Cyberdefence 24

aut. Andrzej Kozłowski 08.05.2019

ATAK IZRAELA NA CYBERJEDNOSTKĘ HAMASU. TAKICH INCYDENTÓW BĘDZIE CORAZ WIĘCEJ [KOMENTARZ]

Media na całym świecie obiegła informacja o zbombardowaniu jednostki hakerów Hamasu przez izraelskie siły powietrzne. Incydent ten pokazuje, że cyberprzestrzeń i jednostki, które w niej operują stały się elementem konfliktu zbrojnego, a tego typu incydenty będą się powtarzać.

W zeszłym piątek wybuchły walki pomiędzy Hamasem i Izraelem. Palestyńczycy wystrzelili kilkaset pocisków, a Izrael odpowiedział uderzeniem w ponad 300 celów. Do działań ofensywnych miały przyłączyć się jednostki hakerów Hamasu, które próbowały dokonać ataku na systemy teleinformatyczne infrastruktury krytycznej w Izraelu. Zagrożenie miało zostać zneutralizowane przez połączony wysiłek Shin Betu i jednostki 8200. Następnie siły powietrzne Izraela dokonały nalotu na jednostkę palestyńskich hakerów.

Nie wiadomo dokładnie, ile osób zginęło w bombardowaniu. Należy podkreślić, że Izrael to państwo dysponujące jednym z najbardziej zaawansowanych zdolności działania w cyberprzestrzeni i już wcześniej łączył operacje w jej ramach z konwencjonalnymi działaniami.

Po pierwsze, warto zauważyć, że to nie pierwszy przypadek, gdy hakerzy zamieszani w cyberataki zostają fizycznie wyeliminowani. W 2015 roku, obywatel brytyjski Junaid Hussain, który służył w ISIS, został zabity przez pocisk wystrzelony z drona. Według przedstawicieli amerykańskiego wywiadu, był autorem licznych cyberataków,w tym tego wymierzonego w stronę i konto na Twitterze US Central Command. Miał również wykraść a następnie ujawnić dane amerykańskich żołnierzy w sieci, w tym ich adresy zamieszkania, co mogło doprowadzić do bezpośredniego zagrożenia ich życia. Różnica w tym przypadku jest taka, że izraelski atak nastąpił bardzko szybko po incydencie i stanowił bezpośrednią odpowiedź na konkretny cyberatak. Zresztą tego typu wydarzenia, będą się powtarzać w przyszłości. Państwa takie jak np. Stany Zjednoczone oficjalnie deklarują, że w odpowiedzi na cyberatak mogą użyć siły kinetycznej, a w uzasadnionych przypadkach nawet arsenału nuklearnego. Oczywiście odpowiedź powinna być proporcjonalna.

W tym obszarze pojawia się kolejny problem związany z izraelskim uderzeniem. Z doniesień IDF wynika, że cyberatak Hamasu nie był zbyt zaawansowany i miał na celu zaszkodzić jakości życia izraelskich obywateli. Z podanego komunikatu wynika, że nie było zagrożone ani życie ludzkie ani infrastruktura krytyczna. Czy w takim razie doszło do złamania prawa międzynarodowego?

Kolejna interesująca kwestia to namierzenie kwatery cyberjednostki Hamasu. Czy Izarel znał jej lokalizację wcześniej? Czy też może podczas przeprowadzania cyberataku, palestyńscy hakerzy nie zatarli swoich cyfrowych śladów, ujawniając swoje położenie? Tego nie wiadomo i wątpliwe, żeby Izrael ujawnił takie wrażliwe informacje. Zdradziłby w ten sposób swoje zdolności wywiadowcze.

Warto również zastanowić się dlaczego IDF pochwaliło się zniszczeniem właśnie takiego celu. W przeprowadzonych nalotach ucierpiało wiele jednostek i struktur Hamasu, ale nie stały się one tematem żadnego z Tweetów. Być może istotny jest też wymiar propagandowy i wiadomość, którą Izrael chciał przekazać swoim wrogom, że nawet sprawcy cyberataków zostaną znalezieni i wyeliminowani.

Przykład Hamasu pokazuje też, że nie tylko państwa, ale również organizacje terrorystyczne kładą coraz większych nacisk na działania w cyberprzestrzeni, tworząc wyspecjalizowane jednostki. Oczywiście Internet od dawna wykorzystywany jest przez podmioty niepaństwowe do różnych celów. Al-Kaida wykorzystywała go głównie do szeroko pojętych działań logistycznych, szerzeniu propagandy, wymianie informacji czy pozyskiwaniu funduszy. Jej strategię rozwinęło ISIS, które na ten wymiar położyło o wiele większy nacisk. Zaangażowało się również w stosunkowo proste cyberataki. Jak widać Hamas idzie w ślady Daesh i rozwija swoje zdolności w cyberprzestrzeni. Przykłady te pokazują, że jednostki do prowadzenia działań w tym obszarze stają się coraz powszechniejsze.

Niestety, incydent ten pokazuje też jak bardzo Polska jest opóźniona w stosunku do innych podmiotów, w tym aktorów niepaństwowych, jeżeli chodzi o rozwój i działanie w cyberprzestrzeni. W naszym kraju dopiero powstaje koncepcja Wojsk Obrony Cyberprzestrzeni, podczas gdy takie siły aktywnie angażują się w obecne konflikty zbrojne, zarówno po stronie państw, jak i organizacji terrorystycznych. Dlatego warto zadać sobie pytanie, jak polskie wojsko przygotowane jest do nowoczesnego konfliktu, który z pewnością zacznie się w cyberprzestrzeni?