

## ISIS (ZBYT)TRUDNYM PRZECIWNIKIEM DLA USCYBERCOM

---

USCYBERCOM miało duże problemy z pokonaniem ISIS w cyberprzestrzeni – wynika z nowych dokumentów opublikowany w Stanach Zjednoczonych. Amerykanie napotkali trudności m.in. z identyfikacją celów, tempem operacji czy wewnętrznymi konfliktami między instytucjami zaangażowanymi w działania. W jednym przypadku niefrasobliwość żołnierzy mogła narazić na szwank zdolności USCYBERCOM.

Operacja Glowing Symphony skierowana przeciwko ISIS w sieci była oficjalnym debiutem nowego amerykańskiego dowództwa USCYBERCOM. Do jej prowadzenia stworzono specjalną grupę zadaniową Ares. Rozpoczęła się ona w 2016 roku a jej celem było zniszczenie sieci i systemów ISIS, co miało ograniczyć zdolności rozprzestrzeniania propagandy oraz komunikowania się członków organizacji. Wcześniej Amerykanie nie prowadzili działań ofensywnych na taką skalę. Działania te zakończyły się ostatecznie sukcesem a sieci komputerowe Daesh zostały sparaliżowane, to jednak w trakcie operacji pojawiło się wiele problemów. Żołnierze napotkali trudności ze zbieraniem informacji oraz ich przechowywaniem. USCYBERCOM nie było przygotowane do radzenia sobie z taką wielką ilością danych, które pojawiły się w trakcie operacji. Amerykanie zebrali terabajty danych i nie byli w stanie ich wykorzystać pomimo, że zbieranie danych z serwerów ISIS i ich wykorzystanie w dalszej działalności było wcześniej zaplanowane jako element operacji. W opublikowanych dokumentach podsumowujących operację przeciwko ISIS sugeruje się, że USCYBERCOM powinno stworzyć procedury pozyskiwania i zarządzania informacjami na wypadek przyszłych działań.

Pojawiły się również konflikty między różnymi instytucjami zaangażowanymi w działania przeciwko ISIS, które doprowadzały do opóźnienia w podejmowanych przez USCYBERCOM operacjach. W dokumencie przyznano, że procedury współpracy między agencjami nie zostały przygotowane z myślą o operacjach w cyberprzestrzeni, które charakteryzują się niezwykłą dynamiką oraz skalą. W operację Glowing Symphony był zaangażowany Departament Sprawiedliwości, CIA, NSA oraz inni członkowie amerykańskiego rządu. Operacje opóźniły również przedłużające się dyskusje w Narodowej Radzie Bezpieczeństwa na temat celów i zakresu działań. Bardzo ważnym wnioskiem jest również, fakt, że operacja zniszczenia sieci ISIS pozostawała w sprzeczności z operacjami wywiadowczymi prowadzonym przez np. NSA. Problemy były również z identyfikacją i weryfikacją celów - proces ten okazał się zbyt długi i zbyt skomplikowany. Inne agencje napotkały też trudności w procedurze sprawdzania czy inne działania USCYBERCOM nie wpłynęły negatywnie na czynności innych instytucji.

W jednym przypadku jeden z żołnierzy wykazał się również niedbalstwem, co prawie umożliwiło wykrycie amerykańskich aktywności przez ISIS oraz naraziło zdolności USCYBERCOM. W celu uniknięcia podobnych sytuacji w przyszłości Departament Obrony rekomenduje zachowanie większej ostrożności w kolejnych działaniach i odradza się podejmowanie niepotrzebnego ryzyka, które może pozwolić na odkrycie działań podejmowany przez USCYBERCOM.

Negatywnie o działaniach USCYBERCOM wypowiedział się również były sekretarz obrony Ash Carter,

który w 2017 roku opublikował wpis na Harvard Kennedy School's Belfer Center for Science and International Affairs. Wyraził w nim rozczarowanie kampanią prowadzoną przeciwko ISIS przez USCYBEROM a także wspomniał, że działania były niweczone przez społeczność wywiadowczą, która opóźniała i jak tylko mogła przeszkadzała w prowadzeniu operacji argumentując, że utrudni im to zbieranie informacji. Wnioski Cartera okazały się być są zbieżne z opublikowanymi dokumentami.

Dokumenty Departament Obrony wskazują również, że rząd Stanów Zjednoczonych musi rozbudować siły odpowiedzialne za ofensywne działania w cyberprzestrzeni żeby skutecznie przeciwstawić się zagrożeniu ze strony o wiele potężniejszych aktorów niż ISIS czyli Rosji, Chin, Iran i Korei Północnej.

Obecny dowódca USCYBERCOM, który sprawuje także pieczę nad Agencją Bezpieczeństwa Narodowego (NSA) powiedział, że operacja Glowing Symphony była drogowskazem dla innych zespołów w USCYBERCOM, które zwalczały innych przeciwników i odpowiadał m.in. za atak na rosyjską Internet Research Agency.

W 2018 roku USCYBERCOM zmieniło swoje wewnętrzne procedury. Także na poziomie strategicznym doszło do poważnych zmian wraz z pojawieniem się Presidential Policy Directive 20, które wprowadzało nowy proces akceptowania cyberataku znacznie go upraszczając.