W poniedziałek opublikowano raport Organizacji Współpracy Gospodarczej i Rozwoju (OECD) na temat cyberbezpieczeństwa w XXI wieku. Brytyjscy naukowcy – autorzy dokumentu – zbadali, w jaki sposób przestępczość wirtualna może wpływać na losy państw i świata . Czy w przyszłości komputery staną się takim samym orężem wojennym, jak broń, samoloty lub czołgi?

Peter Sommer i Ian Brown tworząc „Zmniejszanie systemowego zagrożenia cyberbezpieczeństwa", szukali odpowiedzi na pytanie o rolę systemów IT nie tyle w rozwoju ludzkości, ile w współczesnych konfliktach krajowych i międzynarodowych. Okazuje się, że pojedyncze ataki komputerowe nie grożą paraliżem poszczególnych państw, ale już ich właściwie skoordynowana kombinacja – owszem. „Szerokim echem odbiło się wykrycie w 2010 roku robaka Stuxnet. Ten samodzielnie rozprzestrzeniający się program komputerowy miał za zadanie szpiegować i przeprogramowywać instalacje przemysłowe, zawirusowując sterowniki PLC kontrolujące działanie fabryk, elektrowni itp. Do tej pory nie wiadomo, kto wykorzystywał Stuxnet'a, ale pewne jest, że niebezpieczeństwo ponownych infekcji rośnie. Mimo to - co jednoznacznie wskazali autorzy raportu – cyberataki nie mają póki co globalnego wymiaru, jednak lokalnie potrafią wyrządzić duże szkody." – komentuje Łukasz Nowatkowski, ekspert ds. bezpieczeństwa IT z firmy G Data Software.

Trzeba jednak pamiętać, że z czasem komputery będą coraz częściej wykorzystywane jako broń w starciach między państwami. „Wiąże się to przede wszystkim z postępem technologicznym, jak i z relatywnie niskim kosztem tego typu działań. Prowadzenie 'tradycyjnej' wojny to spore nakłady finansowe: sprzęt, armia – to wszystko kosztuje majątek. Cyberatak natomiast wymaga jedynie rozpoznania obiektów, umiejętności pisania kodu i podjęcia – nierzadko politycznej – decyzji. Dodatkowo krajom nie trudno jest ukryć prowadzenie badań nad wirtualnym napadem: prawie każdy narodowy departament rozwoju, zajmujący się obronnością, ma wiedzę na ten temat lub przynajmniej możliwość jej zdobycia." - podsumowuje Nowatkowski.

W reakcji na raport, rządy Stanów Zjednoczonych i Wielkiej Brytanii już zapowiedziały , że kwestie cyberbezpieczeństwa będą traktowane priorytetowo. „Zarówno USA jak i UK jakiś czas temu podjęły starania o uszczelnienie obrony przed atakami wirtualnymi. Na wyspach dobrze funkcjonuje Biuro Bezpieczeństwa Cybernetycznego i Ochrony Informacji, a w Stanach ułożona nawet została ścieżka kariery i rozwoju dla specjalistów z tego właśnie zakresu. Polska ma jeszcze dużo do zrobienia, by zapobiec potencjalnym komputerowym atakom, chociaż możemy liczyć na pomoc Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), której jesteśmy członkiem. Trzeba także pochwalić się najnowszym, napawającym dumą i optymizmem, osiągnięciem naukowców z Wojskowej Akademii Technicznej, którzy stworzyli urządzenie do szyfrowania przesyłanych danych informatycznych, niemożliwych do odkodowania 'nawet gdyby połączyć wszystkie komputery w sieci i kazali im pracować tyle lat, ile istnieje wszechświat'." – podsumowuje ekspert G Data Software.

G Data Software