Grudzień 2016

INSTYTUT KOŚCIUSZKI

BRIEF PROGRAMOWY INSTYTUTU KOŚCIUSZKI

Joanna Świątkowska, Magdalena Szwiec, Ana-Isabel Llacayo

„Jak zbudować bombę w kuchni Twojej mamy" – czyli jak terroryści wykorzystują cyberprzestrzeń i jak z nimi walczyć

autorzy

Dr Joanna Świątkowska – Dyrektor Programowy Europejskiego Forum Cyberbezpieczeństwa, redaktor naczelny European Cybersecurity Journal, ekspert Instytutu Kościuszki ds. cyberbezpieczeństwa

Magdalena Szwiec – współpracownik Instytutu Kościuszki. Absolwentka kierunku Stosunki Międzynarodowe, stypendystka Uniwersytetu w Tel Avivie, Uniwersytetu w Oslo i Uniwersytetu w Sienie.

Ana-Isabel Llacayo – współpracownik Instytutu Kościuszki. Absolwentka programu podwójnego dyplomu na kierunku Polityka Europejska ze specjalizacją Bezpieczeństwo i Stabilizacja Międzynarodowa Instytutu Nauk Policzycznych Uniwersytetu w Strasburgu oraz Centre for European Studies Uniwersytetu Jagiellońskiego.

Internet to broń obosieczna. Jak większość wynalazków będących efektem działań człowieka, może nieść wiele pożytku, ale także prowadzić do negatywnych konsekwencji. „Ciemna strona" sieci ujawnia się na rożne sposoby, służąc realizacji celów rozmaitych aktorów – przestępców, wrogich państw, ostatnio - coraz częściej - terrorystów.

Cyberprzestrzeń jest szczególnie atrakcyjna dla tych podmiotów, które z racji szeroko rozumianych różnic w potencjale mają mniejszą szansę konkurować z innymi graczami w konwencjonalnym wymiarze. Asymetryczność szeroko rozumianych zasobów sprawia, że słabsi gracze poszukują takich metod działania, które pozwolą im w tym nierównym wyścigu wyrównywać szanse.

Grupy terrorystyczne i pojedynczy terroryści dostrzegli takie właśnie zalety cyberprzestrzeni, wykorzystując ją w sposób wielowymiarowy. Jest to jedno w większych zagrożeń stojących przed społecznością międzynarodową. Jednocześnie każdy medal ma dwie strony - Internet dał całkiem nowe możliwości tym, którzy z terroryzmem walczą.

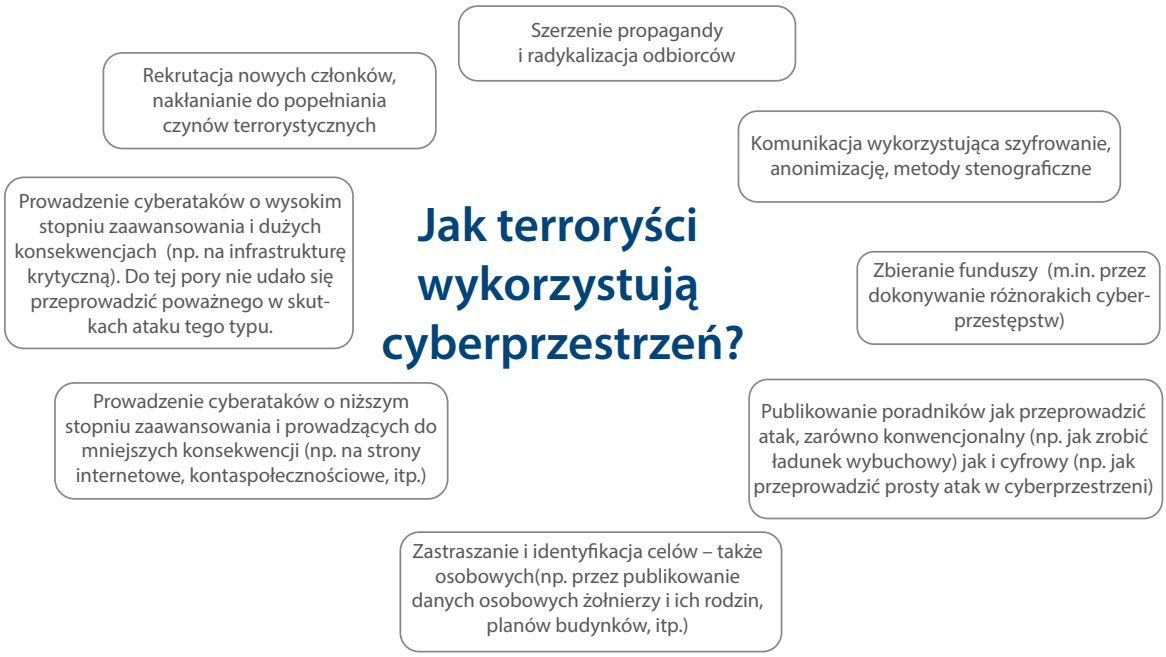
Celem niniejszego tekstu jest nie tylko przedstawienie wybranych metod wykorzystania cyberprzestrzeni przez terrorystów, ale także dokonanie krótkiego przeglądu działań prowadzonych przez pomioty, których główną odpowiedzialnością jest dbanie o bezpieczeństwo.

Jak naprawdę wygląda zagrożenie?

Terroryści bardzo łatwo dostosowują swoje metody działań do warunków, w jakich funkcjonują. Zmieniają taktykę oraz poszukują nowych perspektyw lub narzędzi, które pozwolą im osiągać założone cele. Internet przyniósł w tym zakresie bardzo wiele możliwości. Grupy terrorystyczne, takie jak Al–Qaeda, od lat korzystają z udogodnień Internetu. Już w latach 80-tych posługiwali się nim głównie do celów propagandowych[1]. Internet był także ważnym narzędziem przy przygotowaniu ataków z 11 września; służył głównie do komunikacji, planowania i pozyskiwania

1 J. Scott, D. Spaniel, *The Anatomy of Cyber-Jihad*, Institute For Critical Infrastructure Technology, 2016, s.5.

ISSN 1689-9873



finansowania[2]. Jednakże, choć terroryści od lat używają cyberprzestrzeni do prowadzenia swoich działań, to w ostatnich latach nastąpił ogromy rozkwit tego procederu. Powyższy graf ilustruje, w jakim celu i do jakich działań terroryści eksplorują sieć.

Warto podkreślić, że do tej pory nie mieliśmy do czynienia ze spektakularnymi przypadkami udanych cyberataków mających poważne konsekwencje w świecie fizycznym, aktów, które można by zdefiniować jako cyberterroryzm. Owszem, coraz częściej pojawiają się informacje, że terroryści próbują dokonywać destrukcyjnych działań za pomocą cyberataków, lecz na razie są to próby nieudane.

Obecnie dominującą formą działania jest wykorzystywanie cyberprzestrzeni jako instrumentu wspierającego konwencjonalne działania. Jednym z przykładów jest używanie sieci do komunikacji, zdobywania finansowania, rozpowszechniania propagandy czy wiedzy na temat tego, jak przeprowadzać ataki. Terroryści publikują w sieci poradniki wyjaśniające przygotowanie narzędzi zamachu. Przykładem może być publikacja *How to Make a Bomb in the Kitchen of your Mom*[3] tłumacząca czytelnikowi, jak stworzyć bombę w domowych warunkach, *Mujahideen Poisons Handbook* pomagająca przygotować trucizny, czy choćby *Encyclopedia of Jihad* zwierająca całe rozdziały o tym jak zabijać[4]. Ponadto terroryści poszukują w Internecie informacji o obiektach i podmiotach, którymi są zainteresowani. Jak sami wskazują, w sieci, na ogólnodostępnych stronach, można znaleźć około 80% informacji o danym celu[5]. Informacje o celach ataku są następnie skutecznie dystrybuowane. Niedawno, używając specjalnie dedykowanej aplikacji, terroryści rozpowszechnili listę celów – około 4000 nazwisk osób, do zlikwidowania których w imię zemsty wzywali[6]. Takie działania skutecznie wspierają działania „samotnych wilków", którzy, zainspirowani i bogatsi w informacje, prowadzą pojedyncze zamachy.

Eksperci twierdzą, że głównym powodem, dla którego działania wspierające występują częściej niż poważne cyberataki jest to, że terrorystom brakuje umiejętności i wiedzy, która pozwoliłaby im na spektakularne i wyrafinowane akcje. Jednak okoliczność ta może bardzo szybko ulec zmianie. Po pierwsze, w szeregi grup terrorystycznych rekrutuje się coraz więcej osób, które mogą posiadać zaawansowaną wiedzę technologiczną. Po drugie, dynamicznie rozwija się czarny rynek, na którym można zakupić

2 United Nations Counter-Terrorism Implementation Task Force, *Countering the use of the Internet for Terrorist Purposes - legal and technical aspects*, UN, 2011, s. 1.

3 C. A. Theohary, J. Rollins, *Terrorist Use of the Internet: Information Operations in Cyberspace*, Congressional Research Service 2011, s. 4.

4 United Nations Counter-Terrorism Implementation Task Force, *Countering the use of the Internet for Terrorist Purposes – legal and technical aspects*, UN, 2011, s. 20.

5 United Nations Counter-Terrorism Implementation Task Force, *Countering the use of the Internet for Terrorist Purposes – legal and technical aspects*, UN, 2011, s. 20.

6 Mirror, *ISIS 'kill list' names Brits among 4,000 terror targets it threatens to 'kill strongly' in "revenge for Muslims"* http://www.mirror.co.uk/news/world-news/isis-kill-list-names-brits-8271912.

narzędzia i informacje potrzebne do przeprowadzenia ataku. Wszystko to zwiększa zagrożenie, a państwa nie powinny zmniejszać czujności.

Zainteresowanie grup terrorystycznych bardziej zorganizowanym działaniem w cyberprzestrzeni wyraźnie wzrasta. Coraz częściej tworzą własne „oddziały" odpowiedzialne za działania prowadzone w sieci (np. Al–Qaeda i jej komórka *Qaedet al-Jihad al-Electroniyya*[7]). Pojawiają się także grupy hakerów nieoficjalnie wspierające ich działania. W ostatnim czasie powstało wiele formacji wspierających przede wszystkim tak zwane Państwo Islamskie (np. *Caliphate Cyber Army, Islamic State Hacking Division, United Cyber Caliphate*[8]). Nawołują one do prowadzenia *cyber–jihadu*.

Wielofrontowa walka z terrorystami

Wykorzystywanie cyberprzestrzeni przez terrorystów może stanowić jedno z największych zagrożeń dla międzynarodowego bezpieczeństwa w najbliższej przyszłości. Kiedy środek ciężkości przesunie się z kategorii działań wspierających na rzecz działań o strategicznym znaczeniu (np. poważne cyberataki na infrastrukturę krytyczną), konsekwencje mogą być dramatyczne. To scenariusz jeszcze groźniejszy niż potencjalne ofensywne wykorzystywanie cyberprzestrzeni przez podmioty państwowe. Aktorzy państwowi z natury są podmiotami podejmującymi bardziej racjonalne działania będące wynikiem kalkulacji kosztów i zysków. Terroryści nie mają nic do stracenia – nie obawiają się eskalacji konfliktu czy akcji odwetowych. Liczy się tylko spowodowanie jak największych strat. Nieobliczalność ich działań w połączeniu z brakiem zahamowań sprawia, że scenariusz cyberataków dokonywanych przez terrorystów jest jednym z najgorszych możliwych.

Zagrożenie dostrzegają już poszczególni gracze, którzy podejmują pierwsze zdecydowane reakcje. Potwierdza to choćby przykład Stanów Zjednoczonych, gdzie w kwietniu 2016 Sekretarz Obrony wydał rozkaz podjęcia przez USCYBERCOM cyfrowych działań ofensywnych mających uderzyć w tak zwane Państwo Islamskie[9]. Cyfrowa odpowiedź nie wyklucza także podejmowania działań konwencjonalnych. Wystarczy tylko wspomnieć, że jeden z głównych hakerów tak zwanego Państwa Islamskiego, Junaid Hussain, stał się trzecią najbardziej pożądaną osobą na liście celów podmiotów zwalczających tę grupę terrorystyczną i został zabity przy użyciu dronów[10].

Paradoksalnie, fakt, że terroryści coraz częściej wykorzystują cyberprzestrzeń, daje także nowe możliwości do walki z nimi. Służby odpowiedzialne za bezpieczeństwo w poszczególnych państwach łączą tradycyjne metody śledcze z nowymi typami działań właściwymi dla środowiska cyfrowego. Są w ten sposób w stanie przeciwdziałać grupom terrorystycznym, udaremniać ich plany oraz dokonywać zatrzymań w sposób, który nie był możliwy w przeszłości.

W obliczu niedawnych licznych ataków terrorystycznych, kolejne kraje wprowadzają lub modyfikują swoje rozwiązania prawne w celu wzmocnienia narzędzi pozwalających na walkę z terrorystami. Poza działaniami bardziej konwencjonalnymi, nowe strategie antyterrorystyczne kładą mocny nacisk na mechanizmy umożliwiające służbom bardziej efektywne postępowanie przeciwko terrorystom wykorzystującym cyberprzestrzeń. Trendowi temu towarzyszy wiele dyskusji na temat skuteczności wprowadzanych narzędzi i możliwych zagrożeń mających wpływ choćby na przestrzeganie praw człowieka (szczególnie prawa do prywatności).

Z uwagi na charakter i formę niniejszego dokumentu nie będziemy rozwijać tych wątków. Skupimy się natomiast na przedstawieniu przykładów działań, jakie podjęte zostały w ostatnim czasie w wybranych państwach. Pozwoli to zidentyfikować trendy panujące w tych krajach i może posłużyć jako materiał do dyskusji nad wprowadzanymi mechanizmami. W celu zapoznania się ze szczegółami dotyczącymi stosowania konkretnych narzędzi (warunkach, okolicznościach, itp.) zachęcamy do sięgnięcia do tekstu źródłowego. Poniżej przedstawiamy informacje w formie uproszczonej.

7 J. Scott, D. Spaniel, *The Anatomy of Cyber-Jihad*, Institute For Critical Infrastructure Technology, 2016, s. 6.

8 Więcej: J. Scott, D. Spaniel, *The Anatomy of Cyber-Jihad*, Institute For Critical Infrastructure Technology, 2016.

9 J. Scott, D. Spaniel, *The Anatomy of Cyber-Jihad*, Institute For Critical Infrastructure Technology, 2016, s. 23.

10 J. Scott, D. Spaniel, *The Anatomy of Cyber-Jihad*, Institute For Critical Infrastructure Technology, 2016, s. 15.

KRAJ	NARZĘDZIA PRAWNE ZAWARTE W DOKUMENCIE	DOKUMENT
Francja	1. Zobowiązanie operatorów telekomunikacyjnych, dostawców internetowych, a także wszystkich podmiotów publicznych oferujących dostęp do Internetu (jak np. kafejki internetowe) do przechowywania danych komunikacyjnych w okresie jednego roku od ich uzyskania. Przekazywanie tych danych do wyspecjalizowanych agencji rządowych. Powinny one zawierać informacje techniczne takie jak: ilość połączeń z elektronicznym serwisami komunikacyjnymi, wszystkie personalne dane subskrypcyjne, dane lokalizacyjne użytego sprzętu i numery, z którymi wykonywane były połączenia. 2. Autoryzacja wybranych służb wywiadowczych przez Ministra Spraw Wewnętrznych i Ministra Obrony Narodowej do uzyskania dostępu do zautomatyzowanych systemów danych (np. narodowego systemu dokumentów tożsamości, systemu zarządzającego dla osób nie będących obywatelami Francji).	• Law of Combating Terrorism and on Various Provisions Concerning Security and Borders Controls (2006-64 of 23 January 2006)
	3. Administracyjna blokada stron internetowych, które wspierają terroryzm lub nawołują do dżihadu. Publiczne serwisy komunikacyjne mogą zostać zablokowane nakazem sędziego na wniosek podmiotów publicznych lub prywatnych, jeśli wyraźnie reprezentują treści niezgodne z prawem. 4. Zobowiązanie dostawców usług internetowych i administratorów sieci do zgłaszania treści o charakterze terrorystycznym. 5. Autoryzacja policji sądowej do uzyskania dostępu do danych zlokalizowanych w innych systemach na terytorium Francji, na potrzeby prowadzonych dochodzeń i przy użyciu systemów dostępnych policji lub żandarmerii.	• Law Strengthening Provisions on the Fight Against Terrorism (2014-1353 of 13 November 2014)
	6. Stworzenie ram prawnych, w zakresie których służby wywiadowcze mają przy użyciu zasobów technicznych dostęp do danych niezbędnych do prowadzenia działań wywiadowczych. Opracowanie systemu przechowywania danych szeregującego informacje pod względem sposobu, w jaki zostały pozyskane (np. licząc od dnia ich uzyskania, zniszczenie zebranych danych następuje po: 30 dniach dla przejętej korespondencji i rozmów, 5 latach dla połączeń transmisji danych, 90 dni dla nagrań dźwiękowych, danych lokalizacyjnych i obrazów wideo, a także nie więcej niż 6 lat dla informacji szyfrowanych). 7. Zobowiązanie dostawców serwisów internetowych do instalacji urządzeń do automatycznego analizowania danych (tzw. „blackbox") w celu monitorowania i wykrywania zachowań budzących podejrzenia - sposób działania tej metody jest niejawny. Dostawcy serwisów internetowych są także zobowiązani do zagwarantowania służbom wywiadowczym dostępu do metadanych, które wyodrębniane są od treści przez danego dostawcę (tego typu dane analizowane są przez 60 dni, zachowywane lub usuwane, w zależności od przypadku potwierdzenia zagrożenia terrorystycznego).	• Law on Intelligence (2015-912 of 24 July 2015)
	8. Autoryzacja służb wywiadowczych do legalnego zastosowania obserwacji poza granicami Francji:przepis ten odnosi się zarówno do treści jak i danych komunikacji w przypadku, gdy jedna ze stron - adresat lub nadawca - znajduje się poza terytorium Francji.Premier lub jeden z jego/jej delegatów musi autoryzować tego typu monitoring komunikacji.	• Law on Surveillance of International Electronic Communications (2015-1556 of 30 November 2015)
	9. Zintegrowanie wszystkich służb wywiadowczych i stworzenie skonsolidowanej bazy danych na użytek podmiotów odpowiedzialnych za walkę z terroryzmem.	• Propositions Made by the Commission for Enquiry on the Means Undertaken by the State to Efficiently Fight Terrorism, July 2016
Holandia	1. Autoryzacja zespołu specjalistów w ramach struktur policyjnych do zwalczania treści dżihadystycznych online; publikowanie systematycznie aktualizowanej listy dżihadystów. Autoryzacja służb porządkowych do nakładania sankcji na firmy internetowe (po uprzednim ostrzeżeniu), które umożliwiają zdefiniowanym organizacjom terrorystycznym rozpowszechnianie treści dżihadystycznych. 2. Witryny internetowe, które propagują dyskryminacje, przemoc lub zachęcają do nienawiści zostają usuwane. 3. Stworzenie obywatelskiej gorącej linii, dzięki której możliwe jest zgłoszenie pojawienia się treści dżihadystycznych (gloryfikujących przemoc, nakłaniających do nienawiści i czynów terrorystycznych) pojawiających się w Internecie lub mediach społecznościowych.	• The Netherlands Comprehensive Action Programme to Combat Jihadism – 2014

KRAJ	NARZĘDZIA PRAWNE ZAWARTE W DOKUMENCIE	DOKUMENT
Holandia	4. Autoryzacja odpowiednich służb (w wyjątkowych okolicznościach) do prowadzenia obserwacji - nagrywania, instalowania urządzeń służących do obserwacji, rejestracji i śledzenia, a także ustalania położenia i penetrowania systemów bezpieczeństwa, odkodowywania danych i kopiowania danych zapisanych lub przetwarzanych w zautomatyzowany sposób, zakładania podsłuchu, odbierana, nagrywania i monitorowania w sposób bezpośredni każdej formy – rozmowy, telekomunikacji lub danych. 5. Autoryzacja określonych służb do odbierania i nagrywania określonej i nieokreślonej komunikacji, która odbywa się w sposób bezprzewodowy (np. telefonia komórkowa, łączność satelitarna) wraz z telekomunikacją przychodzącą z innego kraju, wychodzącą do innego kraju i monitorowanie tej komunikacji. 6. Autoryzacja określonych służb (w wyjątkowych okolicznościach) do zwrócenia się do dostawców publicznych sieci telekomunikacyjnych i publicznych serwisów telekomunikacyjnych z prośbą o dostarczenie informacji związanych z ruchem, który już miał miejsce lub dopiero zajdzie za pośrednictwem publicznych sieci telekomunikacyjnych. Przekazanie tych informacji jest na mocy prawa obowiązkowe.	• Intelligence and Security Services Act - 2002
	7. Autoryzacja prokuratora do stwierdzenia, czy dane zdobyte w czasie prowadzenia obserwacji (przy użyciu nagrywających urządzeń tech-nicznych; nagrywanie komunikacji poufnej, nagrywanie komunikacji lub zwrócenie się z prośbą o dostęp do danych użytkownika i rejestru danych ruchu telekomunikacyjnego adekwatnych dla tego użytkownika) mogą zostać użyte w czasie śledztwa.	• Act amending the Code of Criminal Procedure and certain other laws to regulate powers to demand access to data (Access to Data «General Powers Act») – 2005
	8. Wyposażenie odpowiednich służb w specjalne kompetencje dochodzeniowe jak: obserwacja, infiltracja, nagrywania i pseudo-zakupu (kompetencje te mogą zostać użyte tylko w przypadku, gdy istnieje realne zagrożenie, że planowany jest atak o znamionach terrorystycznych).	• Investigation and Prosecution of Terrorist Offences (Extension of Powers) Act) – 2007
Wielka Brytania	1. Zdefiniowanie przestępstw, na podstawie których może zostać postawiony zarzut osobom, które przy użyciu Internetu wspierały działania o znamionach terrorystycznych: a. Przy użyciu Internetu zapewnianie, odbieranie lub zapraszanie do przejścia (lub przedsięwzięcie samemu) treningu w zakresie tworzenia lub wykorzystywania broni palnej, materiałów radioaktywnych lub pokrewnych rodzajów broni, materiałów wybuchowych lub broni chemicznej, biologicznej lub nuklearnej do czynów o znamionach terrorystycznych. b. Posiadanie artykułów, które w uzasadniony sposób wzbudzają podejrzenie, bądź zostały uznane za bezpośrednio związane ze zleceniem,przygotowaniem i nakłanianiem do czynu o znamionach terrorystycznych. c. Nabywanie, posiadanie lub tworzenie nagrań informacji (z włączeniem zdjęć i nagrań w formie elektronicznej), które w sposób wysoce prawdopodobny mogą być użyteczne przez osobę, która przygotowuje lub ma zamiar przeprowadzić atak terrorystyczny, a także posiadanie jakichkolwiek dokumentów lub informacji tego typu. Taki dokument, będąc użytecznym dla osoby fizycznej bez uzasadnionej przyczyny, może być dla władz podstawą do interwencji, w przypadku gdy władze nie posiadają innych dowodów na zaangażowanie podejrzanego w aktywność związaną z działalnością terrorystyczną. d. Podżeganie do popełnienia aktu o znamionach terrorystycznych na terytorium Wielkiej Brytanii lub poza nim (np. prowadzenie witryn lub forów internetowych używanych do publikowania materiałów, które nakłaniają do zbrodni, jak np. w Iraku).	• Terrorism Act 2000 • United Nations Counter-Terrorism Implementation Task Force, New York 2012.
	2. Stworzenie ram prawnych regulujących nadzór prowadzony przez agencje rządowe, pozwalających na kontrolę komunikacji (np. przechwytywanie połączeń telefonicznych lub dostęp do korespondencji e-mailowej) i metadanych (informacji dotyczących komunikacji, ale nie jej treści).	• Regulation of Investigatory Powers Acts 2000 (RIPA) • "The Use of the Internet for Terrorist Purposes", UNODC, United Nations, New York, 2012 • Summary of surveillance powers under the Regulation of Investigatory Powers Act", National Council for Civil Liberties.

KRAJ	NARZĘDZIA PRAWNE ZAWARTE W DOKUMENCIE	DOKUMENT
Wielka Brytania	3. Stworzenie ram definicyjnych dla przestępstw, które konkretnie związane są z użyciem Internetu i w sposób bezpośredni mogą zachęcać lub wspomóc zlecenie aktu terrorystycznego: a. Publikowanie komunikatów, które w sposób pośredni lub bezpośredni nakłaniają społeczność do przygotowania, prowokowania lub popełnienia aktu terrorystycznego(z włączeniem gloryfikowania aktów terrorystycznych). b. Rozpowszechnianie publikacji terrorystycznych, które wspierają nakłanianie do popełnienia czynów o znamionach terrorystycznych. 4. Zapewnienie policji możliwości do wystosowania oficjalnego wezwania osobie (np. webmasterowi) powiązanej z treściami terrorystycznymi w Internecie (komunikaty, artykuły lub nagrania). Treści te powinny zostać usunięte z przestrzeni publicznej w wyniku ich interwencji. 5. Poszerzenie uprawnień śledczych poprzez zdefiniowanie jako przestępstwa odmówienia wezwania do przedłożenia klucza szyfrowania. Służby muszą upewnić się, że podejrzany nie ukrywa danych przy użyciu wielu kluczy dla innych zbiorów danych (np. do kodowania dysku twardego, używając dwóch haseł – jednego dającego dostęp do czystych zbiorów danych i drugiego do danych inkryminujących). W związku z tym, analiza danych materiałów powinna skupić się także na zbadaniu czy istnieją jakieś „brakujące elementy" danych.	• Terrorism Act 2006 • United Nations Counter-Terrorism Implementation TaskForce, New York 2012.
	6. Na podstawie jasnych i wzmocnionych regulacji prawnych, zobowiązanie dostawców usług komunikacyjnych do przechowywania danych na potrzeby śledcze i przeciwdziałania przestępczości. 7. Ograniczenie dostępu do treści danych komunikacji eksterytorialnej, stosując wymóg uzyskania zgodny na przejęcie danej komunikacji. Zgoda ta wydana musi być przez Sekretarza Stanu. 8. Zapewnienie, że definicja „serwisów telekomunikacyjnych" obejmuje także serwisy internetowe i wymaganie dodatkowego regularnego raportowania od Komisarza ds. przechwytywanych informacji (Interception of Communications Commissioner).	• Data Retention and Investigatory Powers Act 2014
	9. Prawne wzmocnienie kompetencji policji i służb wywiadowczych w odpowiedzi na wzrastające zagrożenie związane z sytuacją w Syrii i Iraku, a także działania prewencyjne mające na celu zmniejszenie radykalizacji wśród osób fizycznych. 10. Nowelizacja Ustawy o przechowywaniu danych i uprawnieniach dochodzeniowych z 2014 r. (Data Retention and Investigatory Power-sAct 2014) zawierającej wzmocnienie uprawnień dochodzeniowych służb w poważnych sprawach kryminalnych i terrorystycznych: a. Sekretarz Stanu na mocy prawa może zwrócić się z prośbą do dostawców serwisów komunikacyjnych o przechowywanie dodatkowych danych komunikacyjnych, które pozwolą odpowiednim służbom na połączenie wyjątkowych cech publicznych adresów protokołu internetowego z konkretną osobą (lub urządzeniem) w dowolnym momencie. b. W danych komunikacyjnych nie chodzi o ich treść, a raczej o dane niezbędne do zidentyfikowania nadawcy lub odbiorcy komunikacji, czas jej trwania, typ, metodę lub schemat, a także użyte systemy telekomunikacyjne lub lokalizację osoby komunikującej się.	• Counter-Terrorism and Security Act 2015
	11. Zebranie wszystkich uprawnień dotyczących uzyskiwania komunikacji elektronicznej i stworzenie na ich podstawie jednej kompleksowej ustawy. 12. Wzmocnienie nadzoru nad nakazami wydawanymi przez Sekretarza Stanu, które przed wejściem w życie muszą być zaakceptowane przez niezależnego Komisarza Sądowego (Judicial Commissioner), poprzez dodatkowe zabezpieczenia w kwestii nabywania, używania i przechowywania danych elektronicznych.	• Draft Investigatory Powers Bill, November 2015
Izrael[11]	1. Autoryzacja odpowiednich służb specjalnych do wydania instrukcji licencjobiorcom telekomunikacyjnym(z poszanowaniem sprzętu, wykonywania i dostarczania usług telekomunikacyjnych i dostosowaniem technologii w sposób kompatybilny do sprzętu telekomunikacyjnego), a także zapewnienie służbom dostępu do sprzętu i wyposażenie w skali niezbędnej do wykonywania zadań.	• Telecommunications Act (Telephone and Broadcast) – 1982

11 Autor odwołuje się jedynie do prawa obowiązującego na terytorium Państwa Izrael.

KRAJ	NARZĘDZIA PRAWNE ZAWARTE W DOKUMENCIE	DOKUMENT
	2. Autoryzacja odpowiednich służb do zbierania dowodów cyfrowych w Internecie, w przypadku spraw kryminalnych oraz tych o znamionach aktu terrorystycznego. 3. Zezwolenie odpowiednim organom śledczym na wnioskowanie(w trybie sądowym lub administracyjnym) o uzyskanie zgody do pozy-skania danych przesyłanych pomiędzy komputerami.	• Computers Act – 1995
	4. Autoryzacja Premiera do ustanowienia zasad wykonywania zadań określonych w ustawie przez służby specjalne (GSS), na podstawie których definiowane są kategorie danych znalezionych w bazie licencjobiorcy,oraz zobowiązanie licencjobiorcy do dostarczenia wskazanych kategorii danych służbom. 5. Zezwalanie na użycie danych znalezionych w bazach danych (patrz pkt. 4) za pozwoleniem, które definiuje kategorię danych i jest ograniczone do 6 miesięcy z uwzględnieniem możliwości przedłużenia tego okresu przez szefa służb specjalnych. 6. Zezwolenie szefowi wydziału śledczego i służbom wywiadowczym do uzyskania nie zawierających treści danych od operatorów sieci stacjonarnych i komórkowych, a także dostawców Internetu. 7. Autoryzacja Policji (starszych oficerów) do nałożenia obowiązku na operatorów telekomunikacyjnych, przekazywania zaktualizowanych plików zawierających: szczegóły pozwalające na identyfikacje wszystkich subskrybentów (w tym: szczegółowe informacje identyfikujące urządzenia i ich części),lokalizacje anten (w tym: szczegółowe informacje identyfikujące ich zasięg). 8. Utworzenie bazy danych ze wszystkimi zbieranymi informacjami (w tym: numery telefonów, także niezarejestrowane, nazwiska użytkowników telefonów komórkowych, numery seryjne telefonów komórkowych, map pozwalających na zlokalizowanie anten). 9. Zezwolenie na dostęp do danych komunikacyjnych w przypadku wykroczenia.	• General Security Service Act – 2002 • Criminal Procedure (Enforcement Powers – Communication Data) Law – 2007
	10. Zmiana polegająca na poszerzeniu definicji organizacji terrorystycznej, strefy infrastruktury terrorystycznej (możliwość rządu do egzekwowania prawa na obszarach poza granicami kraju) oraz aktu terrorystycznego. 11. Zidentyfikowania jako czyn zabroniony używania bądź przekazywania własności w celu wspierania, promowania lub finansowania przygotowań do czynu o znamionach terrorystycznych, a także zapewnienie rekompensaty osobie, która popełniła bądź planowała popełnić czyn o znamionach terrorystycznych.	• Counterterrorism Act – 2016
Polska	1. W celu rozpoznania, zapobiegania lub zwalczania przestępstw o charakterze terrorystycznym Szef Agencji Bezpieczeństwa Wewnętrznego (ABW) może zarządzić wobec osoby niebędącej obywatelem Polski, w stosunku do której istnieje obawa co do możliwości prowadzenia przez nią działalności terrorystycznej, prowadzenie czynności polegających między innymi na niejawnym: a. uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych b. uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej c. uzyskiwaniu i utrwalaniu danych zawartych na informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych. Czynności te można prowadzić do 3 miesięcy (istnieje możliwość przedłużenia tych działań na określonych warunkach). 2. W przypadku zagrożenia lub wystąpienia zdarzenia o charakterze terrorystycznym dotyczącym systemów teleinformatycznych organów administracji publicznej i systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, Ustawa wprowadza możliwość wdrażania czterech stopni alarmowych dla cyberprzestrzeni. Są one podstawą do realizacji określonych działań koordynacyjnych i związanych z zapewnianiem bezpieczeństwa.	• Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych

KRAJ	NARZĘDZIA PRAWNE ZAWARTE W DOKUMENCIE	DOKUMENT
Polska	3. W celu wykrywania, zapobiegania i przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym dotyczących: • istotnych z punktu widzenia systemów teleinformatycznych organów administracji publicznej, • sieci teleinformatycznych objętych wykazem systemów infrastruktury krytycznej, • systemów teleinformatycznych właścicieli, posiadaczy infrastruktury krytycznej lub danych przetwarzanych w tych systemach, 4. ABW może przeprowadzić tak zwaną ocenę bezpieczeństwa. Polega ona na przeprowadzaniu testów bezpieczeństwa systemu teleinformatycznego w celu identyfikacji podatności. W celu określenia podatności Agencja może wytwarzać lub pozyskiwać urządzenia i programy komputerowe dedykowane do tego celu. Używając ich może uzyskać dostęp do całości lub części systemu teleinformatycznego. 5. W przypadku pozyskania informacji o wystąpieniu zdarzenia terrorystycznego dotyczącego systemów i danych opisanych w punkcie 3, lub w celu zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze, szef ABW może zażądać przedstawienia informacji o budowie, funkcjonowaniu systemów teleinformatycznych, w tym: haseł komputerowych, kodów dostępu, i innych danych umożliwiających dostęp do systemu. 6. Ustawa wprowadza tak zwaną blokadę dostępności, czyli możliwość żądania przez sąd blokowania dostępności w systemie teleinformatycznym określonych danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym. 7. Szef ABW prowadzi rejestr zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych zawierające m.in. identyfikacje źródła zdarzenia naruszającego bezpieczeństwo systemu, opis stwierdzonego zdarzenia, sposób działania podmiotu powodującego naruszenie bezpieczeństwa, opis szkód w systemie. Na podstawie tych informacji ABW przeprowadza analizę i wydaje rekomendacje, które winny być uwzględnione przez wskazane podmioty.	

Analizując powyższe akty prawne i wybrane ich zapisy, widać wyraźnie, że postępujące wykorzystanie cyberprzestrzeni dla celów terrorystycznych prowadzi do wprowadzania nowych, coraz bardziej zaawansowanych mechanizmów mających na celu przeciwdziałanie temu procederowi. Potrzebna jest debata nad ich skutecznością, rozmowa na temat najlepszych praktyk w zakresie implementacji poszczególnych instrumentów, a także pochylenie się nad kolejnymi krokami. Ten krótki brief ma na celu kontrybucję do owej dyskusji.

INSTYTUT KOŚCIUSZKI

Instytut Kościuszki jest niezależnym, pozarządowym instytutem naukowo-badawczym (ThinkTank) o charakterze non profit, założonym w 2000 r. Misją Instytutu Kościuszki jest działanie na rzecz społeczno-gospodarczego rozwoju i bezpieczeństwa Polski jako aktywnego członka Unii Europejskiej oraz partnera sojuszu euroatlantyckiego. Instytut Kościuszki pragnie być liderem pozytywnych przemian, tworzyć i przekazywać najlepsze rozwiązania, również na rzecz sąsiadujących krajów budujących państwo prawa, społeczeństwo obywatelskie i gospodarkę wolnorynkową.

Instytut Kościuszki jest organizatorem Europejskiego Forum Cyberbezpieczeństwa oraz Polskiego Forum Cyberbezpieczeństwa – pierwszych w Polsce oraz jednych z nielicznych w Europie corocznych konferencji poświęconych strategicznym wyzwaniom płynącym z cyberprzestrzeni i dotyczących cyberbezpieczeństwa. Więcej: http://cybersecforum.eu/.

Instytut Kościuszki jest wydawcą European Cybersecurity Journal (ECJ). ECJ to anglojęzyczny kwartalnik ekspercki poświęcony cyberbezpieczeństwu. Zawiera artykuły wiodących analityków i liderów opinii, ekskluzywne wywiady z decydentami oraz monitoring regulacji dotyczących kluczowych aspektów związanych z cyberprzestrzenią. Więcej: http://cybersecforum.eu/czym-jest-ecj/.

Biuro w Krakowie: ul. Feldmana 4/9, 31-130 Kraków, Polska, tel.: +48 12 632 97 24, www.ik.org.pl, e-mail: ik@ik.org.pl.

Dalsze informacje i komentarze: Joanna Świątkowska – joanna.swiatkowska@ik.org.pl – tel. +48 515 174 389.