak uregulowania w obrębie terytoriów poszczególnych państw. Jak zresztą mierzyć „przynależność” państwową sieci? Obywatelstwem hakerów? Miejscem położenia serwerów? Miejscem rejestracji domeny?

Wszystkie te potencjalne zagrożenia byłyby dzisiaj śmieszne, gdyby kolejne rządy niemal wszystkich państw, ze Stanami Zjednoczonymi na czele, nie ignorowały Internetu. Ostatnią szansę na zbudowanie systemu bezpieczeństwa sieci komputerowych zaprzepaścił George W. Bush. Jego Patriot Act mógł być przyczynkiem do edukacji społeczeństwa w zakresie cyberbezpieczeństwa. Skończyło się na oburzeniu z powodu monitorowania prywatnych e-maili. Wtedy jeszcze Internet znajdował się w fazie 1.0 – nie było społeczności, a i globalny wymiar sieci nie był do końca taki znowu globalny. Dzisiaj jest inaczej: równie dobry sprzęt jak agendy rządowe USA, mają rządy innych krajów, a także grupy terrorystyczne.

W Iraku Amerykanie już wykorzystywali sieć komputerową do walki z Al-Kaidą. Aby zwabić terrorystów w przygotowaną zasadzkę, informatycy pracujący dla US Army włamywali się na strony ugrupowania i odpowiednio modyfikowali informacje tam zamieszczone.

Każdego dnia amerykańską cyberprzestrzeń nękają ataki hakerów – najczęściej z Chin i Rosji. Chociaż oficjalnie te państwa utrzymują z USA dobre stosunki (zwłaszcza Chiny), a ich rządy odcinają się od działań cyberterrorystów, sama sytuacja pokazuje, jak niebezpieczna jest cyberwojna. Można ją prowadzić cicho i z miarę czystymi rękoma, cały czas uśmiechając się do atakowanego partnera. Trudno bowiem zebrać dowody wrogiej działalności, zwłaszcza samemu pozostając „czystym”.

Opracowywane przez Pentagon technologie pozwalałyby dostać się do chińskiego czy rosyjskiego serwera i zniszczyć znajdującą się tam aplikację, która – już po przedostaniu się do amerykańskich komputerów – łączyłaby je w jedną, sterowalną z Chin czy Rosji, sieć.

Problemem jest…zgoda samego prezydenta na udział Stanów Zjednoczonych w cyberwojnach. Do tej pory tego typu działania były osobiście zatwierdzane przez George’a W. Busha. Obecny

prezydent chce większej otwartości i pewnej uniwersalności stworzonych przez jego rząd rozwiązań.

Pierwszym krokiem było upublicznienie raportu na temat cyberbezpieczeństwa, a także zapowiedź powołania eksperta zajmującego się tą kwestią w administracji Obamy.

Prezydent przyznał też, że sam padł ofiarą cyberataków, w wyniku których skradziono wiele informacji dotyczących kampanii prezydenckiej.

W firmowanym przez prezydenta raporcie, podkreślana jest konieczność współpracy rządu z sektorem prywatnym. To nie tylko oszczędność pieniędzy obu stron, ale przede wszystkim – wypracowanie standardów, w tym prawnych, a także stworzenie infrastruktury, które przetrwają na następne lata: – „To nasz zasób strategiczny" – skomentował Obama.

Plan przedstawiony przez Baracka Obamę obejmuje też narodowy dialog i akcję edukacyjną na temat bezpieczeństwa w sieci, zwłaszcza dotyczącego ochrony danych osobowych.

Oprócz dialogu wewnątrz Stanów, Obama chce wyjść z inicjatywą międzynarodowych prac nad utworzeniem minimalnych standardów ochrony sieci komputerowych i sposobów ich egzekwowania.

Dzięki Internetowi można zrobić karierę, znaleźć pracę, męża, a nawet wygrać wybory prezydenckie: granica między wirtualną a realną rzeczywistością jest coraz cieńsza.

Wojna wirtualna może błyskawicznie zmienić się w realną, chociażby przez skutki spustoszenia cyberprzestrzeni, które są bardziej dotkliwe, choć mniej przemawiające do wyobraźni, niż pustynie po wybuchu bomby nuklearnej.

Chociaż kilkugodzinna awaria wyszukiwarki Google sprzed kilku tygodni, dla niektórych jawiła się jako apokalipsa.

Autor: Magdalena Górnicka
Źródło: Portal Spraw Zagranicznych