Zeszyty Naukowe SGSP 2019, Nr 69/1/2019

mgr inż. Jacek Rychlica
PIT-RADWAR S.A.

Cyberterroryzm – ewolucja czy rewolucja w sposobie działania współczesnych organizacji terrorystycznych

Abstrakt

Ostatnie trzy dekady zostały bez wątpienia zdominowane przez niezwykle szybki rozwój technik informacyjnych, które są obecne praktycznie wszędzie i wykorzystuje się je w niemal każdej sferze aktywności człowieka. Co więcej, przetwarzanie olbrzymich ilości informacji (ang. *Big Data*) jest obecnie niezbędne zarówno w polityce, jak i w szeroko rozumianym biznesie. Bez właściwego przetwarzania i przepływu tych informacji nie mogą poprawnie funkcjonować ani różnego rodzaju media, ani wszelkiego typu instytucje, ani też inne – często krytyczne z punktu widzenia życia i zdrowia ludzi – systemy. Niestety, szybki postęp technologiczny wprowadza również wiele nowych zagrożeń, gdyż nowoczesne systemy mogą zostać wykorzystane zarówno do poprawy jakości życia obywateli, jak i przez różnego rodzaju grupy przestępcze, organizacje terrorystyczne, a nawet nieformalne i/lub jawnie działające struktury o charakterze militarnym.

W artykule dokonano próby oceny wpływu opisanych zmian na sposób i zakres działania współczesnych organizacji terrorystycznych.

Słowa kluczowe: cyberperzestrzeń, cyberterroryzm, terroryzm

Cyberterrorism – the Evolution or the Revolution in Modus Operandi of the Contemporary Terrorist Organizations

Abstract

The last three decades have undoubtedly been dominated by the unusually rapid development of information technologies, which today are present practically everywhere and are used in almost every sphere of human activity. What's more, the processing of huge amounts of information (so-called Big Data) is now indispensable both in politics and in broadly understood business activities. It is not an exceptional knowledge that without the proper processing

and the flow of such information, today there can not properly function both different types of media or all types of institutions, and no other systems, often critical from the point of view of human life and health. The rapid technological progress also introduces a number of new threats, as modern systems can be used to improve the quality of the human life as well as by the various types of criminal groups, terrorist organizations and even informal and/or legally operating military structures. This article attempts to assess the impact of the described changes on the manner and the scope of operation of the contemporary terrorist organizations.

Keywords: cyberspace, cybersecurity, cyberterrorism, terrorism

Wprowadzenie

Żyjemy w dynamicznie zmieniającym się świecie, coraz bardziej zależnym od technologii informatycznych. Przez ostatnie 30 lat w tej dziedzinie dokonała się rewolucja. Nowoczesne urządzenia teleinformatyczne są obecne praktycznie wszędzie i wykorzystywane w niemal każdej sferze aktywności człowieka. Co więcej, przetwarzanie olbrzymich ilości informacji niezbędne jest dziś zarówno w polityce, jak i w szeroko rozumianym biznesie. Bez właściwego przetwarzania i przepływu tych informacji nie mogą bowiem funkcjonować ani media, ani wszelkiego typu instytucje. Bez nowoczesnego sprzętu komputerowego nie będą funkcjonowały niektóre placówki i instytucje badawcze i oświatowe (w szczególności uniwersytety, politechniki i inne uczelnie wyższe), placówki handlowe oraz biura czy urzędy. Nawet w sferze mediów i rozrywki praktycznie całkowicie uzależniliśmy się już od techniki cyfrowej.

Dokonując analizy wpływu wymienionych zmian na funkcjonowanie kluczowych dla każdego państwa służb i instytucji, trudno wyobrazić sobie brak opisanych wcześniej zdolności w służbach mundurowych czy podczas prowadzenia działań militarnych, i to zarówno w kraju, jak i za granicą.

Mimo takiego stanu rzeczy, w wielu analizach wpływu rozwoju systemów teleinformatycznych na poziom życia i bezpieczeństwa obywateli często pomija się fakt, że już dzisiaj komputery i technologia informatyczna są wykorzystywane w znacznym stopniu do sterowania różnego rodzaju urządzeniami (nie tylko w przemyśle, ale także w gospodarstwach domowych) oraz bardziej złożonymi systemami w praktycznie każdej dziedzinie naszego życia, w tym w tak wrażliwych obszarach, jak:

- systemach sterowania ruchem drogowym, kolejowym, morskim czy lotniczym,
- coraz bardziej rozbudowanych systemach monitoringu,

- telekomunikacji (zarówno tradycyjnej – przewodowej, jak i w łączności bezprzewodowej czy satelitarnej),
- sferze bankowości (korporacyjnej i osobistej) oraz sektorze finansowym,
- przemyśle wydobywczym i energetycznym (w tym w złożonych instalacjach elektrowni jądrowych, wielkich zakładach petrochemicznych na platformach wiertniczych itd.),

a także w innych, często krytycznych z punktu widzenia życia i zdrowia obywateli, systemach. Taki stan rzeczy powoduje przy tym powstawanie nowych, nieuwzględnianych wcześniej zagrożeń, których pominięcie lub uwzględnienie fragmentaryczne ogranicza przydatność wyników przedmiotowych analiz do zapewnienia poprawy szeroko rozumianego bezpieczeństwa na szczeblu lokalnym, narodowym, a nawet w skali globalnej.

Jeszcze w niedalekiej przeszłości największe obawy budziły zagrożenia dotyczące naruszenia prywatności użytkowników Internetu bądź możliwości zakłócania działania systemów teleinformatycznych przez pojedynczych hakerów. Obecnie dużo większym problemem wydają się być ataki prowadzone przez zorganizowane grupy hakerów (przestępcze lub terrorystyczne), a także – zgodnie z doniesieniami medialnymi oraz wynikami analiz instytucji rządowych i organizacji pozarządowych – ataki realizowane przez grupy hakerów funkcjonujących pod egidą służb specjalnych innych państw lub nawet wewnątrz grup terrorystycznych. Celem takich ataków jest destabilizacja atakowanych systemów lub przejmowanie nad nimi kontroli, kradzież danych, własności intelektualnej, informacji niejawnych itp. W opisywanym obszarze można zatem dostrzec bardzo dużą dynamikę zmian w zakresie występujących zagrożeń, co z kolei wymusza wprowadzanie modyfikacji metod ochrony współczesnych systemów teleinformatycznych i ich zasobów.

Wydaje się to tym bardziej istotne, gdyż obecnie odnotowywany jest znaczny wzrost liczby ataków ukierunkowanych, definiowanych jako działania skierowane na konkretny cel, prowadzone z wykorzystaniem wszelkich dostępnych metod i technik (w tym informatycznych). Ataki tego typu wymierzone są w ściśle określoną, starannie wybraną ofiarę, przy czym ich celem może być zarówno uzyskanie w sposób skryty dostępu do konkretnych informacji przetwarzanych w systemie teleinformatycznym (najczęściej w celu przejęcia lub ingerencji w treść tych informacji lub inwigilowania ofiary), jak też uzyskanie możliwości zdalnego kontrolowania atakowanego systemu, (np. w celu przeprowadzenia sabotażu, zakłócenia pracy systemu, wykorzystania jego zasobów do realizacji innych zadań niż to wynika z jego przeznaczenia) lub konta (pocztowego czy bankowego) należącego do ofiary.

Tego typu ataki charakteryzują się zazwyczaj wysokim poziomem zaawansowania, przy czym do ich przeprowadzenia wykorzystywane są techniki:

- psychologiczne, oparte na tzw. inżynierii społecznej, czyli na metodach socjotechnicznych,
- analityczno-wywiadowcze – atak tego typu poprzedzony jest zwykle rekonesansem obejmującym zebranie i analizę wszelkich informacji dotyczących ofiary znajdujących się w: Internecie, ogólnodostępnych repozytoriach i bazach danych, sieciach społecznościowych – na podstawie tych informacji tworzony jest następnie profil ofiary lub w przypadku firmy/instytucji – jej personelu, określane są sieci zależności, definiowane słabe punkty itp.,

i/lub środki techniczne (np. nieujawnione wcześniej podatności, metody podszywania się czy ukrywania złośliwiej zawartości).

Zaawansowane ataki ukierunkowane są również znacznie trudniejsze do wykrycia, gdyż z reguły są przeprowadzane fachowo, ostrożnie i dyskretnie, a użyte w nich metody i/lub narzędzia zazwyczaj wykorzystują skomplikowane techniki ukrywania nielegalnej aktywności w atakowanym systemie. W wielu przypadkach udany atak ukierunkowany może nigdy nie zostać wykryty, gdyż najczęściej, po osiągnięciu założonego celu, atakujący wycofują się, zacierając za sobą ślady, kasując lub modyfikując logi itp.

Skutkiem tego może być przejęcie kontroli nad atakowanym systemem i/lub podszycie się pod tożsamość ofiary przez przejęcie jej kont (pocztowych, systemowych, bankowych itp.), co z kolei może umożliwić realizację z wykorzystaniem przejętych w ten sposób zasobów, podobnego ataku na inne systemy teleinformatyczne. W wyniku zaawansowanych ataków ukierunkowanych dojść może także do ujawnienia lub utraty integralności przetwarzanych w danym systemie teleinformatycznym informacji wrażliwych, a nawet do dezaktywacji lub uszkodzenia elementów infrastruktury teleinformatycznej lub sterowanych przez nią systemów i/lub urządzeń. W tym przypadku głównym atakującym są zwykle grupy hakerów pracujące pod egidą lub dla służb specjalnych innych państw, organizacji przestępczych czy terrorystycznych, zaś ich celem – kluczowe elementy infrastruktury, zasobów (np. w wojskowych systemach teleinformatycznych, dynamiczny rozwój, integracja i stosowanie komercyjnych komponentów, w tym w urządzeniach radiolokacyjnych czy w systemach rozpoznania oraz wsparcia dowodzenia, prowadzi do sytuacji, w której ich sparaliżowanie spowoduje znaczne obniżenie zdolności bojowych wykorzystujących je jednostek), informacji i/lub personelu strony atakowanej. Do przeprowadzenia udanego ataku mogą one wykorzystać wszelkie:

- informacje i dane przydatne do precyzyjnego wytypowania celu, rozpoznania jego zachowań, przyzwyczajeń, kontaktów, zadań i/lub zakresu obowiązków, czemu sprzyja powszechne wykorzystywanie poczty elektronicznej oraz sieci społecznościowych,
- podatności atakowanego systemu teleinformatycznego, którym sprzyja w szeroko rozumianym biznesie m.in. postępująca globalizacja oraz szybki rozwój technologii przetwarzania danych w chmurach, natomiast w systemach rządowych i wojskowych rosnąca liczba przedsięwzięć międzynarodowych (tj. programy, misje, ćwiczenia), w ramach których tworzone są połączenia różnych systemów teleinformatycznych, a także coraz powszechniejsze stosowanie urządzeń mobilnych i informatycznych nośników danych,
- błędy i zaniedbania strony atakowanej, czemu może sprzyjać zarówno brak wiedzy czy świadomości realności takiego zagrożenia, jak i częste popełnianie przez użytkowników systemów a nawet przez personel bezpieczeństwa teleinformatycznego błędów, np. w wyniku pośpiechu lub nadmiernego obciążenia zadaniami.

1. Cyberprzestrzeń jako potencjalna domena działań grup terrorystycznych – studia przypadków

Dokonując oceny, czy współczesne systemy oraz zawarte w nich dane i oferowane przez nie usługi mogą stać się potencjalną domeną działań o charakterze przestępczym, terrorystycznym czy militarnym, należy w pierwszej kolejności zdefiniować cyberprzestrzeń. Jest to o tyle istotne, że bez właściwego określenia czym jest i w jakim zakresie ww. domena jest lub może być przydatna do prowadzenia tego typu działań, nie wydaje się możliwym jednoznaczne określenie prawdopodobieństwa i wynikającej zeń skali przedmiotowego zjawiska.

Zgodnie z definicją, zawartą w obowiązującej *Polityce Ochrony Cyberprzestrzeni RP* [9] uznaje się, że cyberprzestrzeń to „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (…) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Nie jest to z pewnością jedyna definicja cyberprzestrzeni – próby zdefiniowania tego pojęcia można znaleźć w pracach, zarówno ekspertów instytucji rządowych czy służb specjalnych [6], jak i przedstawicieli wielu różnych uczelni cywilnych [7] i wojskowych [8]. Ze względu na fakt, iż zapisano ją również w wielu aktach normatywnych (np. w ustawie z 29 sierpnia 2002 r. *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości*

konstytucyjnym organom Rzeczypospolitej Polskiej, Dz.U. z 2017 r. poz. 1932; ustawie z 21 czerwca 2002 r. *o stanie wyjątkowym*, Dz.U. z 2017 r. poz. 1928; czy ustawie z 18 kwietnia 2002 r. *o stanie klęski* żywiołowej, Dz.U. z 2017 r. poz. 1897), winno się ją traktować jako obowiązującą. Należy przy tym zauważyć, że zgodnie z przytoczoną definicją, ową cyberprzestrzeń tworzą właśnie systemy i urządzenia teleinformatyczne niezbędne do prawidłowego funkcjonowania współczesnych społeczności oraz całych państw i przez to w wielu publikacjach i dokumentach doktrynalnych definiuje się ją jako dodatkowy (poza lądem, morzem, powietrzem i kosmosem), piąty wymiar, w którym mogą być i często już są prowadzone działania zarówno z zakresu szeroko rozumianej polityki [7], jak i działania *stricte* militarne [8].

Problemem w tym przypadku jest to, że takie sektorowe podejście do cyberprzestrzeni częściowo utrudnia zrozumienie występujących w niej zależności i zagrożeń. Co więcej, błędny obraz cyberprzestrzeni wynikający z przyjętej definicji stał się też przyczyną przyjęcia w polskim systemie prawnym nie do końca właściwych uregulowań. I tak, zamieszczona w cytowanej *Polityce*… definicja cyberprzestrzeni RP, wskazująca, iż jest to „cyberprzestrzeń (a więc przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami – przyp. aut.) w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)" jest z gruntu niewłaściwa, gdyż sugeruje istnienie możliwości określenia konkretnych granic w cyberprzestrzeni, co w żadnej mierze nie przystaje do wykorzystywanych obecnie technologii ani nawet rzeczywistej architektury i budowy systemów przetwarzania danych. W jaki sposób można bowiem zastosować tego typu uregulowania do wykorzystywanej na coraz większą skalę technologii chmurowej lub w jaki sposób jednoznacznie wskazać, które elementy zlokalizowane są w obrębie cyberprzestrzeni RP, jeśli niejednokrotnie, np. serwery, zlokalizowane na terytorium naszego kraju łączone są za pośrednictwem elementów sieciowych zlokalizowanych poza jej granicami?

Dlatego znacznie lepszym rozwiązaniem wydaje się być uwzględnienie w definicji cyberprzestrzeni faktu, że jednym z jej podstawowych elementów są ww. informacje i usługi, gdyż to one są tym najistotniejszym zasobem, który winien podlegać ochronie. Systemy teleinformatyczne, wraz z występującymi między nimi powiązaniami, są bowiem wyłącznie narzędziem zapewniającym właściwe przetwarzanie informacji oraz dostępność niezbędnych usług. Co więcej, elementy te z reguły charakteryzują się też mniejszą wartością i są łatwiejsze do naprawy lub wymiany niż same informacje. Z tego

też powodu dużo lepiej odzwierciedlającą charakter cyberprzestrzeni wydaje się być definicja opracowana przez Departament Obrony USA stanowiąca, że cyberprzestrzeń to „globalna domena środowiska informacyjnego, składająca się ze współzależnej infrastruktury informatycznej wraz z zawartymi w niej danymi, z uwzględnieniem Internetu, sieci telekomunikacyjnych, systemów komputerowych oraz zawartych w nich procesorów i sterowników" [10].

Nie jest to oczywiście definicja idealna, nie uwzględnia bowiem sfery usług oferowanych lub udostępnianych w cyberprzestrzeni, ale z pewnością w znacznie pełniejszy sposób oddaje istotę tej domeny. Co więcej, definicja ta wskazuje (choć może niezbyt dobitnie), że Internet jest tylko częścią składową cyberprzestrzeni. Jest to o tyle istotne, że często cyberprzestrzeń utożsamiana jest wyłącznie z Internetem, choć jest to podejście błędne, gdyż w dostępnej nam sieci pracuje jedynie niewielki odsetek wszystkich urządzeń teleinformatycznych oraz przetwarzana jest wyłącznie mała ilość wszystkich analizowanych w sposób cyfrowy danych. Znacznie więcej z nich występuje za to pod postacią Internetu Rzeczy (ang. *IoT – Internet of Things*) lub systemów M2M (ang. *Machine to Machine*). Dopiero wszystkie te urządzenia, dane i usługi razem wzięte tworzą cyberprzestrzeń, czyli przestrzeń obejmującą cały otaczający nas świat, bez żadnych fizycznych granic.

To właśnie te cechy przedmiotowej domeny, w połączeniu z pełną dostępnością cyberprzestrzeni, powodują, że jest ona coraz częściej postrzegana jako potencjalna strefa działalności przestępczej, działań militarnych czy też działań o charakterze terrorystycznym i to – w wielu przypadkach – działań o potencjalnych skutkach ekonomicznych i psychologicznych porównywalnych ze skutkami użycia broni masowego rażenia. Wynika to przede wszystkim z faktu, że kompetentna osoba lub grupa osób, przy użyciu stosunkowo prostych narzędzi, często nawet pojedynczego komputera, może wyrządzić szkody porównywalne ze szkodami będącymi następstwem działań wojskowych prowadzonych z wykorzystaniem wyspecjalizowanych formacji militarnych.

Co lub kto może więc stanowić zagrożenie w cyberprzestrzeni? Odpowiedź na to pytanie jest niezwykle trudna, gdyż funkcjonują w tej sferze pewne stereotypy. Wyniki prowadzonych przez wiele firm analiz wskazują jednak, że wciąż za największą liczbę incydentów odpowiadają legalni użytkownicy systemów. To oni, często z niewiedzy lub po prostu z lenistwa, umożliwiają infekowanie urządzeń teleinformatycznych oprogramowaniem złośliwym. Są też podatni na manipulację i stosowanie mniej lub bardziej wyrafinowanych technik socjotechnicznych. Coraz częściej możemy jednak

zauważyć, że w cyberprzestrzeni działają wyspecjalizowane grupy hakerów, a czasem nawet zorganizowane oddziały wojskowe i grupy terrorystyczne. To właśnie te grupy są uważane obecnie za największe zagrożenie, gdyż często jako nieliczne dysponują zarówno wiedzą, motywacją, jak i środkami niezbędnymi do prowadzenia skutecznych operacji w tej domenie. Szczególnie często ostatnio mówi się np. o cyberterroryzmie, czyli o działaniach grup terrorystycznych realizowanych z wykorzystaniem lub wobec elementów cyberprzestrzeni. Jednak w tym przypadku, bez właściwego zdefiniowania źródła zagrożenia, niezwykle trudnym okazuje się określenie lub choćby oszacowanie skali i zakresu tego zjawiska.

W literaturze można znaleźć wiele, czasem sprzecznych ze sobą, definicji, stąd tak istotnym jest prawidłowe zdefiniowanie cyberterroryzmu i działań cyberterrorystycznych. Bardzo wnikliwą analizę tego zagadnienia znaleźć można np. w opracowaniu T. Szubrychta [2], przy czym, pomimo iż jest to pozycja sprzed prawie 20 lat, większość z przedstawionych w niej wyników analiz do dziś pozostaje aktualnych. W szczególności omówienia wielu definicji i cech charakterystycznych, dotyczących zjawiska cyberterroryzmu, w znacznym stopniu ułatwiają identyfikację ww. zagrożenia, a także okazują się bardzo przydatne do jednoznacznego określenia, które działania w cyberprzestrzeni, lub wobec elementów cyberprzestrzeni, można uznać za działania o charakterze *stricte* terrorystycznym, a które mają zgoła inne podłoże.

T. Szubrycht w swoim opracowaniu wskazuje np., iż jednym z podstawowych wyróżników pozwalających odróżniać od siebie źródła zagrożeń oraz klasyfikować rodzaje działań niepożądanych są motywacja sprawców oraz przyświecające im cele. Według tego autora, w przypadku cyberterroryzmu najczęstszymi powodami kierującymi sprawcami są motywy o charakterze politycznym, zaś ich głównym celem jest wyrządzenie dużych strat i wywołanie powszechnego poczucia strachu. Takie podejście ma jednak pewne mankamenty, gdyż w wielu przypadkach sama motywacja i cele przyświecające sprawcom nie zawsze wystarczą, by prawidłowo rozróżnić, czy dany czyn zabroniony w rzeczywistości został popełniony przez kogoś, kogo można zakwalifikować jako terrorystę lub przez grupę terrorystyczną, czy być może za jego realizację odpowiadają inne osoby lub grupy osób.

Aby wykazać zasadność wskazanych wyżej wątpliwości, można posłużyć się przykładami dotychczas wykrytych i przeanalizowanych incydentów, w tym na przykład zakłóceniami w funkcjonowaniu sieci teleinformatycznych w Estonii, atakiem na systemy teleinformatyczne firmy Sony czy choćby uniemożliwieniem normalnej pracy kanałów francuskiej stacji TV5 Monde.

Na szczególne omówienie zasługuje przy tym przypadek ataku na estońską infrastrukturę teleinformatyczną, jaki miał miejsce w pierwszej połowie 2007 r. Na jego przykładzie widać jak trudne może być rozróżnienie rodzajów działań niepożądanych wyłącznie w oparciu o motywację sprawców oraz przyświecające im cele.

Omawiany atak spowodowany został usunięciem 27 kwietnia 2007 r. z centrum Tallina (na miejscowy cmentarz wojskowy) pomnika żołnierzy Armii Czerwonej (tzw. Brązowego Żołnierza, upamiętniającego żołnierzy radzieckich poległych podczas wyzwalania Tallina z rąk niemieckich w 1944 r.), co doprowadziło do wielu protestów społeczności rosyjskojęzycznej, a nawet do dwudniowych zamieszek w Tallinie [13]. Rosja wystosowała w tej sprawie oficjalne ultimatum do rządu Estonii, wskazując, że nie godzi się na jakąkolwiek zmianę lokalizacji pomnika. Równocześnie, już wieczorem 27 kwietnia, na serwisy rządowe przypuszczony został atak DDoS (ang. *Distributed Denial of Service*) zaś w kolejnych dniach podobnymi atakami zostały dotknięte strony internetowe estońskiego parlamentu, poszczególnych ministerstw, służb, np. policji, a nawet partii politycznych czy szkół publicznych. 9 maja 2017 r. (czyli w dniu obchodzonym w Rosji jako Dzień Zwycięstwa) atak osiągnął swoje apogeum. W tym czasie unieruchomione zostały nie tylko serwisy rządowe czy administracyjne, ale nawet znaczna część systemów bankowych, portali informacyjnych, firm prywatnych itp. Co więcej, atak udało się przerwać dopiero 18 maja, po odcięciu całego ruchu sieciowego spoza Estonii, co ostatecznie pozwoliło rozwiązać problem.

Wyniki wnikliwych analiz, przeprowadzonych przez ekspertów estońskich przy współudziale specjalistów z krajów takich, jak Niemcy, Finlandia i Słowacja, a także przy wsparciu NATO, pozwoliły ustalić, że za atakiem stała m.in. młodzieżówka rosyjskiej partii Jedna Rosja oraz podporządkowana Kremlowi rosyjska organizacja „Nasi". Z tego też powodu atak na Estonię sklasyfikowany został jako pierwszy w historii przypadek prowadzenia tzw. cyberwojny [14].

W kolejnym z przywołanych przykładów, w 2014 r., w związku z planowanym wydaniem filmu „The Interview" (polski tytuł filmu to „Wywiad ze Słońcem Narodu"), będącego komedią stawiającą w niezbyt dobrym świetle przywódcę Korei Północnej Kim Dzong Una (w filmie Kim Jong-un), doszło do zmasowanego ataku na serwery firmy Sony. W jego wyniku niemożliwe stało się np. korzystanie z usług online, a także wykradzionych i ujawnionych zostało wiele prywatnych informacji oraz e-maili, w tym dotyczących pracowników firmy Sony oraz współpracujących z firmą gwiazd filmowych. Co więcej, grupa hakerów odpowiedzialnych za przeprowadzenie tego ataku wydała również oświadczenie, że jeśli film trafi do kin, przeprowadzony zostanie kolejny atak

„o skali ataków z 11 września" [11]. W efekcie premierę filmu odwołano, a firma Sony poniosła ogromne straty zarówno wizerunkowe, jak i finansowe.

Przeprowadzone przez agentów FBI we współpracy z ekspertami firm Sony i FireEye dochodzenie wykazało, że atak na serwery Sony do złudzenia przypominał przeprowadzone rok wcześniej włamania na południowokoreańskie stacje telewizyjne i bankomaty. Narzędzia, których użyli przestępcy, miały bowiem praktycznie identyczny kod źródłowy co wirus, który znaleziono wcześniej na komputerach w Seulu. Ponieważ analizy wcześniejszego przypadku wskazywały, że ataki przeprowadzone zostały z inspiracji lub przez hakerów z Korei Północnej, stwierdzono, że za atakiem na Sony również stoi reżim Kim Dzong Una. Wydaje się to tym bardziej prawdopodobne, że gdy Sony zapowiedziało realizację „The Interview", Pjongjang głośno domagał się, by film ten nie trafił do kin, a koreański dyktator groził, że uzna tę komedię za akt wypowiedzenia wojny.

W tym przypadku, po zakończeniu drobiazgowego śledztwa, FBI poinformowało, że za spowodowanie cyberataku odpowiedzialna była Korea Północna, zaś sam atak został sklasyfikowany jako atak terrorystyczny na infrastrukturę teleinformatyczną przeprowadzony przez zależną od północnokoreańskiego reżimu grupę hakerską – Strażników Pokoju (ang. *Guardians of Peace*, *GOP*). Pomimo tak kategorycznych stwierdzeń FBI dotyczących zdolności Korei Północnej do prowadzenia działań w cyberprzestrzeni (potwierdzanych również przez inne służby USA), wielu specjalistów uważa, że GOP została po prostu wynajęta do przeprowadzenia tego ataku, co może świadczyć o braku, w tamtym czasie, możliwości jego pełnego przeprowadzenia przez reżim z Pjongjangu wyłącznie przez rodzimych specjalistów (zob. więcej [12, 13]). Wielu ekspertów łączy ten atak z upublicznieniem kliku niewydanych wcześniej filmów Sony Pictures (przed datą ich premiery), co może też świadczyć o cyprzestępczym (choćby częściowo) podłożu tego ataku. Wskazują, że przedmiotowe produkcje mogły zostać po prostu sprzedane nielegalnym serwisom hostingowym, co świadczyłoby o działaniu hakerów GOP również z chęci zysku.

W ostatnim z przywołanych przykładów, w kwietniu 2015 r., doszło do przerwy w nadawaniu programu przez wszystkie 12 kanałów francuskiej stacji TV5 Monde. Przestały działać także strony internetowe stacji. Na stronie internetowej TV5 Monde oraz na jej profilach społecznościowych, m.in. na Facebooku i Twitterze, umieszczone zostały komunikaty, że przerwa w funkcjonowaniu stacji nie wynika z awarii, ale jest efektem ataku przeprowadzonego przez islamską organizację terrorystyczną CyberKalifat (ang. *Cyber Caliphate*). Na stronie internetowej i w serwisach zamieszczono

również manifest polityczny organizacji, rzekome dane personalne francuskich żołnierzy biorących udział w operacjach przeciwko tzw. Państwu Islamskiemu oraz groźby pod ich adresem, a także pod adresem ich rodzin.

Porównując przedstawione przypadki, można stwierdzić, że o ile atak na stację TV5 Monde nie budzi żadnych wątpliwości i spełnia wszelkie przesłanki, by określić go jako akt cyberterroryzmu – jednoznaczny jest bowiem motyw sprawców wykazany w ich manifeście politycznym, jasny jest również cel ataku wyrażony w groźbach dla konkretnych francuskich żołnierzy i ich rodzin – o tyle dwa pozostałe przykłady budzą już znaczne trudności interpretacyjne. Czym bowiem różniły się ataki na estońskie serwery oraz na serwery firmy Sony, skoro jeden z nich zakwalifikowano jako działania o charakterze quasi-militarnym (zdefiniowane jako pierwszy przypadek cyberwojny) zaś drugi jako atak terrorystyczny na infrastrukturę teleinformatyczną?

Należy wyraźnie zaznaczyć, że oba ataki spełniają w zasadzie dwie, wymienione w opracowaniu T. Szubrychta, przesłanki, mogące świadczyć o ich cyberterrorystycznym podłożu (choć w różnym zakresie). W przypadku ataku na serwery Estonii motywacja sprawców była bowiem polityczna, ściśle związana z politycznym aktem przeniesienia w inne miejsce pomnika będącego symbolem zniewolenia narodu estońskiego w latach powojennych. W przypadku ataku na firmę Sony było podobnie, gdyż motywacja sprawców też miała charakter polityczny i wynikała z zamiaru wprowadzenia do kin filmu ośmieszającego dyktatora Korei Północnej. Co do celów, jakie przyświecały sprawcom obu omawianych ataków, to z pewnością jednym z nich, w każdym z powyższych przypadków, było wyrządzenie strat stronie atakowanej. O ile jednak w przypadku ataku na estońską infrastrukturę teleinformatyczną działania strony atakującej z pewnością wzbudziły powszechny strach w społeczeństwie estońskim (ze względu na znaczący poziom informatyzacji praktycznie wszystkich dziedzin życia i funkcjonowania społeczeństwa estońskiego oraz wynikający zeń bardzo duży stopień uzależnienia społeczeństwa od prawidłowego funkcjonowania serwisów rządowych, finansowych itp. oraz wszelkich innych usług świadczonych drogą elektroniczną), o tyle w przypadku ataku na systemy firmy Sony trudno doszukiwać się wśród jego adresatów powszechnego strachu. Pomimo tego, to właśnie atak na firmę Sony zakwalifikowany został jako atak cyberterrorystyczny, a działania wobec Estonii – jako akt cyberwojny.

Mając powyższe na uwadze, na podstawie zgromadzonych danych należy zadać pytanie, czy, skoro za atakiem na serwery firmy Sony stał reżim Kim Dzong Una, wskazana klasyfikacja samego ataku, jako ataku terrorystycznego, jak i jego źródła (grupa GOP) była właściwa. W tym przypadku ważnym wydaje się bowiem fakt, że

jeśli rzeczywiście GOP to grupa północnokoreańskich hakerów – większość analityków określa bowiem GOP jako ponadnarodową grupę hakerów działającą w wielu krajach na świecie – sponsorowanych przez północnokoreański reżim, to czy można tutaj klasyfikować jej działania jako terrorystyczne, czy raczej powinny zostać uznane za działania quasi-militarne lub militarne, realizowane przez struktury podległe dyktatorowi Korei Północnej – podobnie zresztą jak to miało miejsce w przypadku wcześniejszego ataku na infrastrukturę teleinformatyczną Estonii.

Należy bowiem zaznaczyć, że jeśli wyniki analiz FBI są prawdziwe, to zarówno w jednym, jak i w drugim przypadku za atak odpowiadają struktury zależne, a być może i finansowane przez rządy – odpowiednio Rosji oraz Korei Północnej. Gdyby jednak okazało się, że GOP jest jedną z wielu grup hakerów, i że została wynajęta do przeprowadzenia ataku na systemy firmy Sony, trudno byłoby uznać ją za grupę terrorystyczną, a same ataki za akty cyberterrorystyczne. Co więcej, po dokonaniu wnikliwej analizy ataku na stację TV5 Monde, pojawiają się również inne wątpliwości, gdyż wiele przesłanek świadczy o tym, że stoi za nim powiązana z Kremlem i sponsorowana przez Rosję grupa hakerów rosyjskich Fancy Bear[1]. Tym samym ataku na serwisy TV5 Monde również nie powinno się klasyfikować jako aktu cyberterrorystycznego.

Duży poziom skomplikowania systemów informacyjnych oraz coraz bardziej złożony charakter dotyczących ich zagrożeń, a także wynikająca zeń trudność w ścisłym określeniu miejsca cyberterroryzmu w tym obszarze, wymaga zdefiniowania na nowo, czym są i jakimi cechami charakteryzują się tego typu działania. Bazując na wnikliwej analizie etymologii przedmiotowego problemu, przedstawionej w opracowaniu T. Szubrychta, oraz uwzględniając przedstawione w artykule nowe uwarunkowania, celowym wydaje się oprzeć tę definicję nie tylko na motywacji sprawców i celach, jakie im przyświecają, lecz również uwzględnić charakter, przynależność oraz sposób finansowania osoby lub grupy osób dokonujących ataków na elementy lub z wykorzystaniem elementów cyberprzestrzeni. Definiując zjawisko, jakim jest cyberterroryzm, niecelowym wydaje się przy tym jego ograniczanie wyłącznie do skutków dla infrastruktury teleinformatycznej czy

1 Fancy Bear określana jest również jako APT28. To mająca swoją siedzibę w Petersburgu, powiązana z FSB grupa hakerów, odpowiedzialna m.in. za włamania do niemieckich serwerów rządowych i Bundestagu, na serwery: holenderskich agend rządowych oraz Holenderskiej Rady Bezpieczeństwa, ukraińskiej Centralnej Komisji Wyborczej, amerykańskiej Partii Demokratycznej, Światowej Agencji Antydopingowej (WADA), rządowe RP, NATO, Europejskiej Organizacji Bezpieczeństwa i Współpracy (OSCE) i wiele innych – zob. więcej [15, 16, 17].

systemów informacyjnych strony atakowanej, gdyż – jak pokazały przypadki operacji Nitro Zeus[2] czy choćby testu Aurora[3] – za pośrednictwem dostępu przez sieci teleinformatyczne możliwe jest zdalne zniszczenie także innych, niezwiązanych bezpośrednio z siecią elementów infrastruktury technicznej strony atakowanej.

Mając powyższe na uwadze, cyberterroryzm można zdefiniować jako celowe działanie*:*

a) podejmowane przez organizacje terrorystyczne lub przez inne osoby, grupy osób, podmioty itp. z nimi związane lub sympatyzujące albo działające na ich zlecenie,
b) w odniesieniu do lub z wykorzystaniem elementów cyberprzestrzeni,
c) mające na celu wyrządzenie stronie atakowanej szkody z pobudek politycznych, ideologicznych, społecznych i/lub religijnych oraz wprowadzenie zamieszania, poczucia niepewności lub zastraszenia określonej populacji albo wymuszenia na rządzie lub tej populacji określonych działań i/lub zachowań.

Stosując powyższą definicję, nie można żadnego z opisanych ataków zakwalifikować jako atak cyberterrorystyczny, co zresztą wydaje się być w pełni uzasadnione. Zarówno bowiem atak na estońską infrastrukturę teleinformatyczną, jak i czasowe wyłączenie kanałów informacyjnych stacji TV5 Monde wpisują się w obserwowane przez ostatnie kilkanaście lat coraz szersze wykorzystywanie przez Rosję zarówno systemów informacyjnych, jak i technik dezinformacji (np. nadawane w wielu wersjach językowych, sponsorowane przez Kreml kanały informacyjne telewizji Russia Today czy opłacane przez instytucje rosyjskie tzw. Fabryki Trolli) do wpływania na wewnętrzną sytuację polityczną oraz celową destabilizację poszczególnych państw, a tym samym na destabilizację potencjalnych przeciwników, tj. Stanów Zjednoczonych czy Unii Europejskiej.

Z kolei atak na serwery firmy Sony, jeśli był zrealizowany przez hakerów północnokoreańskich lub działających na zlecenie reżimu z Pjongjangu, powinien zostać w tym przypadku zakwalifikowany jako działania quasi-militarne, a więc z pogranicza

2 Celem operacji Nitro Zeus było unieruchomienie, w przypadku konfliktu zbrojnego, systemów obrony powietrznej Iranu, jego systemów komunikacyjnych i kluczowych części infrastruktury energetycznej. Jej elementem było opóźnienie irańskiego programu budowy broni jądrowej z wykorzystaniem robaka StuxNET – zob. więcej [18].

3 W 2007 r. w Narodowym Laboratorium w Idaho (ang. *Idaho National Laboratory*) przeprowadzono test możliwości zdalnego zniszczenia generatora diesla przy użyciu oprogramowania sterującego dołączaniem go do sieci elektroenergetycznej – przez częste odłączanie i ponowne włączanie go do sieci, a tym samym celową desynchronizację jego pracy, spowodowano fizyczne zniszczenie generatora.

cyberprzestępczości (zachodzi bowiem podejrzenie, że stojąca za atakiem grupa hakerska GOP nie działała wyłącznie z pobudek politycznych) i cyberwojny, co zresztą byłoby zgodne z oświadczeniem Kim Dzong Una, iż wprowadzenie „The Interview" jest dla niego równoznaczne z wypowiedzeniem wojny.

2. Współczesny terroryzm – obszary wykorzystania cyberprzestrzeni

Analizując ewolucję sposobu działania oraz podejścia współczesnych grup terrorystycznych do wykorzystania cyberprzestrzeni, należy odpowiedzieć na pytanie, dlaczego coraz częściej przenoszą one swoje działania do Internetu. Do określenia rzeczywistej skali zagrożenia istotne jest też to, do czego i w jakim zakresie mogą, a także, w jaki sposób i w jakim zakresie są w stanie wykorzystać nowoczesną technologię oraz podłączone do ogólnoświatowej sieci urządzenia teleinformatyczne. Szczególnie istotna wydaje się przy tym kwestia, czy terroryści mogą wykorzystać cyberprzestrzeń do realizacji ataków o podobnym znaczeniu i skutkach oddziaływania jak to miało miejsce w przypadku ataków z 11 września 2001 r. na World Trade Center. Odpowiedź na pierwsze z pytań wydaje się prosta, choć należy wskazać kilka powodów tego zjawiska.

Powód 1 – dostępność

Internet jest obecnie łatwo dostępny praktycznie w każdym miejscu na ziemi. Co więcej, dostęp do sieci jest możliwy również z wykorzystaniem miniaturowych urządzeń przenośnych, takich jak smartfony czy tablety, które są stosunkowo niedrogie, a przy tym łatwe do przenoszenia czy nawet ukrycia.

Powód 2 – anonimowość i przydatność do celów komunikacyjnych

Natłok ruchu sieciowego, użytkowników i informacji występujących aktualnie w Internecie daje poczucie pewnej anonimowości. Trudno bowiem wyobrazić sobie możliwość jednoczesnego podsłuchiwania czy choćby identyfikacji miliardów użytkowników sieci. Co więcej, w Internecie nie ma żadnych granic, które mogłyby przeszkadzać w komunikowaniu się, czy w błyskawicznym przekazywaniu informacji na praktycznie dowolne odległości. Warto zauważyć, że obecnie przekazanie nawet obszernego dokumentu czy wielu zdjęć pomiędzy odległymi kontynentami zajmuje zaledwie kilka sekund.

Z tego też powodu współczesny Internet jest idealnym narzędziem do komunikowania się. Dotychczasowe, tradycyjne środki komunikacji z pewnością są łatwo

dostępne, niedrogie jak i łatwe w użyciu. Ich dostępność zależy jednak od obecności skomplikowanej infrastruktury telekomunikacyjnej. W dużych miastach z reguły nie ma z tym problemów, ale poza nimi, w odległych rejonach czy np. w górach, mogą występować problemy z dostępem do sieci nie tylko przewodowej, ale również komórkowej. Należy też zaznaczyć, że tradycyjne środki łączności, zwłaszcza podczas rozmów międzynarodowych lub satelitarnych, mogą być bardzo kosztowne. Są również podatne na podsłuch[4] co wykazało choćby namierzenie Osamy bin Ladena czy innych członków kierowanej przezeń organizacji terrorystycznej. A przecież nie tylko amerykańskie służby dysponują tego typu technologią, już bowiem w 1996 r. Rosjanie namierzyli i zamordowali w ten sposób przywódcę Czeczenów, Dżochara Dudajewa.

Co prawda wśród standardowych środków łączności dostępne są również urządzenia z wbudowanym szyfrowaniem, a więc zabezpieczone przed tego typu podsłuchem, nie zmienia to jednak faktu, że wykorzystują one tę samą infrastrukturę, zatem – poza odpornością na podsłuch – posiadają wszystkie wady charakterystyczne dla tradycyjnych środków łączności, choć ich obecny koszt nie stanowi dla organizacji terrorystycznych znaczącej przeszkody w ich stosowaniu.

W przypadku komunikowania się przez Internet, większość opisanych wcześniej ograniczeń nie występuje. Co więcej sieć dostępna jest praktycznie wszędzie i umożliwia komunikowanie się z dowolnego miejsca na ziemi, w dowolnym czasie, bez względu na porę dnia czy roku. Komunikować się przez Internet można nie wychodząc z domu, jak i z dowolnego miejsca publicznego lub nawet w czasie podróży, z wykorzystaniem infrastruktury prywatnej, komercyjnej, a nawet publicznych, bezpłatnych punktów dostępowych, i to niezależnie od kraju, regionu czy kontynentu. Oczywiście komunikacja przez Internet również może być monitorowana. E. Snowden ujawnił choćby istnienie programów PRIZM[5] czy XKeycore[6], lecz z pewnością w przypadku Internetu jest to przedsięwzięcie znacznie trudniejsze w realizacji niż w przypadku tradycyjnych

4 Dzięki programowi Echelon amerykańska agencja NSA mogła automatycznie identyfikować, a nawet namierzać pojedynczych rozmówców. Funkcjonalność ta była dość powszechnie wykorzystywana, np. przy tropieniu członków Al Kaidy.

5 PRIZM (ang. *surveillance program*) to tajny amerykański program szpiegowski, administrowany od 2007 r. przez NSA, umożliwiający wywiadowi Stanów Zjednoczonych dostęp do danych gromadzonych na serwerach największych przedsiębiorstw internetowych, jak również gromadzenie tych danych na własny użytek; dane nt. tego programu ujawnił w 2013 r. były analityk pracujący dla NSA Edward Snowden, który przekazał informacje na jego temat brytyjskiej i amerykańskiej prasie – zob. więcej [21].

6 E. Snowden upublicznił m.in. wewnętrzną prezentację NSA dotyczącą funkcjonalności tego programu – zob. więcej [19].

środków łączności. Komunikacja i wymiana informacji może bowiem odbywać się za pomocą systemu poczty elektronicznej, ogólnodostępnych serwisów webowych, w tym specjalnych stron internetowych, jak też z wykorzystaniem specjalistycznych aplikacji, sieci społecznościowych, jak Facebook czy Twitter. Wymiana informacji jest też możliwa z wykorzystaniem aplikacji i technologii chmury, przy czym w każdym z tych przypadków, do komunikacji można wykorzystywać zarówno urządzenia stacjonarne, jak i powszechne obecnie smartfony i tablety.

Okazuje się, że to właśnie te powody sprawiają, iż różnego rodzaju grupy terrorystyczne wybierają komunikację internetową jako tańszą i bezpieczniejszą w stosowaniu. Tzw. Państwo Islamskie (ISIS) wydało nawet specjalną instrukcję[7], jak jej używać z wykorzystaniem dodatkowych narzędzi do szyfrowania, tak, by było to jeszcze bezpieczniejsze i by ustrzec ich członków przed wykryciem, podsłuchem czy namierzeniem. W instrukcji tej zaleca się przede wszystkim stosowanie szyfrowania, wskazując przy tym, że ogólnodostępne serwisy, nawet jeśli posiadają taką funkcjonalność, mogą współpracować z rządami różnych krajów, tak jak ma to miejsce w przypadku amerykańskiej NSA. Z tego też powodu specjaliści ISIS zalecają stosowanie niezależnych systemów poczty elektronicznej, takich jak np. szwajcarski Proton Mail, który umożliwia szyfrowanie całej transmisji pomiędzy dwoma użytkownikami. Zapewnia on również w miarę bezpieczną wymianę e-maili z innymi systemami pocztowymi, będąc tym samym nie tylko bezpiecznym, ale i dosyć uniwersalnym rozwiązaniem. ISIS zaleca też szyfrowanie samych plików w wykorzystaniem na przykład starszej wersji TrueCrypta (w nowej wersji pojawiły się wątpliwości jeśli chodzi o jej bezpieczeństwo) lub przy użyciu alternatywnego narzędzia o nazwie VeraCrypt, umożliwiającego proste, szybkie i bardzo skuteczne szyfrowanie wszelkiego rodzaju danych, które później bez obaw można przesyłać przez Internet, w tym również za pośrednictwem zwykłych e-maili.

Z uwagi na dużą popularność, grupy terrorystyczne dosyć powszechnie wykorzystują też sieci społecznościowe. Dlatego też w omawianym poradniku duży jego fragment poświęcono właściwej konfiguracji oraz zasadom poprawnego wykorzystania popularnego Twittera, który posiadając wbudowaną funkcję szyfrowania, przy właściwym użyciu, zapewnia w miarę bezpieczną komunikację, umożliwiając przy

7 Do autorstwa tego podręcznika przyznaje się również prywatna firma Cyberkow z siedzibą w Kuwejcie, która twierdzi, że pierwotnie opublikowała przewodnik w lipcu 2014 r. pod tytułem „Bezpieczeństwo operacyjne dla dziennikarzy, działaczy i pracowników praw człowieka w Strefie Gazy" – zob. więcej [22].

tym rozsyłanie w krótkim czasie znacznych ilości informacji. Co więcej, rosnąca liczba użytkowników Twittera do pewnego stopnia ułatwia zachowanie anonimowości i ukrycie wymiany informacji pomiędzy członkami danej grupy. Część z nich może bowiem komunikować się tylko w trybie prywatnym lub być wyłącznie biernymi odbiorcami przekazywanych treści. Nie bez znaczenia jest też fakt, że Twitter, jako platforma wielojęzykowa, wspiera również język arabski oraz – dzięki możliwości zamieszczania linków i załączników – umożliwia wymianę informacji z systemami działającymi w oparciu o inną technologię. Powszechne jest również wykorzystywanie różnego rodzaju komunikatorów tekstowych, w tym tak popularnych, jak posiadający odrębną arabską wersję Telegram czy uważany za bardzo bezpieczny CryptoCat. Oba wymienione rozwiązania pozwalają bowiem na bezpieczną, bo w pełni szyfrowaną, wymianę wiadomości tekstowych pomiędzy wybranymi użytkownikami, i to zarówno pomiędzy pojedynczymi osobami, jak i zdefiniowanymi ich grupami.

Z innych narzędzi zapewniania bezpieczeństwa transmisji omawiany podręcznik zaleca też stosowanie technologii VPN polegającej na szyfrowaniu całego strumienia przesyłanych danych i przekazywania ich przez coś w rodzaju tunelu przez ogólnodostępne sieci teleinformatyczne. Wykorzystywane w nich algorytmy i klucze zapewniają przy tym bardzo wysoki poziom bezpieczeństwa przekazywanych danych, uniemożliwiając ich przejęcie lub choćby podejrzenie przez osoby niepowołane. W podręczniku szczególnie polecane jest stosowanie komercyjnego systemu Freedom firmy F-Secure, umożliwiającego nie tylko szyfrowanie połączeń, ale w pewnym stopniu również anonimizację lokalizacji respondentów, dając użytkownikowi możliwość wyboru lokalizacji serwera VPN czy też funkcję *tracking protection*.

Innym narzędziem, dosyć szeroko wykorzystywanym przez grupy terrorystyczne, jest sieć TOR (ang. *The Onion Routing)* – wielopoziomowa sieć z pełną anonimizacją ruchu, w której wszelkie dane przekazywane są w postaci zaszyfrowanej przez bezpieczne serwery. Dzięki takiemu rozwiązaniu praktycznie wyeliminowana została możliwość prowadzenia przez służby analizy ruchu sieciowego, co w znacznej mierze zapewnia ukrycie tożsamości użytkownika tej sieci i zabezpiecza go przed wykryciem i namierzeniem. Wielopoziomowe tunelowanie uniemożliwia też określenie, od którego z użytkowników Internetu pochodzą przekazywane przez tę sieć dane.

Ponieważ jednak terroryści często nie tylko ukrywają swoją tożsamość, ale nawet informacje, które między sobą przesyłają lub udostępniają, wykorzystywane są w tym celu metody steganograficznego ukrywania informacji polegające na jej ukryciu wewnątrz innego pliku, będącego np. zdjęciem, filmem, utworem muzycznym itd.

Stosowane obecnie narzędzia umożliwiają takie rozproszenie danych, że plik źródłowy praktycznie nie różni się od pliku zawierającego ukrytą informację, co umożliwia nie tylko skryte jej przesyłanie, ale wręcz zamieszczanie na ogólnodostępnych serwerach, tak, by osoba wtajemniczona mogła je samodzielnie pobrać z sieci. Dodatkowe mechanizmy szyfrowania zapewniają przy tym, że ekstrakcji ukrytej informacji będzie mogła dokonać wyłącznie osoba dysponująca właściwym kluczem.

Ponieważ w konkretnych sytuacjach można założyć, że odpowiedzialne za zapewnienie bezpieczeństwa służby, nie mogąc podsłuchiwać zaszyfrowanych rozmów, mogą wyłączać sieć na konkretnym obszarze, poradnik ISIS zaleca stosowanie rozwiązania bazującego na tym, że współczesne urządzenia mogą samodzielnie komunikować się między sobą. Jednym z narzędzi tego typu, które można wykorzystać w sytuacji braku dostępności sieci, jest oprogramowanie FireChat. Pozwala ono na komunikowanie się ze sobą urządzeń bez pośrednictwa sieci, wyłącznie z wykorzystaniem interfejsów BlueTooth lub Wi-Fi. Dzięki temu możliwe jest tworzenie nawet dosyć obszernych systemów lokalnych, w których zaszyfrowane informacje mogą być przekazywane pomiędzy dwoma użytkownikami za pośrednictwem urządzeń innych użytkowników. W przypadku braku dostępu do sieci, wysłana informacja zostanie zapisana w każdym z urządzeń, i w przypadku, gdy jedno z nich znajdzie się w zasięgu innej sieci lub Internetu, zostanie przesłana dalej, do innego użytkownika. Tego typu rozwiązania mogą być bardzo użyteczne dla współczesnych grup terrorystycznych, gdyż nawet największe światowe agencje wywiadowcze będą mieć problem z ich wykryciem, a tym bardziej z ich lokalizacją.

Powód 3 – nieograniczone zasoby informacyjne

Internet to nie tylko globalna sieć komunikacyjna, ale przede wszystkim ogromny rezerwuar informacji, który już wykorzystują grupy terrorystyczne. Dlaczego akurat Internet jest w tym przypadku szczególnie użyteczny? Bo tradycyjne źródła informacji są po prostu zbyt rozproszone. Z tego też powodu bardzo utrudniony może okazać się dostęp do konkretnych informacji. W tradycyjnych źródłach, wśród wszystkich zgromadzonych w nich zasobów, bardzo trudno jest odnaleźć te informacje, które nas w danym momencie najbardziej interesują. Część z nich może być niedostępna, co wymusza konieczność samodzielnego ich zdobycia. W szczególnych przypadkach mogłoby to pozwolić odpowiednim służbom na wykrycie i zidentyfikowanie osób szczególnie zainteresowanych np. konkretnym obiektem czy instalacją. Wiele służb

używa w tym celu bardzo wyszukanych narzędzi, jak np. systemu TrapWire potrafiącego samodzielnie rozpoznawać i śledzić zdefiniowane wcześniej cele.

Z tego też powodu organizacje terrorystyczne coraz chętniej wykorzystują Internet do zdobywania potrzebnych im informacji. Po pierwsze jest on bowiem niezwykle podatny na przeszukiwanie – zarówno przy użyciu specjalistycznych narzędzi, jak również przy wykorzystaniu najzwyklejszych wyszukiwarek. Po drugie, jest dostępny praktycznie dla każdego, wszędzie i o każdej porze. Przeszukiwanie jego zasobów może być zatem realizowane przez dowolne osoby czy grupy osób, w dowolnym czasie i miejscu. Po trzecie, w Internecie można znaleźć praktycznie wszystko i przy wykorzystaniu właściwych metod nie powinno być problemu ze znalezieniem potrzebnych informacji. Oczywiście mogą one być fragmentaryczne i znajdować się np. w zamieszczonych zdjęciach, dokumentach czy książkach lub w zasobach tzw. głębokiego Internetu[8] albo być dostępne w różnych wersjach językowych. Można jednak założyć, że w każdym z powyższych przypadków, przy wykorzystaniu wydajnych narzędzi do wyszukiwania informacji i korelacji danych pochodzących z różnych źródeł, a także coraz lepszych i wydajniejszych translatorów, w Internecie, w tym w szczególności w jego głębokich, często normalnie niedostępnych zasobach lub w tzw. ciemnym Internecie[9], powinno być możliwe odszukanie praktycznie każdej potrzebnej informacji, w tym tak kluczowych z punktu widzenia grup terrorystycznych, jak:

- przepisów na budowę bomb, miniaturowych podsłuchów, nadajników lub odbiorników radiowych itp.,
- instrukcji produkcji materiałów wybuchowych z filmami instruktażowymi oraz demonstracją poszczególnych czynności włącznie.

Nie bez znaczenia jest też fakt, że znajdujące się w sieci informacje, zdjęcia, filmy i mapy, a nawet obrazy z kamer pracujących on-line, znacząco ułatwiają prowadzenie rozpoznania potencjalnych celów ataków. Dzięki nim można zlokalizować konkretną instalację i instytucję oraz zyskać dostęp do szczegółowych zdjęć lotniczych, nawet

8 Angielskie określenia *Deep Internet*, *Deep Web*, *Hidden Web* lub *Invisible Web* odnoszą się do tej części zasobów internetowych (tzw. Wold Wide Web), które nie są indeksowane przez standardowe wyszukiwarki; tworzą go np. bazy danych, biblioteki, witryny sklepowe niedostępne dla ogółu społeczeństwa, zasoby akademickie prowadzone przez uczelnie, katalogi biblioteczne czy wewnętrzne sieci uczelniane – zob. więcej [20].

9 Angielskie określenia *Dark Intenet*, *DarkNet* lub *Dark Web* odnoszą się do celowo ukrytej części zasobów Internetu, która może być przeglądana jedynie przy użyciu specjalnego oprogramowania, np. TOR, Freenet, I2P itp.

w trybie 3D. Można również znaleźć wiele rzeczywistych zdjęć konkretnych obiektów (np. w usłudze Google Street View) z możliwością ich obejrzenia z wielu stron, zlokalizowania słabych punktów i zabezpieczeń itp.

Powód 4 – narzędzie propagandowe

Współczesny Internet to nie tylko narzędzie komunikacji i nieograniczona baza danych, ale również doskonały nośnik medialny, dzięki czemu może być w prosty sposób wykorzystany w niezwykle istotnych dla grup terrorystycznych celach propagandowych. Może być przy tym znacznie tańszym i pewniejszym narzędziem propagandowym od dotychczas wykorzystywanych mediów tradycyjnych. Należy bowiem podkreślić, że budowa i utrzymanie tych ostatnich są niezwykle kosztowne, a i tak mają coraz mniejszy zasięg oddziaływania, ograniczający się zazwyczaj do zasięgu nadajnika telewizyjnego lub do obszaru dostępności sygnału satelitarnego.

W tym przypadku media elektroniczne mają znaczącą przewagę nad mediami tradycyjnymi, gdyż, z małymi wyjątkami, dostępne są wszędzie tam, gdzie jest Internet, mają zatem dużo większą siłę oddziaływania. Grupy terrorystyczne bardzo chętnie publikują na przykład materiały propagandowe, by przekonywać do swojej sprawy, prezentować swój punkt widzenia oraz wygodne dla siebie materiały. W sieci zamieszczane są również, charakterystyczne dla grup terrorystycznych, materiały, których celem jest zastraszanie całych społeczności, a nawet narodów lub wybranych, konkretnych osób, zawierające np. filmy lub zdjęcia z egzekucji pojmanych przeciwników lub z przeprowadzanych zamachów terrorystycznych. Nie brakuje też treści propagandowych, których celem jest zdobycie nowych zwolenników, rekrutacja terrorystów, samobójców czy nawet kobiet i dzieci.

Do celów propagandowych organizacje terrorystyczne chętnie wykorzystują nie tylko specjalnie tworzone internetowe kanały medialne, ale również bardzo popularne obecnie sieci społecznościowe. W wielu przypadkach to właśnie przez Facebooka i Twittera przekazywane lub udostępniane są przedmiotowe materiały propagandowe, prowadzona jest rekrutacja nowych zwolenników lub męczenników, co jest o tyle łatwiejsze, że część wykorzystywanych do tego celu aplikacji wspiera lub posiada arabskie wersje językowe.

Powód 5 – miejsce nielegalnego handlu oraz dodatkowe źródło finansowania

Internet może być postrzegany nie tylko jako narzędzie komunikacji czy propagandy lub jako źródło informacji, ale wykorzystywany do innych, niekoniecznie legalnych celów. Przykładem mogą być choćby giełdy działające w tzw. DarkNecie[10], na których można kupić wiele nielegalnych rzeczy – od podręczników do konstrukcji bomb i narkotyków począwszy, na broni kończąc. Serwisy takie z reguły funkcjonują w zapewniających anonimowość sieciach TOR, dzięki czemu praktycznie niemożliwe staje się namierzenie zarówno sprzedających, jak i kupujących. Co prawda służby różnych krajów starają się śledzić transfery pieniężne, mogące świadczyć o prowadzeniu przez obserwowane osoby czy grupy osób nielegalnych transakcji, lecz w przypadku, gdy jako środek płatniczy wykorzystywane są różnego rodzaju e-pieniądze (np. bitcoiny) nawet tak zaawansowane metody śledcze stają się bezużyteczne.

Z uwagi na te specyficzne funkcjonalności DarkNetu świetnie nadaje się on do prowadzenia w miarę bezpiecznego obrotu nielegalnymi towarami i usługami, i z tego też powodu grupy terrorystyczne często wykorzystują go do zapewnienia sobie zaopatrzenia w broń lub inne produkty podwójnego zastosowania, ale też i do zdobywania funduszy niezbędnych do ich właściwego funkcjonowania. Nie da się bowiem ukryć, że w wielu przypadkach swoistymi źródłami dochodów grup terrorystycznych są narkotyki (np. dla większości tego typu grup działających w Afganistanie lub Pakistanie stanowią one główne źródło dochodów) czy inne nielegalnie zdobywane towary. Wykorzystanie więc DarkNetu do ich sprzedaży wydaje się być, z punktu widzenia metod i zakresów działania grup terrorystycznych, rozwiązaniem ze wszech miar pożądanym.

Powód 6 – nowe rodzaje ataków

Terroryści coraz częściej interesują się wykorzystaniem cyberprzestrzeni także do prowadzenia wrogich działań wobec swoich oponentów. Media nie raz już donosiły na przykład o hakerach pracujących dla tzw. Państwa Islamskiego. Dotychczas zrealizowanych zostało zresztą kilka spektakularnych ataków DDoS (głównie na serwisy i firmy medialne), przy czym nie jest do końca jasne, czy za ataki te odpowiadają rzeczywiście wyłącznie grupy terrorystyczne. Faktem natomiast jest, że przynajmniej w kilku z takich przypadków ataki obejmowały nie tylko zakłócenie pracy tych serwisów, ale w dużej

10 Najbardziej znaną tego rodzaju giełdą był, zamknięty przez FBI w 2013 r., tzw. SilkRoad.

mierze również wykorzystanie ich infrastruktury do celów propagandowych (np. przez podmianę treści na prowadzonych przez nie stronach internetowych). W ostatnich latach odnotowano też kilka kampanii phishingowych z użyciem oprogramowania złośliwego, służącego do kradzieży pieniędzy z kont bankowych, o których przeprowadzenie podejrzewane są grupy wspierające organizacje terrorystyczne (w tym np. Islamic State Hacking Division, United CyberCaliphate).

Podsumowanie

W artykule wykazano, iż obecnie grupy terrorystyczne wykorzystują cyberprzestrzeń głównie jako narzędzie do komunikowania się i planowania, a nie do prowadzenia ataków. Cyberprzestrzeń wykorzystywana jest też przez nie z powodzeniem do celów propagandowych, a nawet do pozyskiwania narzędzi czy środków finansowych niezbędnych do ich funkcjonowania. Zjawiska te, z uwagi na większy poziom bezpieczeństwa w zakresie obrotu towarami nielegalnymi czy rosnące możliwości zdobywania środków finansowych z wykorzystaniem nowoczesnego malware'u, czyli złośliwego oprogramowania (w tym np. typy RansomWare), mogą w najbliższym czasie się nasilać. Niestety, w tym obszarze można założyć zwiększenie zainteresowania grup terrorystycznych infrastrukturą krytyczną. Problemem jest bowiem to, że coraz więcej ważnych systemów stanowi lub będzie stanowić element cyberprzestrzeni lub choćby posiada lub będzie posiadać połączenie z Internetem. Jeśli zatem podstawowe systemy sektora energetycznego, finansowego albo innego, krytycznego z punktu widzenia państwa lub bezpieczeństwa obywateli, mają obecnie lub będą miały połączenie z Internetem, to naturalnym wydaje się, że organizacje terrorystyczne mogą być zainteresowane ich destabilizacją lub zniszczeniem.

Złamanie zabezpieczeń dobrze chronionych i właściwie skonfigurowanych systemów nie należy do zadań łatwych i wymaga albo bardzo dużej wiedzy, czyli zaangażowania do realizacji tego celu dużej grupy dobrych hakerów, albo, co wydaje się naturalne, może być możliwe z wykorzystaniem specjalistycznego oprogramowania złośliwego. Już bowiem przypadek stworzonego przez CIA i Mosad StuxNETA pokazał, że przy użyciu nowoczesnego malware'u można dokonać nawet fizycznej destrukcji istotnej infrastruktury przeciwnika. Oczywistym przy tym wydaje się, że stworzenie odpowiednio zaawansowanego oprogramowania złośliwego nie jest zadaniem łatwym, ale należy zauważyć, że kody wielu tego typu programów zostały już publicznie ujawnione i przeanalizowane, dzięki czemu wielu hakerów na jego podstawie stworzyło

i wciąż tworzy nowe wersje coraz bardziej zaawansowanego malware'u. Jeśli więc grupy terrorystyczne nie będą w stanie same stworzyć nadającego się do realizacji ataku oprogramowania złośliwego, mogą go po prostu kupić. Podobnie, w przypadku braku odpowiedniej klasy specjalistów, do ataków na istotne z punktu widzenia terrorystów cele, w tym te szczególnie medialne, jak elektrownie czy choćby giełda, istnieje możliwość wynajęcia zewnętrznej grupy hakerów, przy czym koszty usług takich grup z pewnością znajdują się w zasięgu współczesnych grup terrorystycznych.

Mając powyższe na uwadze, kwestia zapewnienia odpowiedniego poziomu cyberbezpieczeństwa staje się więc coraz bardziej kluczowa, gdyż w przypadku zagrożeń tradycyjnych istnieje szansa, by je w porę wykryć i mieć czas na reakcję. Należy jednak założyć, że dobrze przygotowany atak na infrastrukturę krytyczną, przeprowadzony z wykorzystaniem elementów cyberprzestrzeni lub atak na systemy informacyjne albo na krytyczne elementy cyberprzestrzeni, może być atakiem trudnym do wykrycia, a przy tym błyskawicznym i tym samym niedającym czasu na organizację obrony. Jaki jest więc obecny poziom zagrożenia w tym zakresie? Wydaje się, że organizacje terrorystyczne obecnie w są w stanie na dużą skalę dokonać ataku cybernetycznego lub choćby ataku na infrastrukturę z wykorzystaniem elementów cyberprzestrzeni. Jednak biorąc pod uwagę wzrastający poziom komplikacji współczesnych systemów teleinformatycznych oraz rosnące uzależnienie struktur państwowych oraz całych społeczeństw od nowoczesnych technologii, już w niedalekiej przyszłości sytuacja ta może ulec zmianie.

Literatura

[1] Smolski W., *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*, Prawnicza i Ekonomiczna Biblioteka Cyfrowa, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2015.

[2] Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej 2005, nr 1(160).

[3] Kowalewski J, Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki Informacyjne" 2014, nr 1–2.

[4] Krztoń W., *Cyberterroryzm jako zagrożenie bezpieczeństwa w społeczeństwie informacyjnym*, „Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2012, nr 4, s. 89–100.

[5] Bielski K., *Cyberterroryzm – nowe zagrożenie bezpieczeństwa państwa w XXI wieku*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2015, nr 889; „Acta Politica", nr 34.

[6] Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.
[7] Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015.
[8] Nowak A., *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe AON" 2013, nr 3(92).
[9] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Ministerstwo Administracji i Cyfryzacji, 25 czerwca 2013 r.
[10] *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1–02, 8 listopada 2010 r. (z poprawkami z 15 lutego 2016 r.), https://fas.org/irp/doddir/dod/jp1_02.pdf (dostęp: 26.03.2019).
[11] White J., *Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies*, "Global Security Studies" 2016, nr 7(4).
[12] Ismail M., *Sony Pictures and the U.S. Federal Government: A Case Study Analysis of the Sony Pictures Entertainment Hack Crisis Using NormalAccidents Theory*, The University of Southern Mississippi 2017, praca magisterska, https://aquila.usm.edu/cgi/viewcontent.cgi?article=1360&context=masters_theses (dostęp: 26.03.2019).
[13] Haggard S., Lindsay J.R., *North Korea and the Sony Hack: Exporting Instability Through Cyberspace*, "Asia Pacific Issues, Analysis from the East-West Center" 2015, nr 117.
[14] Cendrowski W., *Cyberwojna i jej znaczenie dla bezpieczeństwa NATO w kontekście przypadków i dokumentów strategicznych*, Uniwersytet Pedagogiczny w Krakowie, Kraków 2017, http://rep.up.krakow.pl/xmlui/bitstream/handle/11716/2028/10--Cyberwojna-i-jej-znaczenie-dla-bezpieczenstwa-NATO--Cendrowski.pdf?sequence=1&isAllowed=y (dostęp: 26.03.2019).
[15] *Cybereason Intelligence Group – Owning the Battlefield Fighting the Growing Trend of Destructive Cyber Attacks*, https://www.cybereason.com/hubfs/Content%20PDFs/ Owning%20the%20Battlefield-Fighting%20the%20Growing%20Trend%20of%20Destructive%20Cyber%20 Attacks.pdf?t=1514399927494 (dostęp: 26.03.2019).
[16] Pols P., *Modeling Fancy Bear Cyber Attacks, Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks*, Cyber Security Academy (CSA).
[17] *FireEye iSight Intelligence*, "FireEye | APT28: At The Center Of The Storm" 2017.

[18] Stockburger P.Z., *Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum*, "American University International Law Review" 2016, nr 31(4).
[19] Prezentacja ujawniona przez E. Snowdena nt. programu XKeyscore, https://edward-snowden.com/wp-content/uploads/2013/10/2008-xkeyscore-presentation.pdf (dostęp: 26.03.2019).
[20] Szpunar M., *Sieć ukryta a sieć widzialna. O zasobach WWW nieindeksowanych przez wyszukiwarki*, „Przegląd Kulturoznawczy" 2014, nr 1(19).
[21] https://en.wikipedia.org/wiki/PRISM_(surveillance_program) (dostęp: 26.03.2019).
[22] https://www.wired.com/wp-content/uploads/2015/11/ISIS-OPSEC-Guide.pdf (dostęp: 26.03.2019).