Perspektywy cyber-bezpieczeństwa Unii Europejskiej

30 kwietnia 2009

XXI wiek niesie ze sobą wiele nowych wyzwań, lecz duża ich część jest stricte powiązana z niepohamowanym rozwojem technologicznym. Cyber-ataki na Estonię, Litwę i Gruzję były tego groźnym memento.

Historia uczy, że kiedy następuje względna stabilizacja zawsze pojawia się nowe zagrożenie, które generuje sytuacje prowadzące do zaogniania wygasłych konfliktów lub tworzenia nowych. XXI wiek niesie ze sobą wiele nowych wyzwań, lecz duża ich część jest stricte powiązana z niepohamowanym rozwojem technologicznym.

Kiedy Zimna Wojna dobiegła końca a razem z nią (pozornie) wyścig zbrojeń, wydawało się, że status quo zostało osiągnięte, i trzeba wiele aby ten stan rzeczy zburzyć. Takie, niewątpliwie racjonalne podejście miało rację bytu przez wiele lat. Jednak okazuje się, że powstała nowa sfera, sfera w której dochodzi do tzw. nowego wyścigu zbrojeń. W dzisiejszym skomputeryzowanym i zautomatyzowanym świecie, bronią stał się komputer. Nie jest to jednak broń zwykła czy też konwencjonalna. Komputer stał się bronią wielowymiarową, która jednocześnie może stać się narzędziem manipulacji gospodarkami, systemem kontroli broni militarnej czy nieocenioną metodą w wojnie informacyjnej.

Od roku 2007 Europa zderzyła się z wirtualną rzeczywistością. Estonia stała się pierwszą ofiarą, której nie udało się uchronić przed cyber-atakiem. Zaraz po tym, jak przeniesiono pomnik żołnierzy Armii Czerwonej z centrum Tallina na miejski cmentarz, doszło do cybernetycznego ataku na setki witryn

rządowych ale nie tylko- ofiarami ataku padały strony serwisów informacyjnych a także banków. Zastosowano wtedy tzw. atak DdoS (Distributed Denial of Service). Polega on na łączeniu się z konkretnymi stronami internetowymi tysiące razy, wykorzystując komputery zupełnie postronnych osób. To prowadzi do kompletnej blokady serwisów, których serwery nie są w stanie obsłużyć takiej ilości klientów jednocześnie. Atak ten spowodował paraliż całego kraju, gdyż nie było możliwe przeprowadzanie transakcji finansowych w wielu bankach, system komunikacji szwankował, a strony władz państwowych nie mogły udzielać żadnych wyjaśnień, gdyż same uległy atakowi. Jak się okazało po pewnym czasie, za atakami stała prokremlowska młodzieżówka, której członkowie sami przyznali się do zorganizowania tej akcji. Miał to być protest wobec zachowania władz estońskich w odniesieniu do pomnika żołnierzy Armii Czerwonej.

Atak ten spowodował mobilizację Sojuszu Północnoatlantyckiego. W roku 2008 stworzono centrum ds. cyber-obrony, z siedzibą w Tallinie. Miało ono przeprowadzać symulacje, tworzyć specjalne systemy zabezpieczeń a także przedkładać praktyczne projekty, mające na celu tworzyć podstawy cyber-bezpieczeństwa w NATO. Oczywiście chodziło o bezpieczeństwo systemów informatycznych samej instytucji a nie krajów członkowskich. Jak się jednak okazuje, centrum to nie funkcjonuje, a przynajmniej nie tak jak powinno. Powodem takiego stanu rzeczy, jest fakt obciążenia zarzutami o współpracę z rosyjskim wywiadem, pomysłodawcy i głównego dyrektora tegoż centrum. To spowodowało pewnego rodzaju klincz, z którego wyjścia nie znaleziono po dziś dzień.

Jednak estoński przykład to nie jedyny taki w Europie. W roku 2008 doszło aż dwa razy do podobnych incydentów. Pierwszy miał miejsce na Litwie. Niedługi czas po ogłoszeniu zakazu używania i posiadania symboli Związku Radzieckiego, setki stron rządowych zostało przejętych i podmienionych na inne. Zazwyczaj przedstawiały one symbole sowieckie wraz z

niecenzuralnymi tekstami odnoszącymi się do władz Litwy. Był to atak mniej paraliżujący niż ten z 2007 roku, lecz ukazujący jak prostym jest włamanie do systemów informatycznych należących do władz państwa.

Chronologicznie rzecz ujmując, kolejną ofiarą cyber-ataku stała się Gruzja. Miało to miejsce podczas, a tak naprawdę tuż przed, wkroczeniem armii rosyjskiej na teren Abchazji i Osetii Południowej. Atak miał charakter mieszany, co oznacza kombinację ataków DDoS i przejmowania niektórych witryn. Nie można oprzeć się wrażeniu, iż był to element normalnej rozgrywki wojennej. Paraliż informacyjny jaki zaistniał w Gruzji sprzyjał regularnym działaniom wojennym.

Wszystkie powyższe przypadki mają jeden wspólny mianownik – Federacja Rosyjska. Pomimo braku niezbitych dowodów, wszystkie trzy incydenty miały powiązanie z sytuacjami, w których dochodziło do zagrożenia interesów Moskwy. Można to porównać do niegdysiejszego „prężenia muskułów", chęci pokazania, że oprócz Stanów Zjednoczonych i Chin jest jeszcze trzeci znaczący „gracz" biorący udział w wojnie strategicznej w cyberprzestrzeni. Jest to broń o tyle skuteczna, że zdobycie bezsprzecznych dowodów jest praktycznie niemożliwe, a efekt ataku – bardzo znaczący.

Niezależnie jednak od tego, czy za atakami stała Rosja czy też nie (dywagacje bezdowodowe są tylko insynuacjami) widać, iż tworzy i nabiera siły nowe zagrożenie dla bezpieczeństwa – cyber-atak. Unia Europejska stanęła przed niewątpliwym problemem. Możliwość manipulacji informacjami, niezauważalny wpływ na gospodarki poszczególnych członków UE ale także na samą machinę tej organizacji, powinno powodować zdecydowane reakcje. Tak się jednak nie dzieje. Jest to dość szczególne postępowanie. USA, będące najmocniej informatycznie zabezpieczonym krajem świata, nie ustrzegają się infiltracji swoich systemów, jedyne co jest ich siłą to fakt, że dostrzegają takie ataki i mogą im choć w minimalny sposób przeciwdziałać. W UE systemu obrony nie ma.

Oczywiście najlepiej rozwinięte kraje Unii mają swoje wewnętrzne systemy, jednakże nie dochodzi do ujednolicenia względem innych członków, co stanowi o słabości całej UE. Przepływ informacji jest bowiem nieustającym procesem zachodzącym pomiędzy państwami członkowskimi. W taki o to sposób, dane chronione w jednym państwie w sposób zadowalający, dostają się do systemów słabo chronionych i są narażone na przechwycenie. System SIS, mający pomagać krajom należącym do Shengen w walce ze zorganizowaną przestępczością, również nie jest dopracowany. Sama jego idea jest godna pochwały, lecz sam sposób realizacji już nieco mniej. Faktem jest, że informacje na temat przestępców przekazywane są w sposób bardzo szybki, jednak bazy danych nie są należycie chronione- to generuje możliwość manipulacji danymi krążącymi w całym systemie a także w samym tzw. panelu centralnym, który ma za zadanie kierować całością przedsięwzięcia.

Jest to jedynie przykład na potwierdzenie tezy, że Europa nie jest bezpieczna od cyber-ataków. Największym problemem zdaje się być jednak obserwacja zjawiska. Brak prognoz oraz przewidywania potencjalnych przyszłych działań, stwarza ryzyko braku odpowiedniego przygotowania na ataki. USA po atakach z 11 września 2001 roku, odeszły od praktyki analizy wyłącznie zdarzeń, które już miały miejsce. Teraz głównie bazuje się na tworzeniu symulacji, które mają ukazywać nowe niebezpieczeństwa. Pytanie brzmi – co musi się stać, aby ten sposób myślenia zaczął być dostrzegany, doceniany i wprowadzony w życie w Unii Europejskiej?

Autor: Piotr Borkowski
Źródło: Portal Spraw Zagranicznych