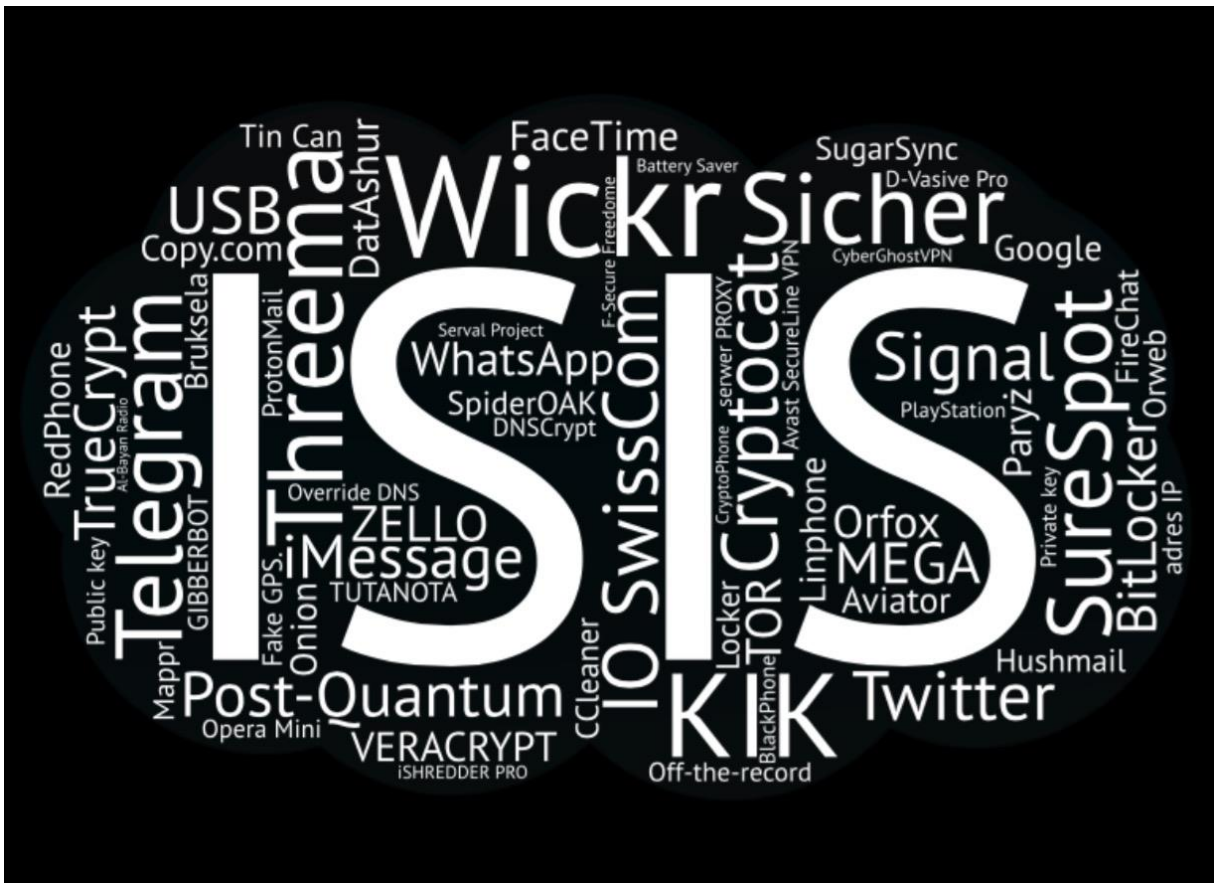
Security
in practice

Metody komunikacji Państwa Islamskiego (ISIS)

Opracował: Jacek LASHMANN

Materiał jest streszczeniem rozdziału opracowania opublikowanego oryginalnie w: K. Danielewicz (red.), Państwo Islamskie (ISIS), historia powstania, taktyka działania, Oświęcim 2019, s. 93-120.



Wprowadzenie

Na co dzień nie rozstajemy się z naszymi smartfonami, nosimy je wszędzie ze sobą – w kieszeni dżinsów, marynarki czy w damskiej torebce. Według badania z 2016 roku opublikowanego przez „Daily Mail”[1] przeciętny użytkownik smartfona dotyka ekranu 2617

[1] S. Liberatore, *Are YOU obsessed with your phone? Researchers reveal addicts touch their handset over 5,400 times a DAY*, „ Daily Mail”, 27.06.2017, http://www.dailymail.co.uk/sciencetech/article-3662555/Are-obsessed-phone-Researchers-reveals-addicts-touch-handset-5-400-times-DAY.html, 27.07.2017.

razy na dzień, a osoby uzależnione – nawet 5400 razy dziennie. Najczęściej korzystamy z aplikacji Facebooka i różnych komunikatorów internetowych. Jeszcze jedenaście lat temu telefon komórkowy służył nam do funkcji, do których został stworzony, czyli telefonowania i komunikowania się za pomocą krótkich wiadomości tekstowych. Krokiem milowym w rozwoju nowoczesnych technologii było zaprezentowanie przez Steve'a Jobsa w 2007 roku pierwszego smartfona firmy Apple – iPhone'a. Od tego momentu rozpoczął się dynamiczny rozwój technologii i urządzeń mobilnych, co doprowadziło do tego, że telefony komórkowe przeszły transformację, stając się smartfonami, czyli przenośnymi urządzeniami zdolnymi robić rzeczy zarezerwowane wcześniej wyłącznie dla komputerów. Można by się rozwodzić nad zaletami smartfonów oraz ułatwień, jakie wniosły w nasze codzienne życie, ale niestety – jak zwykle – jeśli są zalety, to muszą być i wady. To właśnie smartfony stanowią główne narzędzie używane do komunikacji przez dżihadystów.

Zanim Państwo Islamskie (IS-Islamic State) zaczęło używać bardziej zaawansowanych technologicznie metod komunikacji, do szerzenia swojej propagandy wśród mieszkańców zamieszkujących Syrię i Irak wykorzystywało ulotki oraz gazetki, rozprowadzane w takich dużych miastach, jak Rakka i Mosul, a także billboardy. Następnie rozpoczęło nadawanie w 13 prowincjach audycji radiowych na paśmie FM, zawierających różne treści: od wiadomości po kazania, modlitwy, poezję, aż do emitowania treści poradników dla dżihadystów. W związku z tym, że IS rosło w siłę i zwiększało swój obszar działania, naturalną potrzebą stało się wprowadzenie bardziej zaawansowanych i bezpiecznych środków komunikacji[2].

Podejrzenie o używanie szyfrowanych metod komunikacji pojawiło się po atakach w Paryżu 13 listopada 2015 roku, kiedy bojownicy Państwa Islamskiego zamordowali 130 osób. Standardowo po takim ataku śledczy stosują technikę analizowania śladów wstecz, sprawdzając potencjalne źródła informacji, tzn. telefony, komputery, tablety, by w ten sposób odtworzyć sieć kontaktów, współpracowników, metody planowania i przygotowywania się do zamachu, źródła finansowania itp. Po paryskich atakach śledczy jednak nie znaleźli żadnego śladu w mediach społecznościowych, w poczcie elektronicznej – kompletnie nic, co zostawiłoby jakiś cyfrowy ślad. Czy to możliwe w obecnych czasach?

Na tym polu dochodzi do różnicy zdań między ekspertami. Jedni twierdzą, że brak takich śladów wynika z faktu, iż terroryści nie komunikowali się za pośrednictwem poczty

[2] J. Goldsmith, *The Jihadists' Digital Toolbox: How ISIS keeps quiet on the web*, Bellingcat, 22.06.2016, https://www.bellingcat.com/news/mena/2016/07/22/the-jihadists-digital-toolbox-how-isis-keeps-quiet-on-the-web/, 03.01.2017.

elektronicznej ani mediów społecznościowych, gdyż byli bardzo zdyscyplinowani i porozumiewali się wyłącznie osobiście lub za pomocą burner phone[3], używanych często tylko do jednej rozmowy, a następnie wyrzucanych. Drudzy natomiast nie zgadzają się z tą tezą i uważają, że terroryści używali szyfrowanej komunikacji. Na potwierdzenie tego są dwa dowody[4]. Po pierwsze, wielu świadków, którym udało się uciec z klubu Bataclan, zgodnie twierdzi, iż widzieli jednego zamachowca otwierającego laptopa i korzystającego z niego. Po drugie, słyszeli również rozmowy terrorystów na temat internetu: „Dlaczego to właśnie teraz nie działa?". W jakim celu terrorysta w trakcie (w środku) ataku terrorystycznego chce się połączyć z internetem? Niektórzy świadkowie twierdzą, że widzieli na ekranie laptopa zamachowca dziwny kod. Podejrzewa się, iż chodzi o program szyfrujący o nazwie TrueCrypt, który opisany będzie w dalszej części rozdziału.

W tym miejscu warto zastanowić się, czy IS posiada sposób na komunikowanie się w sieci, którego nikt jeszcze nie odkrył i nie potrafi podsłuchać.

Rukmini Callimachi jest dziennikarką „New York Times", zajmującą się terroryzmem i działalnością Państwa Islamskiego. Przeszukuje internet, zakłada konta w różnego rodzaju mediach społecznościowych, próbuje wpiąć się do różnych wątków na czatach i forach internetowych poświęconych Państwu Islamskiemu – wszystko po to, aby wślizgnąć się do środowiska IS i zdobyć jak najwięcej informacji na ich temat.

Jak donosi Rukmini Callimachi w artykule opublikowanym w „New York Times" 29 marca 2016 roku[5], francuski wywiad w sierpniu 2015 roku schwytał 29-letniego obywatela Francji – Redę Hame'a, który opuścił Syrię z zadaniem przeprowadzenia ataku terrorystycznego we Francji. Hame, z zawodu technik branży IT z Paryża, twierdzi, iż wyjechał do Syrii z planem wstąpienia do IS w celu podjęcia walki z reżimem Bashara al-Assada. W ostateczności po przyjeździe do Syrii w czerwcu 2015 roku został skierowany na ekspresowe szkolenie dla bojowników przygotowywanych do przeprowadzania ataków w krajach zachodnich. Okazał się idealnym kandydatem do takiej misji ze względu na dwa mocne atuty. Po pierwsze, miał obywatelstwo francuskie, a po drugie – z wykształcenia był informatykiem z praktyką w firmie Astrium należącej do grupy Airbus. Jeden z etapów szkolenia odbył się w

[3] Burner phone – to tzw. telefon na kartę (prepaid), który zapewnia użytkownikowi anonimowość w takich sposób, że albo jest zarejestrowany na inną osobę, albo w kraju, w którym nie trzeba rejestrować kart prepaidowych.
[4] P.J. Vogh, A. Goldman, *How ISIS Communicates Secretly on the Internet*, „Digg", 23.04.2016, http://digg.com/2016/rukmini-callimachi-isis-reply-all, 03.01.2017.
[5] R. Callimachi, *How ISIS Built the Machinery of Terror Under Europe's Gaze*, „New York Times", 29.03.2016, http://www.nytimes.com/2016/03/29/world/europe/isis-attacks-paris-brussels.html?_r=1, 04.01.2017.

kafejce internetowej w Rakka, gdzie informatyk IS wręczył mu nośnik USB, zawierający program CCleaner, używany do usuwania historii przeglądanych stron internetowych, a także program TrueCrypt, wykorzystywany do szyfrowania informacji (w tamtym okresie jeszcze niezhakowany i bezpieczny). Hame otrzymał również szczegółowe instrukcje dotyczące bezpiecznych sposobów komunikowania się. Procedura przekazywania informacji w obie strony miała wyglądać następująco. Najpierw należało zaszyfrować wiadomość przy wykorzystaniu programu TrueCrypt, następnie przenieść (załadować) ją do folderu znajdującego się na wirtualnym dysku w komercyjnej tureckiej chmurze, do którego pełen dostęp posiadał „opiekun prowadzący" z Syrii – słynny Abdelhamid Abaaoud, uważany za scenarzystę zamachów w Paryżu. Powiedziano mu, że zabronione jest wysyłanie zaszyfrowanej wiadomości za pomocą poczty elektronicznej, gdyż może to doprowadzić do ujawnienia metadanych. Oznacza to, że nawet jeśli wiadomość przesyłana mailem była zaszyfrowana, to i tak jawne są informacje kto, kiedy i z kim się komunikował.

Reda Hame, składając zeznania na temat metod komunikowania się, opisał folder w chmurze jako martwą skrzynkę kontaktową, czyli umówione sekretne miejsce na pozostawianie wiadomości dla drugiej osoby. Opowiedział również o środkach bezpieczeństwa stosowanych w komórkowej łączności telefonicznej. Powiedziano mu, aby kontaktował się na turecki numer telefonu komórkowego, który miał znajdować się na terenie Syrii, ale na tyle blisko tureckiej granicy, żeby być w zasięgu tureckiego operatora komórkowego, IS podejrzewało bowiem, że służby bezpieczeństwa będą bardziej skłonne podsłuchiwać łączność komórkową z Europy do Syrii niż do Turcji. Po przybyciu do Pragi miał wynająć pokój w hotelu jako turysta i kupić czeską kartę komórkową pre-paid, a następnie zadzwonić na wskazany turecki numer do Syrii, wysyłając tylko pojedynczy sygnał (bez nawiązywania rozmowy). Dla jego opiekuna Abaaouda miało to oznaczać, że Reda Hame osiągnął kolejny etap misji, a to zainicjowałoby użycie folderu wirtualnego dysku w chmurze w celu przekazywania dalszych instrukcji i informacji. Francuski informatyk nie zdołał wykonać swojej misji, ponieważ inny bojownik, schwytany w Hiszpanii, zdradził plany i miejsce przebywania Hame'a. Śledząca go francuska policja dotarła do paryskiego mieszkania jego matki, w którym znaleziono nośnik USB wraz z kartką zawierającą login i hasło do programu TrueCrypt[6].

Powyższe odkrycie francuskich służb po raz pierwszy potwierdza, że dżihadyści używali szyfrowania podczas wymiany informacji. Jednakże eksperci od cyberprzestępczości

[6] *Ibidem.*

po przeanalizowaniu wspomnianych faktów mają wątpliwości, czy to było fizycznie możliwe, gdyż wymagałoby to zaszyfrowania całej zawartości dysku, a następnie załadowania go do wirtualnego dysku w chmurze, pozostawiając miejsce na ludzki błąd oraz mnóstwo cyfrowych śladów podczas każdego ładowania danych. Jeszcze większe zamieszanie wprowadziła opublikowana w „New York Times" informacja, że według policji i przesłuchań świadków paryskich ataków nie znaleziono najmniejszych śladów wymiany korespondencji elektronicznej pomiędzy terrorystami[7].

Problem jest dość złożony, gdyż stosowanie szyfrowania pozostawia ślady, a wygląda to następująco: kiedy wyśle się zaszyfrowany e-mail, ślad po nim istnieje w skrzynce odbiorczej odbiorcy i w wysłanych nadawcy, jedynie treść tego maila jest nie do odczytu. Idąc tym tropem rozumowania, ślady po mailach powinny zostać na skrzynkach sprawców paryskich ataków i adresatów w Syrii lub Iraku, chyba że używane były opisane wcześniej martwe skrzynki mailowe.

Niezaprzeczalny dowód na to, że IS stosuje szyfrowane formy komunikacji, przyniosło śledztwo po ataku w Brukseli. Śledczy przeszukujący wynajmowane przez zamachowców mieszkanie znaleźli laptopa w pobliskim śmietniku na zewnątrz. Po sprawdzeniu komputera stwierdzili, że był on najprawdopodobniej używany do planowania ataków terrorystycznych. Podczas szczegółowego sprawdzania komputera technicy napotkali wiele utrudnień na swojej drodze. Po pierwsze, zauważyli, że większość zawartości dysku została trwale usunięta, to znaczy w taki sposób, że nie można odzyskać treści zapisanych na tym nośniku. Po drugie, spostrzegli, że wszystkie dane były zabezpieczone za pomocą powszechnie dostępnego programu szyfrującego. Po trzecie, terroryści używali oprogramowania zapewniającego anonimowość i usuwającego wszelkie ślady obecności pozostawione w sieci. Dzięki wykorzystaniu najnowszego oprogramowania i narzędzi śledczym udało się odzyskać dość istotne dane. Uzyskali informacje na temat skasowanych na dobre plików, takie jak ich nazwy, czas – kiedy ostatnio były używane oraz kiedy po raz pierwszy zostały zapisane na dysku. Chociaż większość danych pozostała poza zasięgiem śledczych, to odzyskany materiał dowodowy odgrywa istotną rolę w dalszych działaniach antyterrorystycznych.

Na dysku znaleziono dużo materiałów propagandowych, zawierających między innymi nagrania Osamy bin Ladena oraz duchownego Anwara al-Awlakiego. Niektóre odzyskane pliki

[7] S. Frenkel, *Everything You Ever Wanted to Know About How ISIS Uses The Internet*, „BuzzFeedNews", 13.05.2016, https://www.buzzfeed.com/sheerafrenkel/everything-you-ever-wanted-to-know-about-how-isis-uses-the-i?utm_term=.tjDegvlPA#.ra4Kj13ke, 04.01.2017.

wskazują, iż grupa interesowała się bronią, fałszowaniem dokumentów, ładunkami wybuchowymi, inwigilacją oraz metodami jej zapobiegania. Jednakże to, co najbardziej poruszyło śledczych, to metadane uzyskane z trwale usuniętych plików. Plik o nazwie „13Novembre" otwierany był między 7 a 11 listopada 2015 roku i ujawniał, że data ataku została wybrana wcześniej. Następnie okazało się, że plik ten zawierał kilka podtytułów opisujących grupy bojowe.

Śledczym dodatkowo udało się odzyskać siedem plików audio. Zawierały one raporty na temat postępów grupy w przygotowaniu ataków oraz ładunków wybuchowych. W jednym z nagrań zdradzono, że główny cel ataków miała stanowić Francja, a Belgia miała być traktowana jako baza i schronienie. Powyższe odkrycie dowodzi, że dżihadyści są świadomi faktu, iż dane pozostawione na dyskach komputerów mogą stanowić niebezpieczne narzędzie w walce z nimi, jeśli dostaną się w ręce służb bezpieczeństwa. Jednakże mimo stosowania przez nich szczególnych środków ostrożności, śledczym udaje się dojść do niektórych śladów dzięki wykorzystaniu najnowszych technologii i oprogramowania.

Wykorzystanie internetu

Państwo Islamskie doskonale nauczyło się wykorzystywać internet do swoich celów i prowadzi wojnę w sieci, wykorzystując do tego urządzenia mobilne oraz media społecznościowe. Z jednej strony, tweety ze zdjęciami i filmami z egzekucji sieją postrach w internecie, z drugiej – media społecznościowe służą jako idealne narzędzie do prowadzenia rekrutacji online. W obecnych czasach otaczające nas najnowsze technologie umożliwiają publikowanie w czasie rzeczywistym filmów z miejsca wydarzeń (np. egzekucji) bez wykorzystania zaawansowanego sprzętu. Wystarczy posiadać smartfona z dostępem do internetu, konto w mediach społecznościowych i można publikować przeróżne treści i dzielić się nimi z tysiącami dżihadystów na całym świecie. Można spotkać się z opiniami, że sama przeglądarka Google, niecelowo, ale mimo wszystko, wspiera działalność IS. Ostatnio Google poinformowało, że więcej niż 50 tysięcy osób miesięcznie wstukało frazę: „Jak wstąpić do ISIS" (w samej Jordanii średnio 100 osób tygodniowo)[8]. Według jordańskiego wywiadu pierwsze z listy wyniki wyszukiwania po arabsku zawierają szczegółową instrukcję, krok po kroku, co zrobić, kiedy spakować plecak, co powiedzieć rodzicom itd. To, co sprawia, że IS

[8] S. Frenkel, *Everything You Ever…*

jest bardzo niebezpieczne, to fakt, że wyszukiwarka Google „zna" odpowiedź na prawie każde pytanie dotyczące IS.

Aby przybliżyć związany z tym problem, warto zacytować pracownika jordańskich służb bezpieczeństwa: „Nawet jeśli zamknę wszystkie meczety, pozamykam ludzi wspierających IS w Jordanii, nie będę w stanie zrobić tego samego z filmami na YouTube rekrutujących młodych mężczyzn. To samo dotyczy Twittera, gdzie dżihadyści nadal będą publikować informacje o tym, jak dobrze żyje im się w raju z trzema żonami i domem. Również nie zamknę WhatsAppa ani Telegramu, ani żadnego innego medium, za pomocą którego będą komunikować się z kim zechcą"[9].

Dżihadyści doskonale wiedzą, że nie każde medium jest bezpiecznym środkiem komunikacji, dlatego do komunikowania się używają protokołu OTR (Off The Record), zapewniającego pełne szyfrowanie na całej drodze przesyłu informacji (end-to-end encryption). W skrócie ten rodzaj szyfrowania można opisać w następujący sposób: dwie osoby komunikują się ze sobą za pomocą aplikacji, wymieniając się jednocześnie (wykonywane jest to automatycznie, często bez wiedzy użytkowników) długimi i unikatowymi cyfrowymi kluczami. Wiadomość może być odczytana tylko przez urządzenie, z którego pochodzi, oraz urządzenie, które posiada unikatowy klucz dekodujący. Klucz, za pomocą którego dochodzi do zakodowania, nazywa się publicznym (public key), a klucz odszyfrowujący zwany jest kluczem prywatnym (private key). Według prof. Alana Woodwarda[10], konsultanta ds. cyberprzestępczości, nawet jeśli uda się zabronić firmom dostarczania oprogramowania z OTR, to na rynku i tak jest mnóstwo darmowych narzędzi zapewniających pełne szyfrowanie, które można samodzielnie zainstalować.

Terroryści z Państwa Islamskiego są świadomi tego, że amerykańskie agencje rządowe podsłuchują ruch internetowy na amerykańskich komunikatorach (fizycznie używając amerykańskich serwerów), tj. WhatsApp czy iMessage, toteż generalnie ich unikają, koncentrując się na mniej popularnych lub bezpieczniejszych komunikatorach. Aby uniknąć niechcianej inwigilacji, potrzebują medium, które jest – po pierwsze – niezależne od USA, a po drugie – tak zwanym narzędziem open source, czyli z możliwością sprawdzenia kodu źródłowego. Istnieje podejrzenie, że Państwo Islamskie stworzyło własną aplikację do bezpiecznego komunikowania się, jednakże nie znaleziono na to żadnych dowodów.

[9] *Ibidem.*
[10] J. Wakefield, *How does IS communicate securely*, BBC, 17.11.2015, http://www.bbc.com/news/technology-34842854, 05.01.2017.

Agencje wywiadowcze wielu krajów próbują dowiedzieć się, w jaki sposób IS wykorzystuje internet w swojej działalności. Zauważalne jest to, że grupa zwolenników IS na całym świecie rośnie w siłę, stąd też wzrasta potrzeba bezpiecznej komunikacji. Wywiad amerykański[11] uważa, że w szeregach IS znajduje się wysoce wyspecjalizowana grupa ludzi zdolna przeprowadzać ataki hakerskie przeciwko swoim wrogom. Śledząc adresy IP, znaleziono ślady prowadzące nie tylko do Syrii czy Iraku, ale również do Turcji i Kataru. Grupa ta publikuje również w sieci poradniki dotyczące sposobów maskowania się w internecie, by nie zostawiać najmniejszych śladów obecności i tym samym uniemożliwić identyfikację oraz uchronić się przed „namierzeniem" przez służby bezpieczeństwa.

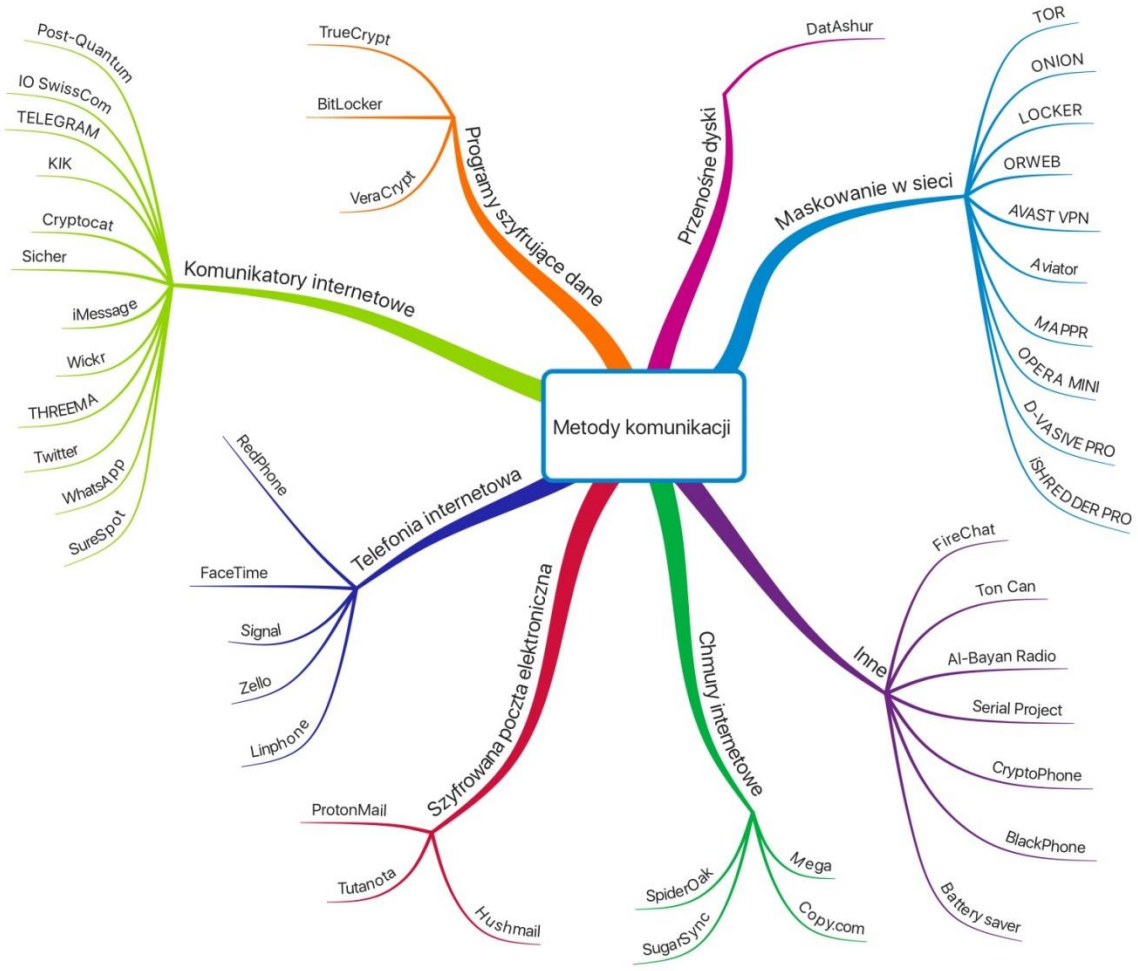
Poradnik bezpieczeństwa dla zwolenników IS

Zespół pod przewodnictwem profesora Aarona Brantly'ego z Combatting Terrorism Center z Akademii Wojskowej West Point w trakcie przeszukiwania forów i mediów społecznościowych odkrył poradnik bezpieczeństwa w sieci dla zwolenników Państwa Islamskiego. Dokument ten został napisany w 2014 roku po arabsku przez zajmującą się bezpieczeństwem kuwejcką firmę Cyberkov. Stworzono go w celu ochrony prywatności i źródeł informacji dziennikarzy oraz działaczy politycznych ze Strefy Gazy, jednakże Państwo Islamskie zaadaptowało poradnik na swój użytek. Dokument zawiera zbiór przydatnych porad dotyczących sposobu ochrony swojej prywatności, danych, kontaktów, miejsca położenia oraz bezpiecznej komunikacji w dobie nowoczesnych technologii. Link do poradnika bezpieczeństwa w sieci dla dżihadystów został opublikowany 19 listopada 2015 roku na stronie Wired w artykule[12] Kima Zettera.

Przykładowo, według autorów poradnika, konta pocztowe Google są bezpieczne pod warunkiem, że zostały utworzone na bazie fałszywych danych użytkownika, a dostęp do nich jest realizowany dzięki sieciom Tor lub VPN, pozwalających na anonimowość w sieci. Mobilne systemy operacyjne mogą być wykorzystywane tylko wówczas, gdy cały ruch internetowy będzie prowadzony przez Tor. Zaleca się wyłączanie automatycznej lokalizacji GPS w smartfonach, gdyż może to przypadkowo zdradzić położenie bojowników. Odradzane jest używanie Instagramu, WhatsAppa oraz Skype'a, ocenianych jako mało bezpieczne. Na czarnej

[11] S. Frenkel, *Everything You Ever…*
[12] K. Zetter, *Security manual reveals the OPSEC advice ISIS gives recruits*, „Wired.com", 19.11.2015, https://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/, 06.01.2017.

liście znalazł się również Dropbox z racji tego, że była sekretarz stanu USA Condoleezza Rice należy do jednego z większych udziałowców tej firmy. Zalecane jest stosowanie mocnych haseł i nieotwieranie podejrzanych linków internetowych. W poradniku znajdziemy również wskazówki do konfiguracji sieci Wi-Fi. Do przesyłania zdjęć i krótkich wiadomości zaleca się używanie takich aplikacji, jak FireChat, działającej bez łączności z internetem. W celu prowadzenia bezpiecznej komunikacji rekomendowane jest stosowanie połączeń VPN (np. fińskiego Freedom), jednakże zdecydowanie odradzani są amerykańscy dostawcy tej usługi – podobnie jak amerykańskie komunikatory, dla których alternatywą miałyby być niemieckie produkty, jak Telegram czy Sicher. Dużym zaskoczeniem dla grupy badaczy z West Point było to, że w poradniku nawet nie wspomniano o możliwości komunikowania się za pomocą Sony PlayStation. Według Brantly'ego nie znaleziono również najmniejszych śladów samodzielnie tworzonych programów do szyfrowania wiadomości – w to miejsce powszechnie stosowany jest Telegram.



Poradnik nie jest jedynym środkiem pomocy, jaki dżihadyści otrzymali od Państwa Islamskiego. Prawdopodobnie istnieje 24-godzinne wsparcie techniczne online, coś w rodzaju całodobowego „helpdesk". Co więcej, Combatting Terrorism Center spostrzegło, że na forach IS użytkownicy bardzo różnią się od siebie umiejętnościami i wiedzą na temat nowoczesnych technologii i coraz bardziej zauważalne jest to, że ciekawi ich nie tylko bezpieczeństwo komunikacji, ale również rośnie zainteresowanie cyberprzestępczością. IS posiada zagorzałą grupę zwolenników zamieszkującą wysoko rozwinięte kraje. Często są to młodzi ludzi, którzy nigdy nie brali udziału w żadnych akcjach zbrojnych, ale przed ekranem komputera podziwiają IS za jego działalność. Jedyną aktywność, jaką prowadzą na rzecz IS, to wspieranie ich w mediach społecznościowych czy udzielanie się w grupach dyskusyjnych.

Poniżej zostały przedstawione najpopularniejsze narzędzia wykorzystywane do ukrywania tożsamości w sieci, komunikacji, przeglądania internetu i szyfrowania danych przez bojowników Państwa Islamskiego, polecane w poradniku bezpieczeństwa i znalezione przez Autora niniejszego rozdziału w internecie.

Maskowanie w sieci i ochrona prywatności

Członkowie IS do ukrywania swojej aktywności w sieci, m.in. historii odwiedzanych stron, wykorzystują tzw. głęboką i mroczną część internetu (deep & dark web), która często używana jest do nielegalnych działań. Aby mieć wgląd do tych zasobów, należy zastosować konkretną przeglądarkę lub aplikację, a czasami również i to nie wystarczy, ponieważ informacje można zdobyć tylko wtedy, jeśli wiadomo, gdzie ich szukać i jak uzyskać do nich dostęp. Jednym z pierwszych elementów szkolenia związanego z bezpiecznym poruszaniem się w sieci jest powszechne kształcenie nowo wcielonych członków w użyciu bezpłatnej sieci Tor, pozwalającej na anonimowe[13] surfowanie, która początkowo była najpowszechniejszym narzędziem używanym do zacierania śladów w internecie. Sama nazwa pochodzi od „The Onion Router" (w wolnym tłumaczeniu: „cebulowy rozgałęźnik"). Aplikacja została wynaleziona na potrzeby wojska przez zespół naukowców, w którego skład wchodził m.in. matematyk Paul Syverson. Aby ukryć prawdziwy adres IP, Tor wykorzystuje kryptografię, wielowarstwowo szyfrując przesyłane komunikaty (stąd nazwa – skojarzenie z warstwami cebuli), zapewniając poufność szyfrowania między routerami. Dżihadyści mieli zapisywać

[13] S. Frenkel, *Everything You Ever…*

sobie przeglądarkę Tor na przenośnym dysku pamięci Flash i używać go w publicznych miejscach, np. w kafejkach internetowych, w celu ukrywania swoich śladów w internecie[14]. Onion jest mobilną wersją Tora na iPhone'y i iPad'y. Jego odpowiednikiem na Androida są aplikacje Orweb oraz Orfox. Innymi polecanymi w poradniku bezpieczeństwa przeglądarkami internetowymi są Aviator oraz Opera Mini.

- **Avast SecureLine VPN** - służy do maskowania obecności w sieci.
- **Mappr – używany** w celu zmiany danych o lokalizacji, aby nie ujawniać miejsca gdzie zostały zrobione zdjęcia.
- **Locker** - automatycznie kasuje pliki i usuwa prywatne dane ze smartfona.
- **D-Vasive Pro** - aplikacja, która dla zmniejszenia ryzyka bycia podsłuchiwanym i śledzonym usuwa uprawnienia niektórych aplikacji do używania GPS, kamery, mikrofonu, BlueTooth i Wi-Fi[15].
- **iShredder Pro** - całkowicie usuwa dane zapisane na urządzeniu mobilnym[16].

Komunikatory internetowe

Ostatnimi czasy na popularności zyskały komunikatory na urządzenia mobilne. Ich przewaga polega na tym, że często są one bezpłatne i wygodniejsze niż np. SMS. Poza zwykłym tekstem, który w SMS-ach ma ograniczenie liczby znaków, można wysyłać zdjęcia, gify, a nawet wideo. Wiadomości przesyłane za pomocą niektórych komunikatorów są szyfrowane, co oznacza, że poza odbiorcą i nadawcą nie sposób jest odczytać ich treści.

Wymiana informacji za pomocą komunikatorów internetowych narażona jest na ataki cyberprzestępców i hakerów oraz podsłuchiwanie ze strony władz i agencji państwowych. Terroryści Państwa Islamskiego, wiedząc o powyższym ryzyku, znaleźli wyjście z sytuacji i używają do tego celu komunikatorów zapewniających pełne szyfrowanie.

Po atakach w Paryżu mówiło się, że terroryści korzystają z internetu i szyfrowanej łączności, ale nie podawano żadnych szczegółów. Pierwsze podejrzenia padły na Telegram po tym, jak IS za pośrednictwem tej aplikacji poinformowało swoich bojowników i zwolenników, w jaki sposób chronić się przed cyberatakami zapowiadanymi przez grupę hakerów zrzeszonych w organizacji Anonymous.

[14] J. Goldsmith, *The Jihadists' Digital Toolbox*…
[15] *Ibidem.*
[16] *Ibidem.*

- Telegram służy do publikowania i udostępniania postów, wysyłania wiadomości, zdjęć, filmów i plików w różnym formacie do nawet 200 użytkowników w tak zwanych kanałach.
- **Threema** - komunikator szyfrujący, stosujący pełne szyfrowanie (end-to-end, czyli przechowywane na urządzeniach użytkowników klucze szyfrujące).
- **SureSpot** - nie jest powiązany ani z numerem telefonu, ani adresem e-mail. Pozwala stworzyć wiele profili na jednym urządzeniu, np. do prowadzenia kilku konwersacji jednocześnie, z wykorzystaniem różnych tożsamości (kont).
- **Wickr** - pozwala użytkownikom wymieniać się samoniszczącymi się wiadomościami, włączając w to zdjęcia i załączniki, jeśli nadawca wysłanej wiadomości (pliku) usunie ją na swoim urządzeniu, wówczas zostanie ona bezpowrotnie usunięta ze wszystkich innych urządzeń, na których się znajdowała. Stosuje pełne szyfrowanie.
- **Cryptocat** posiada mechanizm przeciwdziałania atakom hakerskim „man-in-the-middle", polegającym na podsłuchiwaniu i modyfikacji wiadomości przesyłanych pomiędzy dwiema komunikującymi się stronami bez ich wiedzy.
- **IO SwissCom** posiada funkcję komunikatora internetowego, z którego można prowadzić czat (live chat oraz wideoczat) z innymi rozmówcami.
- **Post-Quantum** specjalizuje się w zapewnianiu bezpiecznej komunikacji i zabezpieczaniu transakcji finansowych.
- **Sicher** jest komunikatorem internetowym z funkcją samoniszczenia wiadomości.
- **KIK** to komunikator, którego wyróżnia brak obowiązku podawania numeru telefonu – do rejestracji wystarczą tylko imię, nazwisko, adres e-mail i rok urodzenia.
- **iMessage** - pomimo tendencji do odchodzenia od amerykańskiego oprogramowania iMessage jako jeden z nielicznych widnieje na liście programów polecanych do użycia przez bojowników Państwa Islamskiego.
- **Twitter** jest wykorzystywany przez Państwo Islamskie jako główne narzędzie do szerzenia propagandy, rekrutacji nowych zwolenników/bojowników oraz zbierania informacji.
- **WhatsApp** - jeden z najpopularniejszych komunikatorów internetowych. Aktualnie nie jest polecany przez dżihadystów, ale początkowo był przez nich używany.

Programy szyfrujące dane zapisane na nośnikach

- **TrueCrypt** jest popularnym i darmowym programem do szyfrowania danych. Za jego pomocą można szyfrować zarówno całe dyski, ich partycje i przenośne dyski USB (pendrive'y),

jak i tworzyć wirtualne szyfrowane dyski (dyski te mogą być ukryte oraz mieć zdefiniowany maksymalny rozmiar). Dane chronione hasłem są zaszyfrowane za pomocą bardzo silnych algorytmów szyfrujących.

- **Windows BitLocker** jest programem szyfrującym, wbudowany w wyższe wersje systemu operacyjnego Microsofta.
- **VeraCrypt**, zapewnia szyfrowanie zarówno całego dysku, pojedynczych partycji, jak i przenośnych dysków USB (pendrive'ów).

Przenośne dyski

Dość zaskakującym rozwiązaniem jest stosowanie przez dżihadystów przenośnych dysków USB (pendrive'ów), do zawartości których dostęp możliwy jest po wprowadzeniu poprawnego kodu PIN.

- **DatAshur** to nośnik brytyjskiej firmy iStorage. Przechowywane na nim dane zabezpieczone są nie tylko za pomocą kodu PIN, ale również bardzo mocnego szyfrowania (AES 256-bit na poziomie sprzętu, a nie oprogramowania). Nośnik datAshur jest wyposażony w akumulatorek umożliwiający użytkownikowi wprowadzenie kodu PIN (od 7 do 15 znaków) za pomocą klawiatury znajdującej się na obudowie. Użytkownik przed użyciem musi wprowadzić kod PIN, a dopiero później podłączyć nośnik do komputera przez port USB. W przypadku zagubienia lub kradzieży dziesięciokrotne wprowadzenie złego PIN-u aktywuje mechanizm samodestrukcji. DatAshur blokuje się automatycznie, gdy nagle zostanie odłączony od komputera lub w przypadku odcięcia zasilania[17].

Telefonia internetowa

Skype jest jedną z najpopularniejszych aplikacji używanych do prowadzenia rozmów i wideorozmów przez internet. Jednakże mimo swej wysokiej popularności nie cieszy się zaufaniem wśród dżihadystów. Do rozmów (wideo)telefonicznych wykorzystywane są bezpieczniejsze aplikacje, takie jak **Linphone**, **Redphone**, **Signal** czy **Facetime**.

- **Signal** powstał z połączenia RedPhone oraz TextSecure i jest jedną z najbezpieczniejszych aplikacji używanych do bezpiecznej (szyfrowanej) komunikacji przez

[17] https://istorage-uk.com/product/datashur/, 12.04.2017.

telefon przy wykorzystaniu internetu (VoIP). Dla zwiększenia bezpieczeństwa wiadomości tekstowych sugeruje się zabezpieczenia aplikacji hasłem oraz ustawienie jak najmniejszej liczby SMS-ów przechowywanych w pamięci urządzenia. W praktyce oznacza to, że rządy, służby bezpieczeństwa lub sądy nie mogą otrzymać dostępu do wiadomości konkretnych użytkowników, gdyż firma nie posiada kluczy do odszyfrowania tych wiadomości.

- **FaceTime** to produkt firmy spod znaku nadgryzionego jabłka, połączenia wideo są szyfrowane i niedostępne dla nikogo poza interlokutorami.
- **Zello** - tworzenie kanałów (chronionych hasłem), za pomocą których mogą przesyłać do siebie zaszyfrowane komunikaty głosowe, zamienia smartfona w walkie-talkie, a do jego użycia wystarczy dostęp do internetu[18].

Chmury internetowe

Chmury internetowe to serwisy internetowe wykorzystywane do zdalnego ładowania, przechowywania, synchronizacji i dzielenia się informacjami w postaci dokumentów, zdjęć, filmów wideo czy lokalizacji. Ponieważ zalecane są we wspomnianym wcześniej poradniku, można przypuszczać, że używane są właśnie do takich celów, jak przekazywanie sobie informacji odwołujących się do innych odnośników. Dzielenie się dostępem/zarządzanie uprawnieniami polega na wysłaniu linku do dokumentu zapisanego w chmurze lub w bardziej skomplikowanym przypadku – przesłanie linku z hasłem.

- **Mega** to serwis, który wręcz nokautuje konkurencję, tj. Google Drive, Dropbox, Microsoft OneDrive czy iCloud. Przechowywane dane są zaszyfrowane po stronie klienta i pozostają w pełni bezpieczne, niedostępne nawet dla administratorów.
- **SpiderOAK** - ciągła i automatyczna synchronizacja danych online na nieograniczonej liczbie komputerów, oferuje wysoki poziom prywatności.
- **SugarSync** - synchronizacja plików i folderów między urządzeniami/komputerami, jak również do tworzenie kopii zapasowych, wygodne zarządzanie dostępem i uprawnieniami.
- **Copy.com** - synchronizacja danych na wielu urządzeniach użytkownika (podobnie jak w SugarSync) oraz duża prostota obsługi na komputerach i smartfonach.

Szyfrowana poczta elektroniczna

[18] https://zello.com, 12.04.2017.

Szyfrowana poczta elektroniczna zyskuje coraz więcej zwolenników, gdyż zapewnia bezpieczeństwo i prywatność w komunikacji. Zalecanymi dostawcami usług poczty elektronicznej dla dżihadystów są firmy nieamerykańskie. Największą popularnością cieszą się Hushmail i ProtonMail.

- **Hushmail** (firma kanadyjska), nawet jej pracownicy mający fizyczny dostęp do serwerów nie są w stanie odczytać szyfrowanych maili klientów.
- **ProtonMail** (Szwajcaria) - treść wiadomości jest w pełni bezpieczna i nie może być odczytana przez nikogo innego niż odbiorca wiadomości. Wszystkie dane są zaszyfrowane, dostęp do nich można uzyskać, gdy posiada się drugie hasło, wysyłanie maili z określonym terminem ważności, z opcją samodestrukcji.
- **Tutanota (**Niemcy) – oferuje szyfrowanie maili, w których poza treścią szyfrowane są również załączniki i temat wiadomości.

Inne komunikatory

Na rynku aplikacji dostępne są również darmowe komunikatory, których można używać na urządzeniach mobilnych nawet bez dostępu do sieci telefonii komórkowej czy internetu, tj. FireChat, Tin Can czy Serval Project.

- **FireChat** zamiast łączyć się ze stacją bazową/przekaźnikową telefonii komórkowej, szuka innych urządzeń będących w pobliżu w zasięgu anteny Wi-Fi i bluetooth smartfona z zainstalowanym FireChatem. Po znalezieniu pobliskich urządzeń powstaje rodzaj połączenia sieciowego (mesh network), za pomocą którego można przesyłać sobie wiadomości tekstowe (nieszyfrowane) nawet na odległość do 200 m[19]. Mamy tu do czynienia z funkcją retranslacji, czyli przekazywania sygnału/komunikatu przez urządzenie pośrednie.
- **Tin Can** działa podobnie jak FireChat i również jest komunikatorem tekstowym. Różnicą jest to, że działa tylko na Androidzie. Rozsyłane w ten sposób wiadomości nie niosą ze sobą żadnych informacji o nadawcy i nie są szyfrowane.
- **Serval Project**[20] od swoich poprzedników wyróżnia się tym, że jest komunikatorem głosowym i tekstowym (dostępny tylko na Androida). Na stronie internetowej Serval reklamuje się jako alternatywa dla telefonii komórkowej w sytuacji, gdy ta przestanie działać. Poza tym

[19] P. Szoldra, *15 secure apps ISIS…*.
[20] http://www.servalproject.org, 15.04.2017.

jest odpowiedzią na czarne dziury zasięgu telefonii (w Australii aż 75% powierzchni nie ma pokrycia sygnałem telefonii komórkowej).

- **CryptoPhone** to odpowiedź niemieckiej firmy GSMK[21] na rosnący rynek urządzeń podsłuchowych. GSMK produkuje telefony (komórkowe, biurowe, satelitarne i internetowe) zapewniające łączność szyfrowaną dla osób prywatnych, firm, organizacji i rządów.
- **BlackPhone** to odporny na szpiegowanie smartfon szwajcarskiej firmy Silent Circle[22]. Pracuje na zmodyfikowanym systemie Android, zwanym SilentOS.
- **Al-Bayan Radio** jest aplikacją mobilną stworzoną przez IS dla IS. Dzięki niej można odbierać i słuchać radia internetowego, za którego pośrednictwem jest szerzona propaganda dżihadystów.

Battery Saver to aplikacja wykorzystywana do wydłużania życia akumulatora w smartfonach.

Wnioski

Analizując sposób, w jaki Państwo Islamskie wykorzystuje różnego rodzaju narzędzia do komunikacji, można stwierdzić, że mamy do czynienia z technologicznie rozwiniętą organizacją, umiejącą wykorzystać najnowsze zdobycze techniki do własnych celów. Najprawdopodobniej również dzięki tej wiedzy członkom IS udaje się uchronić przed inwigilacją przez służby bezpieczeństwa. Ta cecha właśnie – zaawansowanie technologiczne i używanie bezpiecznych środków komunikacji – odróżnia IS od podobnych organizacji, takich jak np. Al-Kaida.

Eksperci od cyberprzestępczości uważają, że członkowie IS stosują szczególne środki bezpieczeństwa wychodzące poza zwykłe szyfrowanie. Na przykład unikają aplikacji, których serwery mieszczą się w USA, aby zmniejszyć do zera ryzyko związane z kontrolowanym wyciekiem informacji i potencjalną współpracą firm świadczących usługi komunikacyjne z amerykańskimi służbami. Członkowie IS wiedzą, że z natury wszystkie aplikacje zainstalowane na serwerach amerykańskich są mniej bezpieczne. Kolejnym czynnikiem determinującym wybór aplikacji używanej do komunikacji jest jej popularność – im mniej popularna i mało znana, tym lepiej dla bojowników IS. Oczywiste jest bowiem, że

[21] http://www.cryptophone.de, 15.04.2017.
[22] https://www.silentcircle.com, 15.04.2017.

porozumiewanie się za pomocą popularnych komunikatorów zwiększa prawdopodobieństwo bycia „podsłuchiwanym w sieci", gdyż organizacje, chcące podsłuchać czaty terrorystów, najpierw obierają za cel te najpopularniejsze komunikatory. Powszechnie nieznane aplikacje mają tę przewagę, że wiele osób nawet nie wie o ich istnieniu.

Dostępność różnorodnych systemów, programów czy aplikacji używanych do szyfrowanej komunikacji powoduje ogromną trudność dla władz i agencji rządowych. Nasłuchiwanie znanych władzom mediów często może być bezsensowne, bo w tym czasie IS może używać całkiem nowego, nieznanego medium.

Musimy pamiętać o tym, że chociaż Państwo Islamskie nie posiada najnowszego uzbrojenia, to dysponuje środkami komunikacji, które stały się groźną bronią w rękach dżihadystów. Mając powyższe na uwadze, bądźmy świadomi tego, że mamy do czynienia z „grupą zbrojną ery internetu, Facebooka, smartfonów i wiadomości tekstowych". Aby wygrać walkę z Państwem Islamskim w internecie, muszą być spełnione dwa kluczowe warunki. Pierwszym z nich jest międzynarodowa współpraca rządów i agencji bezpieczeństwa na wszystkich możliwych szczeblach, ponieważ tej wojny nie można wygrać w pojedynkę. Drugi – to zaangażowanie się firm komercyjnych przez udzielanie pomocy służbom bezpieczeństwa. Niedopuszczalne jest to, aby ścigani przez agencje rządowe różnych krajów bojownicy znajdowali bezpieczne schronienie w niedostępnych zakamarkach internetu, tworzonych i utrzymywanych przez firmy komercyjne.

Rządy i firmy komercyjne muszą zdecydować, czy stawiają na bezpieczeństwo, czy na wolność i swobodę w komunikowaniu się. W sumie dotyczy to każdego z nas i chyba nadszedł czas, aby zadać sobie to zasadnicze pytanie: co jest dla nas cenniejsze – wolność i swoboda czy bezpieczeństwo?