Cyberatak byłby katastrofą dla Wielkiej Brytanii

13 stycznia 2013

Komitet Obrony w Departamencie Obrony Wielkiej Brytanii ostrzegł, że brytyjskie Ministerstwo Obrony (MoD), pozostaje wysoce podatne na cyberataki i musi zrobić więcej, by wesprzeć jego obronę. Podkreśla się obawy, że brytyjska armia zależy od technologii, dla których nie posiada sprawdzonych zabezpieczeń, pozostawiając brytyjskie siły na ryzyko „śmiertelnego zagrożenia" ze strony sieci cyfrowych.

W swoim bardzo krytycznym sprawozdaniu odnośnie rządowej cyberstrategii, komisja stwierdza: „Rząd musi wprowadzić – jeśli tego jeszcze nie uczynił – mechanizmy, ludzi, wykształcenie, umiejętności, myślenie i politykę, które biorą pod uwagę zarówno możliwości i luki, które daje cyberprzestrzeń. Nadszedł czas by rząd zwrócił uwagę na ten temat".

Cyberbezpieczeństwo pozostaje najważniejszym priorytetem dla koalicji rządzącej w Wielkiej Brytanii, z budżetem ok. 650 mln funtów. Ma na celu wzmocnić obronę brytyjską, promować kampanie bezpieczeństwa w sieci oraz zapewnić dodatkowe inwestycje dla krajowego wywiadu GCHQ (Governmental Communication Headquaters).

„Dowody, jakie otrzymaliśmy, stawiają nas w poczuciu niepokoju, ponieważ siły zbrojne są uzależnione od technologii informacyjnych i komunikacyjnych, które to systemy mogą na trwałe ucierpieć w cyberataku, a ich zdolność do pracy mogą okazać się śmiertelnym zagrożeniem" – czytamy w raporcie. „To nie jest wystarczające dla sił zbrojnych, aby zrobić wszystko, by zapobiec atakowi… rząd powinien określać szczegóły planów gotowości na miejscu, o ile taki atak nastąpi Jeśli nie ma żadnego, należy to zrobić. I pilnie jakiś stworzyć".

Opinia odnośnie programu Strategia Obrony i Bezpieczeństwa 2010 poinstruowała wszystkie departamenty rządowe, aby umieścić cyberobronę na szczycie ich programów. Posłowie, którzy są autorami raportu wzywają do większego zaangażowania się w tej sprawie. „To jest nasz pogląd, że cyberbezpieczeństwo jest na tyle poważne, znacząca i kompleksowa aktywność w tej dziedzinie zapewni zwiększeniem ministerialnej uwagi. Właściwy minister powinien mieć uprawnienia do kierowania ministerstwami aby podjąć działania, jeżeli nie występuję one jako wymagane”.

Raport zwraca też uwagę na niewygodnej rzeczywistości, dzięki zeznaniom ekspertów wywiadowczych GCHQ. Ich urzędnicy przyznali, że: „Największe zagrożenie elektronicznego ataku nadal stwarzane jest przez podmioty państwowe w tym przede wszystkim Rosję i Chiny, które stoją za większością ataków. Ich cele są w rządzie, jak również w przemyśle”.

Opracowanie: ECAG
Na podstawie: www.securitydefenceagenda.org
Źródło: Geopolityka.org