Cyberdefence 24

aut. Tomasz Fastyn 08.07.2016

SZCZYT NATO: MEDIA SPOŁECZNOŚCIOWE TEŻ SĄ NARZĘDZIEM WALKI HYBRYDOWEJ

Według raportu przygotowanego przez NATO Strategic Communications Centre of Excellence (COE) przestrzeń mediów społecznościowych może w rękach nieodpowiednich osób stać się narzędziem do prowadzenia wojny hybrydowej. To szczególnie ważne w kontekście aktualnie trwającego szczytu NATO, na którym internet zostanie uznany za przestrzeń działań wojennych.

Jak wynika z raportu przygotowanego przez COE przestrzeń cybernetyczna będzie w najbliższych latach rosnąć w tempie dużo większym niż do tej pory. To za sprawą rozwoju nowych technologi i globalizacji zjawiska internetu rzeczy (Internet of Things - IoT), które jest w ostatnim czasie szczególnie narażone na ataki cybernetyczne. – Szybki wzrost oraz używanie internetu jako jednej z typowych codziennych czynności czy to na portalach społecznościowych czy za pomocą mobilnych aplikacji pokazuję w jaką stronę będzie się kierować rozwój sieci – czytamy w raporcie.

Działania w cyberprzestrzeni nie posiadają rozgraniczenia pomiędzy strefą wojenną i pokojową, szczególnie w przypadku hakerów powiązanych z siłami Rosji oraz Daesh. W przypadku obu tych aktywnych aktorów w przestrzeni sieciowej widać, pewne podobieństwa w strategi działań wojny hybrydowej. W raporcie wymienione są tylko niektóre zaobserwowane sposoby walki takie jak – fałszywe zdjęcia, fałszywe konta na portalach, sianie plotek, dezinformacja i inżyniera społeczna. Jednak prowadzenie kampanii dezinformacyjnej może przybrać także postać zwykłego trollingu internetowego czy podszywanie się pod ważne osobistości lub firmy.

Według raportu siła osób odpowiedzialnych za prowadzenie wojny hybrydowej w internecie polega na ich dopasowaniu do nowych realiów technologicznych oraz światowych wydarzeń. Szybkość działania, zarówno w przestrzeni cybernetycznej jak fizycznej jest także, jednym z atutów, który pozwala na małe zwycięstwa w internecie. Zjawisko to jest zdecydowanie łatwiejsze dzięki darmowym lub tanim narzędziom do komunikacji czy ukrywania swojego adresy IP. Hakerzy czy osoby zajmujące się prowadzeniem takich działań również bardzo łatwo przystosowują się do nowych warunków legislacyjnych czy technologicznych, są bardziej elastyczni, przez co wyprzedzają organy ścigania – jak podaję raport.

Całe zjawisko dużo szybciej zrozumieli właśnie przywódcy z Rosji i Daesh. Powiązanie władz tych podmiotów z hakerami przeprowadzającymi operacje w cyberprzestrzeni jest niemal niemożliwe. Raz uruchomiona maszynka szerzenia dezinformacji powoduję jej dalszą penetrację i poszerzanie przekazu, internauci popierający informacje przekazywane za pomocą internetu stają się kolejnym nośnikiem tej informacji.

Brak zaangażowania organów decydujących o bezpieczeństwie na różnych szczeblach w sprawy związane z działaniami na portalach społecznościowych powoduję, że państwa przegrywają z dezinformacją w sieci. Dłuższe ignorowanie tej strefy nie może mieć miejsca – czytamy w podsumowaniu raportu.

Czytaj też: Amerykańska strategia odstraszania chińskich hakerów nie działa