dr hab. Tomasz Aleksandrowicz

ROZDZIAŁ 1

Zagrożenia terrorystyczne – 10 minionych lat

10 lat w rozwoju zagrożeń terrorystycznych to cała epoka. Zmiany jakie miały miejsce w ostatniej dekadzie potwierdzają starą tezę, że terroryzm jest zjawiskiem podlegającym dynamicznym zmianom, a tak naprawdę istnieje – jak to ujął Walter Lacqueur – wiele różnych terroryzmów.

Skalę zagrożeń terrorystycznych w ujęciu statystycznym przedstawia tabela 1.

Tabela 1.1. Skala zagrożeń terrorystycznych za lata 2005–2013 w ujęciu statystycznym

Rok	Liczba ataków	Ofiary śmiertelne	Ranni	Ofiary ogółem (łącznie z uprowadzonymi)
2005	11 157	14 560	24 845	74 280
2006	14 546	20 468	36 386	74 709
2007	14 415	22 720	44 103	71 803
2008	11 663	15 709	33 901	54 290
2009	10 968	15 311	32 660	58 720
2010	11 641	13 193	30 684	49 928
2011	10 283	12 533	25 903	43 990
2012	6 711	11 098	21 652	34 033
2013	9 707	17 891	32 577	53 458

Źródło: Kolejne wydania *Country Report on Terrorism* 2009, 2010, 2011, 2012, 2013. United States Department of State, Office of the Coordinator for Counterterrorism, Wash., DC. http://www.state.gov/j/ct/rls/crt/index.htm, dostęp 14.04.2014.

Al Kaida u szczytu potęgi

Przyjmując jako subiektywną cezurę czasową naszych rozważań czerwiec 2005 r. (wszak wtedy właśnie powstało Centrum Badań nad Terroryzmem Collegium Civitas!) nie sposób nie zauważyć, że omawiana dekada rozpoczęła się jednym z groźniejszych zamachów Al Kaidy w londyńskim metrze i autobusie wybuchły ładunki wybuchowe.

Al Kaida wydawała się być wówczas u szczytu swojej potęgi, udowadniając to zamachami na World Trade Center, w Madrycie i właśnie w Londynie. W porównaniu z wiekiem XX – mieliśmy do czynienia z zupełnie nowa jakością, przeciwnikiem znacznie trudniejszym do zwalczania i znacznie bardziej niebezpiecznym. Nie pretendując do hierarchizacji czynników różnicujących należy wskazać następujące elementy: motywację, środowisko działania i strukturę[1].

Motywacja. Biorąc pod uwagę podstawowe źródło zagrożeń, jakim jest islamski fundamentalizm, należy podkreślić niezwykle silną motywację sprawców. Wynika ona ze spójnej konstrukcji ideologiczno-religijnej, zasadzającej się na przekonaniu o absolutnej wyższości moralnej i racji uzasadniającej odrzucenie podstawowych norm współżycia społecznego. To przekonanie o wyższości moralnej jest na tyle silne, iż dopuszcza nie tylko zabijanie niewinnych, przypadkowych ofiar, lecz także dążenie do multiplikacji ofiar. Z drugiej strony, służba w imię tak rozumianej idei pociąga za sobą nagrodę w postaci transcendentalnej (pośmiertna nagroda w postaci życia wiecznego w raju), co pociąga za sobą nie tyle odrzucenie strachu przed śmiercią, co wręcz przezwyciężenie nakazów i zakazów wynikających z instynktu samozachowawczego. To właśnie należy uznać za podstawową przyczynę pojawienia się w takiej skali zamachów samobójczych, co stanowiło samo w sobie radykalną zmianę. Dotychczas śmierć sprawcy aktu terrorystycznego, jego zranienie czy pochwycenie przez siły policyjne było naturalnie uwzględniane podczas konstruowania planów zamachu; zakładały one taką możliwość, bowiem ryzyka nie można całkowicie wyeliminować, jednak dążono do jego minimalizacji. Planowanie zamachów samobójczych oparte jest na zupełnie innej logice: śmierć sprawcy (sprawców) jest immanentną częścią planu, *conditio sine qua non* jego powodzenia, a więc zachowanie życia przez sprawcę jest tożsame z jego porażką[2].

Tak silna motywacja i determinacja w osiąganiu wyznaczonych celów warunkuje brak możliwości kompromisu i negocjacji. Z wrogiem rozumianym

---

[1] Zob.: T. Aleksandrowicz, *Cezura 11 września*, [w:] *Bezpieczeństwo w XXI wieku. Asymetryczny świat*, K. Loedel, P. Piasecka, T. Aleksandrowicz (red. nauk.), Warszawa 2011, s. 61 i nast.

[2] Zob.: T. Aleksandrowicz, *Terroryzm międzynarodowy*, Warszawa 2008, s. 37.

w kategoriach absolutystycznych (Wielkim Szatanem) nie wolno iść na żadne kompromisy i nie wolno niczego negocjować, byłoby to jawną zdradą ideałów leżących u podstaw motywacji islamskich fundamentalistów i osób, które uznają ich przekonania za swoje.

Z punktu widzenia strategii zwalczania i przeciwdziałania zagrożeniom terrorystycznym kwestia tak silnej motywacji terrorystów pociągnęła za sobą dwie konsekwencje. Po pierwsze, sytuacja taka oznaczała koniec wszelkich strategii opartych na odstraszaniu potencjalnych sprawców, na co zwraca uwagę John Lewis Gaddis w swojej analizie polityki bezpieczeństwa narodowego Stanów Zjednoczonych, będącej *de facto* intelektualną biografią George'a Kennana[3]. Po drugie, oznaczało to zmianę w całym systemie reagowania kryzysowego, który musi być przygotowany na wielką liczbę ofiar i zakłócenia w funkcjonowaniu aglomeracji miejskich w przypadku udanego zamachu terrorystycznego.

Środowisko działania. Terroryści zawsze wykorzystywali cechy otoczenia społecznego, w jakim przyszło im działać, w tym także dostępne technologie – czy to w charakterze narzędzia, czy celu zamachu. Tak jak w XIX wieku nie dokonywano uprowadzeń samolotów pasażerskich, tak w wieku XXI nikt nie porywa dyliżansów; brak jest danych o zamachach dokonywanych w XIX wieku za pomocą semteksu, trudno też znaleźć przykład aktu indywidualnego terroryzmu dokonanego w dzisiejszych czasach za pomocą sztyletu. Są to stwierdzenia oczywiste, jednakże trudno nie zauważyć, iż rozwój cywilizacyjny, z jakim mamy do czynienia w ciągu ostatnich kilkudziesięciu lat został przez organizacje terrorystyczne wykorzystany niemal perfekcyjnie, co stworzyło – jeśli chodzi o zagrożenia – nowa jakość.

Najbardziej spektakularnym czynnikiem określającym kształt tworzącego się nowego ładu międzynarodowego wydaje się być status państwa narodowego jako aktora stosunków międzynarodowych. Mamy tu do czynienia z radykalną zmianą, jaka dokonała się w przeciągu ostatniego półwiecza, przy czym szczególnie istotne okazał się okres po 1990 r.

Przede wszystkim należy zauważyć, że państwo, które jeszcze 50 lat temu było podstawowym i najsilniejszym podmiotem stosunków międzynarodowych w nieuchronny sposób traci swoją uprzywilejowaną pozycję. Z jednej strony, pojawili się znaczący konkurenci zarówno w postaci podmiotów prawa międzynarodowego (jak np. organizacje międzynarodowe) czy prawa prywatnego (koncerny transnarodowe), ale też podmioty funkcjonujące nielegalnie (organizacje terrorystyczne, zorganizowane grupy przestępcze). Poszczególne państwa posiadają

[3] J.L. Gaddis, *Strategie powstrzymywania*, Warszawa 2007, zwł. rozdz. XII zawierający analizę strategii powstrzymywania po zakończeniu zimnej wojny.

znikomy (o ile jakikolwiek) wpływ na ich działalność, nie mówiąc już o zdolności do tworzenia samodzielnie obowiązujących reguł postępowania.

Z drugiej strony, procesy globalizacyjne i integracyjne spowodowały, że większość decyzji o charakterze strategicznym zapada na szczeblu ponadnarodowym. Następuje także prywatyzacja poszczególnych funkcji państwa, w tym również w zakresie bezpieczeństwa i legalnego użycia siły, a samo państwo coraz częściej występuje w roli podmiotu prawa cywilnego – kontrahenta, a nawet stronę w procesie cywilnym czy arbitrażowym, przy czym drugą stroną jest podmiot niepaństwowy.

Na wskazane powyżej zmiany nakłada się powstawanie nowej formy funkcjonowania społeczeństw – powstawanie społeczeństwa informacyjnego. Czym jest społeczeństwo informacyjne? Zgodnie z definicją proponowaną przez P. Sienkiewicza jest to „taki system społeczny, ukształtowany w procesie modernizacji, w którym systemy informacyjne i zasoby informacyjne determinują społeczną strukturę zatrudnienia, wzrost zamożności społeczeństwa (dochodu narodowego) oraz stanowią podstawę orientacji cywilizacyjnej" Wśród cech społeczeństwa informacyjnego przywołany Autor wymienia m.in. wysokie tempo rozwoju sieci komunikacji społecznej oraz modernizacji struktury informacyjnej; bezpieczeństwo informacyjne jako istotny element bezpieczeństwa społeczeństwa; wysoki wpływ IT i mediów elektronicznych na zmiany zachowań społecznych, wskazując przy tym na rozszerzenie potencjalnego i realnego dostępu jednostek (określonych grup) do zasobów informacyjnych oraz potencjalne i realne możliwości komunikowania się „każdego z każdym" w dowolnym czasie. Nie wdając się w tym miejscu w szczegółową analizę tego zjawiska poprzestańmy na stwierdzeniu, iż charakteryzuje się ono wzrostem znaczenia zasobów informacyjnych i rozszerzeniem zakresu potencjalnego i realnego dostępu jednostek do nich oraz radykalnymi zmianami sieci komunikacyjnych, polegających na dominacji kontaktów pośrednich nad bezpośrednimi oraz potencjalnymi i realnymi możliwościami komunikacji[4].

Struktura. Al Kaida przybrała organizacyjną postać sieci. W praktyce oznacza to nie tylko odejście od klasycznej struktury hierarchicznej, ale przede wszystkim brak jednoznacznej, stałej lokalizacji, bezterytorialność. Ulrich Beck nazywa takie grupy terrorystyczne *nowymi aktorami globalnymi, pozbawionymi korzeni terytorialnych i narodowych pozarządowymi organizacjami przemocy*[5]. Jedną z istotnych

---

[4] Zob.: P. Sienkiewicz, *Teoria rozwoju społeczeństwa informacyjnego*, http://winntbg.agh.edu.pl/skrypty2/0096/027-040, s. 508–509.

[5] U. Beck, *Władza i przeciwwładza w epoce globalnej. Nowa ekonomia polityki światowej*, Wydawnictwo Naukowe Scholar, Warszawa 2005, s. 31 i nast.

konsekwencji takiego stanu rzeczy jest fakt, iż organizacje sieciowe nie muszą się opierać na państwach – sponsorach, stanowiąc byty w miarę autonomiczne i samodzielne, są zatem mniej podatne na np. sankcje ekonomiczne.

Warto w tym kontekście zauważyć, iż sieciowy model organizacji został opisany jeszcze w latach 70. jako SPIN – *Segmented, Polycentric, Ideologically Integrated Network*. Struktura takich sieci jest amorficzna, a sposób ich działania (w tym – ataku na określone cele) się określa się mianem *swarming* (rojenie się, atak roju)[6].

W literaturze przedmiotu wskazuje się, iż struktury sieciowe charakteryzują się trzema zasadniczymi cechami: działania i koordynacja elementów systemu nie są formalnie skodyfikowane przez relacje hierarchiczne, lecz wyłaniają się i zmieniają w zależności od konkretnego zadania; sieci posiadają dynamicznie tworzone i zmieniające się połączenia obustronne, wykraczające poza daną organizację i swobodnie przekraczające granice państw, zacierając w ten sposób granice pomiędzy poszczególnymi strukturami autonomicznymi; więzy zewnętrzne i wewnętrzne nie stanowią skutku decyzji biurokratycznych, lecz efekt wspólnych norm, wartości, interesów i wzajemnego zaufania (np. wspólny przeciwnik, ideologia, pochodzenie etniczne, religia)[7].

Sieciowość organizacji wiąże się ściśle z efektywnym wykorzystywaniem produktów najnowszej technologii, szczególnie w sferze komunikacji i przekazu informacji. Z tego punktu widzenia *nowy terroryzm* wydaje się być wręcz produktem ery informatycznej. Można wręcz zaryzykować stwierdzenie, iż funkcjonowanie Al Kaidy w jej dzisiejszej postaci było przed gwałtownym rozwojem technologii informatycznych po prostu niemożliwe. Analizujący fenomen sieciowości Manuel Castells podkreśla, iż sieci społeczne są tak stare jak ludzkość, dopiero jednak nowy paradygmat technologiczny pozwolił na ich pełny rozwój i wykorzystanie tkwiących w nich możliwości[8]. Pod tym względem fenomen Al Kaidy można określić jako połączenie sieci typu SPIN z możliwościami stwarzanymi przez internet i telefon komórkowy[9].

---

[6] Zob.: G. Luter, W. Hine, *People, Power, Change: Movements of Social Transformation*, The BobbsMerrill Co., Inc., New York 1970, passim. Por.: J. Arguilla, D. Ronfeldt, *The Advent of Netwar*, [w:] *Networks and Netwars. The Future of Terror, Crime and Militancy*, J. Arguilla, D. Ronfeldt (red.), Santa Monica 2001, s. 8–10.

[7] Zob.: B. Bolechów, *Sieci przeciwko hierarchiom – wyzwanie dla suwerenności państw*, [w:] *Suwerenność państwa we współczesnych stosunkach międzynarodowych*, Z. Leszczyński, S. Sadowski (red.), Warszawa 2005, s. 162 i nast.

[8] Manuel Castells nazywa np. zapatystów „pierwszym informacyjnym ruchem partyzanckim". Zob.: *idem*, *Siła tożsamości*, Wydawnictwo Naukowe PWN, Warszawa 2008, s. 85.

[9] Por.: T. Aleksandrowicz, *Sieć jako forma organizacji terrorystycznej*, [w:] *Cyberterroryzm. Nowe wyzwania XXI wieku*, T. Jemioło, J. Kisielnicki, K. Rajchel (red. nauk.), Warszawa 2009, s. 273 i nast.

Po pierwsze, trzeba zwrócić uwagę na te cechy internetu, które powodują niezwykłą użyteczność tego narzędzia dla terrorystów. Należy do nich przede wszystkim stosunkowo łatwy i tani dostęp, mała kontrola ze strony rządów i anonimowość w komunikacji internetowej, potencjalnie nieograniczony krąg odbiorców i możliwość wykorzystywania platform multimedialnych, możność zachowania tajemnicy treści przekazu (szyfrowanie, steganografia etc.), zdolność do wywierania wpływu na pozostałe media korzystające z internetu jako źródła informacji oraz tzw. *operational flexibility*, a więc możliwość do przenoszenia stron internetowych z serwera na serwer, wykorzystywanie czatów, serwerów poczty elektronicznej etc.[10].

Po wtóre, istotna w tym kontekście staje się analiza celów, w jakich organizacje terrorystyczne wykorzystują internet. Nie sposób bowiem nie zauważyć, iż w rękach terrorystów internet stał się już sprawnym, efektywnym i tanim wielofunkcyjnym narzędziem[11].

Poza podstawową funkcją, jaką jest wymiana informacji, terroryści traktują internet jako środek do propagowania swoich idei i rekrutacji nowych zwolenników, a także podtrzymywania zapału i poparcia już pozyskanych. Internet spełnia w tym przypadku funkcję socjalizacyjną, stwarzając możliwość partycypacji, udziału we wspólnocie i stosunkowo łatwego przyłączenia się do niej[12]. Poprzez sieć www prowadzone są także akcje zbierania funduszy, które częstokroć przybierają postać wypełniania religijnego obowiązku każdego muzułmanina, tj. *zakat* – swoistego podatku dobroczynnego przeznaczonego dla biednych.

Internet stał się zatem nowym narzędziem w wojnie psychologicznej (informacyjnej). Pod wieloma względami sieć staje się bardziej efektywnym środkiem przekazu, niż tradycyjna prasa czy nawet telewizja. Z jednej strony, sieć zapewnia dostęp do najbardziej wykształconej, a więc opiniotwórczej części odbiorców, z drugiej – przekaz internetowy zapewnia możliwość samodzielnej i nieskrępowanej konstrukcji jego treści, która nie podlega przecież tzw. *obróbce redakcyjnej* ze strony dziennikarzy przygotowujących materiał (np. eliminujących treści ciągle jeszcze uznawane za zbyt drastyczne). Terroryści zyskali zatem nowe, niejako własne medium, uniezależniając się od mediów *oficjalnych*. Stanowi to niebywałe

---

[10] Zob.: J.J. Carafano, R. Weitz, *Combating Enemies Online: State Sponsored and Terrorist Use of Internet*, Backgrounder, The Heritage Foundation, No. 2105, February 8, 2008, s. 3–4. http://www.heritage.org/Research/nationalSecurity/bg2105.cfm.

[11] Zob.: *ibidem*.

[12] Zob.: D. Tucker, *Terrorism, Networks and Strategy: Why the Conventional Wisdom is Wrong*, Homeland Security Affairs, Vol. IV, No. 2, June 2008, s. 9–10.

wzmocnienie ich przekazu, zwłaszcza, iż media *tradycyjne* bez wątpliwości powtórzą i dodatkowo nagłośnią przekaz internetowy[13].

W rękach terrorystów internet stał się także narzędziem wywiadowczym, dzięki któremu mogą oni dokonywać wyboru celu zamachu, dokonywać co najmniej wstępnego rozpoznania, określić drogi dojścia, wybrać najbardziej optymalny *modus operandi*, a w przypadku dokonania włamania do sieci wewnętrznej – także zneutralizować istniejące zabezpieczenia czy wręcz doprowadzić do zakłóceń w funkcjonowaniu instytucji wybranej jako cel. W ten sposób mogą zatem powstawać plany ataku, które – także poprzez sieć – mogą być przekazywane i koordynowane z uczestniczącymi podmiotami.

Można zatem stwierdzić, że wykorzystując narzędzia sieciowe organizacje terrorystyczne mogą realizować klasyczne zadania określane jako C^{4}I – Command, Control, Communication, Coordination, Intelligence[14].

Zarysowane powyżej aspekty działalności terrorystycznej eksponują znaczenie informacji. Wszystko wskazuje na to, że współczesne organizacje terrorystyczne stosują – intuicyjnie lub intencjonalnie – wskazówki Carlosa Marighelli. „Nowoczesne media – pisał on jeszcze w 1971 r. – poprzez proste powiadamianie o tym, czego dokonali rewolucjoniści, stają się potężnymi narzędziami naszej propagandy. Jednakże, ich działanie nie zwalnia bojowników od zakładania własnych podziemnych drukarni i posiadania własnych kopiarek (…) Wojna nerwów – albo wojna psychologiczna – jest techniką walki opartą na bezpośrednim i pośrednim użyciu mass mediów. (…) Jej celem jest demoralizowanie władz. Poprzez nie możemy rozpowszechniać fałszywe lub nawet sprzeczne informacje oraz szerzyć lęk, niepewność i wątpliwości wśród elit reżimu”[15].

Uznanie informacji za kluczowy element nie ogranicza się wyłącznie do terroryzmu, lecz stanowi immanentną cechę współczesnych konfliktów, w których informacja jest wykorzystywana zarówno jako broń, jak i traktowana jako cel. Autorzy prognozy „Świat w 2025 r.” podkreślając zmieniający się charakter współczesnych konfliktów wskazują na 4 rysujące się trendy. Po pierwsze, jest to rosnące znaczenie informacji, związane z wynalazkami z zakresu technologii informacyjnej. Po wtóre, to ewolucja możliwości prowadzenia wojny nieregularnej. „Nowoczesne technologie telekomunikacyjne, takie jak telefony satelitarne czy

---

[13] Na temat wykorzystania internetu przez terrorystów zob.: B. Bolechów, *Internet as a Flexible Tool of Terrorism*, [w:] *Terrorism, Media, Society*, T. Płudowski (red.), Wydawnictwo Adam Marszałek, Collegium Civitas, Toruń 2006, s. 34–44.

[14] Carafano, Weitz, *op. cit*., s. 3; por.: M. Zanini, S.J.A. Edwards, *The Networking of Terror in the Information Age*, [w:] *Networks and Netwars. The Future of Terror, Crime and Militancy*, J. Arguilla, D. Ronfeldt (red.), Santa Monica 2001, s. 35, 41; Aleksandrowicz, *Sieć…*, *op. cit.*

[15] T. Goban-Klas, *Media i terroryści. Czy zastraszą nas na śmierć?*, Warszawa 2009, s. 188.

komórkowe, internet, zaawansowane szyfrowanie, w połączeniu z ręcznymi urządzeniami nawigacyjnymi oraz systemami informatycznymi o dużej mocy, które mogą pomieścić duże ilości tekstów, map, zdjęć cyfrowych oraz filmów, znacznie ułatwią siłom nieregularnym organizowanie, koordynowanie oraz przeprowadzanie operacji rozproszonych". Po trzecie, wzrost znaczenia niemilitarnych aspektów konfliktów zbrojnych. „Niemilitarne sposoby walki, takie jak konflikty cybernetyczne, ekonomiczne, psychologiczne oraz oparte na informacji staną się dominujące (…) uczestnicy konfliktów będą angażować się w 'wojny medialne', by zdominować dwudziestoczterogodzinny cykl informacji oraz manipulować opinią publiczną do realizacji własnych celów oraz zdobycia szerokiego poparcia dla swojej sprawy". Po czwarte wreszcie, rozwój oraz eskalacja konfliktów wykraczających poza tradycyjne pole walki[16]. Na marginesie niejako warto wspomnieć, iż zdaniem *National Intelligence Council* dostęp do zaawansowanych technologii oraz wiedzy naukowej sprawiają, iż w zasięgu organizacji terrorystycznych znajdują się coraz bardziej niebezpieczne możliwości[17].

Czy zatem kategorię walki informacyjnej możemy zastosować do analizy zagrożeń terrorystycznych? Pytanie to możemy uznać za retoryczne, szczególnie wobec uznania terroryzmu za konflikt asymetryczny, co wiąże się również z uznaniem za wojnę konfliktu pomiędzy państwem a podmiotem niepaństwowym[18].

Od WTC do mikrozamachów

Zamach londyński w 2005 r. był ostatnim tej skali zamachem Al Kaidy w Europie. Zmieniało się modus operandi. Zamachy zaczęły być dokonywane przez niewielkie grupy bądź wręcz pojedyncze osoby (*lone wolf/solo terrorist*). Połączenie obu tych tendencji stanowi istotę taktyki *mikroterroryzmu*, zdefiniowanej przez internetowy magazyn Al Kaidy *Inspire* jako „taktyka wykrwawienia wroga za pomocą tysiąca ciosów"[19].

---

[16] *Świat w 2025. Scenariusze Narodowej Rady Wywiadu USA*, Kraków 2009, s. 195–196.

[17] *Ibidem*, s. 194.

[18] Zob. na ten temat: T. Aleksandrowicz, *Zagrożenia dla bezpieczeństwa państwa ze strony terroryzmu międzynarodowego*, [w:] *Krytyka prawa. Niezależne studia nad prawem*, tom II „Bezpieczeństwo", W. Sokolewicz (red. nauk.), Warszawa 2010; *idem*, *Nowy paradygmat bezpieczeństwa na progu XXI wieku in statu nascendi*, [w:] *Wymiary bezpieczeństwa na progu XXI wieku. Między teorią a praktyką*, A. Zaremba, B. Zapała (red.), Wydawnictwo Adam Marszałek, Toruń 2010.

[19] Zob.: F. Zakaria, *The Year of Microterrorism*, Time, Dec. 14, 2010, http://content.time.com/time/specials/packages/article/0,28804,2036683_2037181_2037470,00.html, dostęp 30.03.2014.

Za szczególnie istotną tendencję w obszarze zagrożeń terroryzmem bombowym należy uznać pojawienie się i rosnącą popularność tzw. improwizowanych urządzeń wybuchowych (IED – *Improvised Explosive Device*). Nie wdając się w tym miejscu w szczegółowe rozważania definicyjne, dla celów niniejszego opracowania przyjmijmy[20], iż są to takie urządzenia służące celom śmiercionośnym i niszczącym, które zostały przygotowane przez sprawców *ad hoc* z materiałów powszechnie dostępnych. Wśród badających tą problematykę kryminologów popularne stało się nawet określenie „materiały wybuchowe z łazienki" – różnego rodzaju powszechnie dostępne substancje chemiczne, wykorzystywane np. w przemyśle kosmetycznym, które po połączeniu w odpowiednich proporcjach tworzą mieszankę wybuchową. Stąd m.in. wywodzą się uznawane niekiedy przez podróżnych rygorystyczne zakazy wnoszenia na pokład samolotu niewinnych z pozoru substancji, które połączeniu tworzą materiał wybuchowy – zdaniem znawców przedmiotu sporządzenie kompletnej listy takich substancji jest niemożliwe[21].

IED należy ocenić jako broń tanią, łatwą konstrukcji i – biorąc pod uwagę komponenty – powszechnie dostępną. W praktyce do ich konstrukcji stosowana jest różnego rodzaju amunicja, materiały wybuchowe, środki zapalające oraz powszechnie dostępne urządzenia elektroniczne. Rodzaje zapalników i bomb przygotowywanych przez sprawców w warunkach domowych charakteryzują się indywidualna i niepowtarzalną budową[22].

Niestety, wiedza na temat przygotowywania tego typu urządzeń i produkcji materiałów wybuchowych nie jest już od dawca wiedzą ekskluzywną, stosowne wskazówki można bez problemu znaleźć choćby w internecie, w tym także na stronach polskich[23].

Stosunkowo łatwy dostęp do komponentów służących do produkcji IED i wiedzy w tym zakresie powoduje, iż tradycyjne metody prewencyjne polegające na kontroli potencjalnych źródeł zaopatrzenia sprawców (np. magazyny wojskowe,

---

[20] Na temat definicji IED zob. np. S. Kowalkowski, *Bezpieczeństwo wojsk w aspekcie zagrożeń wynikających z użycia improwizowanych urządzeń wybuchowych* i T. Ciszewski, Z. Kamyk, *Zagrożenie IED w konfliktach asymetrycznych*, [w:] *Kierunki i możliwości rozwoju narodowych zdolności w zakresie przeciwdziałania improwizowanym urządzeniom wybuchowym (materiały z konferencji)*, Dowództwo Wojsk Lądowych, Szefostwo Wojsk Inżynieryjnych, Centrum Szkolenia Wojsk Inżynieryjnych i Chemicznych, Wrocław 2010.

[21] Wg. Alfreda Blumsteina z Carnegie Mellon University w Pittsburghu (USA), powodem zakazu jest to, że potencjalnie można połączyć je na pokładzie, a nie wyglądają wcale na bombę, kiedy prześwietla się bagaż, http://wiadomosci.wp.pl/kat,1356,title,Materialy-wybuchowe-z-domowej-lazienki,wid,8459031,wiadomosc.html?ticaid=1b8ef, dostęp 30.03.2014.

[22] Zob.: Ciszewski, Kamyk, *op. cit.*, s. 116.

[23] Zob. np.: Źródło: *Vortal Młodego Chemika*, http://vmc.org.pl, dostęp 15.10.2010.

kopalnie etc.) stały się niewystarczające. Równocześnie zjawisko nazwane „bombą z łazienki" powoduje, iż niezwykle trudno jest sporządzić listę substancji potencjalnie niebezpiecznych, których obrót komercyjny powinien podlegać ograniczeniom czy kontroli. Możliwość przygotowania ładunku wybuchowego jednorazowo, *ad hoc*, z przeznaczeniem do wykorzystania w konkretnym zamachu terrorystycznym wyeliminowała potrzebę tworzenie przez terrorystów i zorganizowane grupy przestępcze specjalnych „manufaktur", będących potencjalnie słabym punktem z powodu możliwości ich ujawnienia przez policję. Co więcej, sprawców cechuje nieograniczona wręcz pomysłowość, co w połączeniu z możliwością stworzenia (konstrukcji) IED bezpośrednio na miejscu planowanego zamachu stawia przed służbami antyterrorystycznymi nowe wyzwania.

Konsekwencją takiego stanu rzeczy stała się konieczność zmiany podejścia szeroko rozumianych służb antyterrorystycznych i innych podmiotów potencjalnie związanych ze sferą bezpieczeństwa i porządku publicznego. Punktem wyjścia stała się konstatacja, że terrorystyczny zamach bombowy (podobnie zresztą, jak każdy z wykorzystaniem dowolnego modus operandi) jest procesem złożonym, w skład którego wchodzi kilka ogniw: radykalizacja postaw, rekrutacja, planowanie, trening, wybór celu, pozyskanie materiałów i wiedzy, przygotowanie komponentów, konstrukcja IED etc.). Każde ogniwo tego łańcucha stwarza potencjalne możliwości dla służb antyterrorystycznych. Stąd znaczenie rozpoznania operacyjnego środowisk radykalnych, procesu profilowania potencjalnych sprawców, monitorowanie potencjalnych celów. Istotnego znaczenia nabiera także edukacja antyterrorystyczna społeczeństwa, dzięki której udaje się zapobiegać tragedii: reagowanie na porzucone, bezpańskie pakunki, nietypowe zachowania, zakupy środków chemicznych (kosmetycznych, farmaceutycznych) w nietypowych ilościach, zachowanie się bezpośrednio po zamachu – listę tych elementów można długo wymieniać.

Pojawienie się w wyniku rewolucji technologicznej w sferze komunikacji i łączności środowiska sieciowego, co stało się czynnikiem determinującym powstanie i rozwój społeczeństwa informacyjnego, umożliwiło wzrost możliwości destrukcyjnych pojedynczych osób i ich niewielkich grup. Z tego punktu widzenia działalność terrorystyczna prowadzona przez takie pojedyncze podmioty przypomina taktykę typu *swarming*, czyli atak roju.

W literaturze przedmiotu[24] dokonuje się rozróżnienia na *solo terrorism* i *lone wolf terrorism*. Z kategorią *solo terrorism* mamy do czynienia wówczas, gdy pojedyncza

[24] M. Adamczuk, *Terroryzm indywidualny jako zagrożenie dla bezpieczeństwa europejskiego*, [w:] *Zamach w Norwegii. Nowy wymiar zagrożenia terroryzmem w Europie*, K. Liedel, P. Pasecka, T.R. Aleksandrowicz (red. nauk), Warszawa 2011, s. 33 i nast.

osoba, nie będąca członkiem organizacji, a jedynie jej sympatykiem, sama szuka z nią kontaktu, radykalizuje się pod wpływem głoszonej przez taką organizację ideologii, planuje, przygotowuje i dokonuje samodzielnie zamachu terrorystycznego. Jej działania mogą być inspirowane wskazówkami i sugestiami organizacji, jednak sprawca działa sam, na własną rękę i bez powiązań organizacyjnych. Przykładem takiego działania może być choćby Umar Farouk Abdulmutallab, który 25 grudnia 2009 r. dokonał samobójczej (nieudanej) próby zamachu na samolot Northwest Airline (lot 253 Amsterdam – Deitroit). W prowadzonym po zatrzymaniu sprawcy postepowaniu ustalono, iż przed zamachem pozostawał w kontakcie z Anwarem al Awlakim i Al Quaeda Arabian Penisula (AQAP), a informacje służące skonstruowaniu urządzenia wybuchowego uzyskał dzięki open source Jihad – a więc ze źródeł otwartych, rozpowszechnianych m.in. przez AQAP[25].

Natomiast *lone wolf terrorism* oznacza, że sprawca nie ma żadnych – pośrednich ani bezpośrednich – kontaktów z żadną organizacją terrorystyczną, a inspirację do działania i wskazówki dotyczące metod i technicznych aspektów dokonania zamachu czerpie z mediów masowych (głównie z internetu). Do tej kategorii zalicza się m.in. Andrew Ibrahim, brytyjski konwertyta, który planował dokonanie samobójczego zamachu bombowego w centrum handlowym w Wielkiej Brytanii w kwietniu 2008 r. W toku prowadzonego postępowania nie ustalono jakichkolwiek śladów świadczących o wsparciu innych osób czy organizacji, ani też kontaktów z jakimikolwiek organizacjami terrorystycznymi. Inspiracją do podjęcia działań (oraz jedną z przyczyn radykalizacji poglądów) były treści dostępne w internecie[26].

Przywołana Autorka wskazuje na jeszcze jedną kategorię – *lone wolf pack*. Nosi ona identyczny charakter, co *lone wolf*, jednak w tym przypadku mamy do czynienia nie z pojedynczą osobą, lecz niewielką grupą osób, które wzajemnie się radykalizują i postanawiają w imię podzielanej przez siebie ideologii dokonać zamachu.

Śmierć Osamy bin Ladena

Osama bin Laden zginął 2 maja 2011 r. w wyniku operacji amerykańskich sil specjalnych. Jego śmierć miała charakter symboliczny: Stany Zjednoczone, likwidując swojego wroga nr 1, przekazały terrorystom jasne przesłanie – nie można bezkarnie atakować USA. Całą koncepcja amerykańskiej *War on Terror* była

[25] *Ibidem*, s. 45.

[26] *Ibidem*, s. 46.

wielokrotnie poddawana ostrej krytyce. Trzeba jednak przyznać, że stanowiła – obok zdecydowanego wzrostu sprawności zachodnich służb antyterrorystycznych – istotny czynnik powodujący ograniczenie aktywności Al Kaidy w Stanach Zjednoczonych i w Europie. Regionem zapalnym pozostał Afganistan.

Nie oznaczało to jednak, że zagrożenia terrorystyczne związane z działalnością radykalnych islamistów zostały zminimalizowane. Trudno zaprzeczyć, że Amerykanie odnieśli bezapelacyjne zwycięstwo w Iraku; równocześnie nie można powiedzieć, iż udało się w tym państwie utworzyć stabilne struktury władzy i zapewnić bezpieczeństwo. Irak stał się równie niebezpiecznym miejscem, co Afganistan. Trzeba jednak zauważyć, iż cele zamachów terrorystycznych ograniczały się do regionu; nadal nie próbowano dokonywania zamachów na wielką skalę w Europie[27].

Arabska Wiosna i jej konsekwencje

Rok śmierci Osamy bin Ladena to także radykalna zmiana na mapie politycznej Bliskiego Wschodu, która została określona mianem Arabskiej Wiosny. Mówiąc precyzyjnie Arabska Wiosna zaczęła się 17 grudnia 2010 roku w Tunezji, gdy bezrobotny sprzedawca uliczny Mohamed Bouazizi podpalił się w proteście przeciwko brakowi perspektyw na poprawę swojej sytuacji życiowej. W krajach arabskich zaczęły się protesty społeczne, demonstracje przeciwko autorytarnym rządom, wezwania do budowania demokracji i wprowadzenia wolności i swobód obywatelskich. Zwolennicy demokratycznych przemian ponieśli porażkę, jej przyczyny to temat na odrębne opracowanie. W kontekście zagrożeń terrorystycznych ważne jest co innego – powstały w wyniku przewrotów chaos, słabe rządy i nieefektywna władza stworzyły polityczną próżnię, którą skwapliwie wykorzystały organizacje islamistyczne. Wojna domowa w Syrii, wojna domowa w Libii, ciągłe napięcia w Egipcie… Okazało się, że nie tak prosto jest zbudować demokrację i że nie wystarcza do tego obalenie panującego dyktatora.

W regionie MENA – Bliski Wschód i Afryka Północna – powstało nowe centrum islamistycznego terroryzmu. Śmierć bin Ladena była mocnym ciosem osłabiającym Al Kaidę, jednak nie oznaczała jej końca. Nikt zresztą nie przypuszczał, że śmierć Osamy bin Ladena zakończy funkcjonowanie Al Kaidy i negatywnie wpłynie na aktywność islamistycznych organizacji terrorystycznych.

---

[27] Zob.: T. Aleksandrowicz, *Terroryzm jako zagrożenie dla bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, [w:] *Ocena poziomu zagrożenia terroryzmem i organizacji systemu antyterrorystycznego w Polsce*, P. Bogdalski, Z. Nowakowski, K. Rajchel (red. nauk.), Warszawa 2012, s. 17 i nast.

Al Kaida zawsze była organizacją sieciową, składała się z wielu połączonych ze sobą więzami ideologicznymi węzłów. Dziś widać to wyraźniej niż kiedykolwiek. Po śmierci lidera – symbolu, w korzystnych warunkach politycznego zamętu będącego faktycznym efektem Arabskiej Wiosny, zaczęła wzrastać liczba ugrupowań terrorystycznych i liczba ich członków[28]. Wzrasta także zagrożenie, choć na Zachodzie tego nie odczuwamy. Jednak śledząc rozwój sytuacji w Syrii, w Iraku, Somali czy Jemenie nie sposób oprzeć się wrażeniu, że mamy do czynienia z rosnącą siłą[29].

To poważne zagrożenie, którego neutralizacja wymaga zaawansowanej współpracy międzynarodowej z udziałem państw regionu, wypracowania i realizacji strategii regionalnej. Potencjalni sojusznicy Zachodu nie są łatwymi koalicjantami. Algieria posiada co prawda potencjał militarny, nie jest jednak skłonna do nawiązania ścisłej współpracy ani ze Stanami Zjednoczonymi, ani ze swoimi sąsiadami. Mali – skłonne do współpracy, zwłaszcza z Francją – jest państwem słabym, o niewielkich zdolnościach militarnych. Libia po upadku Muammara Kadafiego z kolei wydaje się być chętna do współpracy, ma jednak niewiele do zaoferowania. Potencjalni sojusznicy zachodu wydają się zatem być w tej roli co najmniej problematyczni.

To jednak tylko jedna strona medalu. Zachód trudno jest traktować jako polityczny monolit w sprawie sytuacji w Afryce Północnej. Amerykanie są już wyraźnie zmęczeni militarnymi interwencjami w świecie, Europejczycy – zajęci kryzysem w Unii Europejskiej – nie byli i nie są chętni do interwencji, poza Francją, która ma w Afryce Północnej określone interesy[30]. Nie ulega też wątpliwości, że z punktu widzenia Europy ważniejszą sprawą stał się kryzys na Ukrainie.

Sam problem staje się coraz poważniejszy. W Afryce Północnej mamy do czynienia z uzbrojonymi grupami, które w miarę swobodnie przekraczają iluzoryczne niekiedy granice państwowe. Trzeba także zauważyć, że poszczególne ugrupowania terrorystyczne, reprezentujące nurt islamskiego fundamentalizmu (w tym Al Kaida Islamskiego Magrebu) są organizacjami samodzielnymi, działającymi poza kontrolą liderów Al Kaidy w Pakistanie i Afganistanie.

---

[28] Zob.: K. Izak, *Leksykon organizacji i ruchów islamistycznych*, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2014, passim.

[29] Zob.: *A Persistent Threat. The Evolution of al Qa'ida and Other Salafi Jihadists*, http://www.rand.org/pubs/research_reports/RR637.html, dostęp 19.11.2014.

[30] Zob.: M.R. Gordon, *North Africa Is a New Test*, The New York Times, January 20, 2013, http://www.nytimes.com/2013/01/21/world/africa/north-africa-new-test-for-us-as-terror-cells-spread.html?_r=0, dostęp 19.11.2014.

Państwo Islamskie – nowa jakość, nowe zagrożenia

Prognozowane zagrożenia zaczęły się bardzo szybko sprawdzać. Powstanie Państwa Islamskiego przyjęto początkowo jako utworzenie nowej terrorystycznej organizacji islamistycznej pod dość osobliwą nazwą; uznano ją za kontynuację Al Kaidy prowadzoną przez młodszych liderów. Jednak rychło okazało się, że mamy do czynienia z nowym zjawiskiem – oto bowiem organizacja terrorystyczna o charakterze islamistycznym zaczęła faktycznie odgrywać rolę państwa. Jeśli przyjąć, iż państwo to organizacja dysponująca swoim terytorium, mająca ludność i sprawująca na tym terytorium i zamieszkującą tam ludnością efektywną władzę, jak definiują państwo politolodzy i prawnicy, to nie ulega wątpliwości, iż mamy do czynienia z nowym z państwem właśnie. Specyficznym – ale państwem. Państwo stworzone przez organizację terrorystyczną stanowi zaś bez wątpienia zagrożeniem samym w sobie.

Zagrożenie to ma wiele wymiarów. Przede wszystkim to kolejna siła sprawcza, aktor na arenie politycznej i militarnej Bliskiego Wschodu, bardzo poważny czynnik destabilizujący, którego nie sposób nie brać pod uwagę w analizach rozwoju sytuacji w tym regionie. Biorąc pod uwagę słabość Libii czy Egiptu, o Syrii czy Iraku nie wspominając, aktor zyskujący coraz większe wpływy w regionie. Bliski Wschód nigdy nie był regionem spokoju i bezpieczeństwa, jednak po powstaniu Państwa Islamskiego zaczyna już nie tylko przypominać przysłowiową beczkę prochu. Co więcej, stało się już zagrożeniem dla samych muzułmanów i innych państw islamskich; trudno zatem jednoznacznie wykluczyć, iż Bliski Wschód przekształci się w obszar, na którym toczy się *bellum omnium contra omnes*[31]. A przecież Bliski Wschód jest nie tylko areną, na której istotną rolę odgrywają państwa arabskie; trudno w tym kontekście nie zadać pytań o stanowisko Izraela, Iranu, Rosji czy USA.

Państwo Islamskie zaczęło też stanowić bezpośrednie i pośrednie zagrożenie dla państw zachodnich[32]. Rzecz dotyczy nie tylko politycznych czy gospodarczych interesów Zachodu w regionie MENA. Obywatele państw zachodnich są na Bliskim Wschodzie porywani, torturowani i mordowani; efekt propagandowy

---

[31] Zob.: T.L. Friedman, *Who Are We*, The New York Times, November 15, 2014, http://www.nytimes.com/2014/11/16/opinion/sunday/thomas-l-friedman-who-are-we.html?smid=nytcore-ipad-share&smprod=nytcore-ipad, dostęp 19.11.2014.

[32] Zob.: G. Miller, *Airstrikes against Islamic State do not seen to have affected flow of fighters to Syria*, The Washington Post, October 28, 2014, http://www.washingtonpost.com/world/national-security/airstrikes-against-the-islamic-state-have-not-affected-flow-of-foreign-fighters-to-syria/2014/10/30/aa1f124a-603e-11e4-91f7-5d89b5e8c251_story.html, dostęp 19.11.2014.

tych zbrodni zdaje się narastać. Ponadto, a to wydaje się już znacznie poważniejszą kwestią dal bezpieczeństwa poszczególnych państw Unii Europejskiej, zauważalny jest napływ ochotników, którzy chcą walczyć w „siłach zbrojnych" Państwa Islamskiego. Są to obywatelami państw, także zachodnich, także rodowici Europejczycy, którzy – z różnych powodów – stali się wyznawcami islamu i to w jego najbardziej radykalnej wersji. Dzięki nim Państwo Islamskie rośnie w siłę. Ci ochotnicy kiedyś prawdopodobnie wrócą do swoich macierzystych krajów; część z nich jako ideolodzy radykalnego islamu, część – jako terroryści, z zamiarem dokonywania zamachów. Powoduje to również zagrożenia pośrednie, związane z reakcjami poszczególnych państw na tego typu zagrożenia. Po raz kolejny rodzą się napięcia między wolnością, z której jesteśmy słusznie dumni, a bezpieczeństwem, które można zwiększyć ograniczając wolność jednostki. Zabronić chętnym wyjazdu? Odmówić prawa powrotu? Pozbawić obywatelstwa? Zatrzymać po przekroczeniu granicy? Objąć ścisłą kontrolą operacyjną? A może zniszczyć Państwo Islamskie zabijając większość jego członków/obywateli? Tu nie ma dobrych odpowiedzi.

Rośnie ryzyko zamachów terrorystycznych i śmierci niewinnych ofiar. Jeśli w wyniku podjętych działań do tych zamachów nie dojdzie – władze znowu będą oskarżane przez organizacje chroniące prawa człowieka o wszystkie możliwe grzechy i wykorzystywanie sytuacji do wprowadzania systemu totalnej inwigilacji. Jeśli dojdzie – zostaną oskarżone o bezradność i niedocenienie zagrożeń. Co wybrać? *Tertium datur*?

Nie tylko islamiści

Nie ulega wątpliwości, iż oceniając zagrożenia terrorystyczne na pierwszym miejscu trzeba postawić organizacje islamistyczne. Jednak nie wyczerpuje to katalogu zagrożeń, szczególnie jeśli spojrzymy na te kwestie z punktu widzenia bezpieczeństwa antyterrorystycznego państwa europejskich, a przede wszystkim – państw członkowskich Unii Europejskiej[33].

Przede wszystkim trzeba zwrócić uwagę na aktywność organizacji o charakterze anarchistyczno-lewackim. Tendencja ta znalazła swoje potwierdzenie już w 2010 r., gdy początek listopada przyniósł całą serię zamachów bombowych w Grecji. Ładunki wybuchowe eksplodowały w ambasadach Szwajcarii i Rosji,

[33] Zob.: T. Aleksandrowicz, *Zagrożenia terrorystyczne w drugiej dekadzie XXI wieku. Analiza i próba prognozy*, [w:] *Bezpieczeństwo osób podlegających ustawowo ochronie wobec zagrożeń XXI wieku*, P. Bogdalski, J. Cymerski, K. Jałoszyński (red. nauk.), Szczytno 2014, s. 128–130.

Policji udało się przechwycić i zdetonować paczki z ładunkami wybuchowymi (ładunek umieszczony był pomiędzy książkami zapakowanymi w tekturowe pudła) na lotnisku w Atenach i w firmie kurierskiej. Były one adresowane do ambasady niemieckiej, siedziby EUROPOLU i Europejskiego Trybunału Sprawiedliwości, a także do prezydenta Francji Nicolasa Sarkoziego. Identyczne paczki dotarły do ambasad Bułgarii i Chile oraz do Urzędu Kanclerskiego w Bonn – jako nadawcę wskazano greckie ministerstwo gospodarki. Na szczęście – obeszło się bez ofiar. Sprawcami okazali się członkowie anarchistycznej organizacji *Fire Conspiracy Cells*, utworzonej stosunkowo niedawno, bo w 2007 r. Ma ona już na swoim koncie szereg zamachów terrorystycznych, których celem były m.in. postaci z greckiego życia politycznego czy biuro AFP.

Korelacja z kryzysem gospodarczym i finansowym jest wyraźna – zarówno pod względem czasu, jak i geografii. Wprowadzane reformy spotykają się ze społecznym niezadowoleniem tworzącym podglebie dla masowych protestów i wzrostu nastrojów radykalnych. Część z nich może kanalizować się właśnie w formie zamachów terrorystycznych. Na szczęście, powolne wychodzenie z kryzysu przełożyło się na spadek aktywności organizacji terrorystycznych, czego przykładem jest sytuacja w Grecji.

W kategoriach zagrożeń terrorystycznych należy także rozpatrywać aktywność organizacji skrajnie prawicowym, przede wszystkim neonazistowskim. Aresztowania, jakich dokonały władze węgierskie wskazują, iż coraz więcej państw spotyka się z tym problemem. Oprócz znanych z przeszłości ugrupowań typu *Blood&Honour*, *White Power* czy *Combat 17* pojawiają się kolejne, min. właśnie na Węgrzech, gdzie HANLA (*Hungarian Arrows National Liberation Army*) planowała m.in. zamachy bombowe przed domami członków parlamentu. Tego zagrożenia nie można zlekceważyć, ponieważ istnieje swoista międzynarodówka tego typu organizacji (bazujących ideologicznie na nazistowskich sentymentach); funkcjonują one nie tylko w państwach UE, lecz także m.in. w Rosji. Warto w tym kontekście zauważyć, że Rosja także jest areną działań terrorystów. W latach 1991–2012 doszło tam do 1 895 zamachów terrorystycznych. Ponad 50% były to zamachy bombowe, prawie 2% – samobójcze. Warto o tym pamiętać choćby z dwóch przyczyn: Rosja jest naszym sąsiadem, a kryzys ukraiński nie wydaje się zmierzać do szczęśliwego zakończenia. Możliwe są różne scenariusze, także te negatywne[34].

Zagrożenie to zwiększa ksenofobiczny charakter tych organizacji i narastająca islamofobia, co w kontekście radykalizacji środowisk muzułmańskich w Europie

[34] Dane dotyczące Rosji zob.: http://russiansphinx.blogspot.com/2014/01/terrorist-attacks-in-russia-since-1991.html, dostęp 30.03.2014. Por.: *Global Terrorism Database*, http://www.start.umd.edu/gtd, dostęp 30.04.2014.

tworzy w dającej się przewidzieć perspektywie kolejne punkty zapalne. Również w tym kontekście można spodziewać się pojawienia *samotnych wilków*.

Zagrożenia ze strony organizacji o profilu etno-nacjonalistycznym (separatystycznym) noszą charakter lokalny i wiążą się z trwającymi od dziesięcioleci konfliktami w Europie. Przede wszystkim operujących w Hiszpanii organizacjach takich jak *ETA*, *Taldes Y*, *Resistentcia Galega* i *Independentismo Radical Galega*, korsykańskiej organizacji FLNC (*Front Liberation de Nationale de la Corse*). Aktywne są także następczynie Irlandzkiej Armii Republikańskiej (CIRA – *Continuity IRA*, RIRA – *Real IRA*), odnotowano także aktywność INLA (*Irish National Liberation Army*). Warto także odnotować aktywność w Europie organizacji wywodzących się spoza naszego kontynentu, przede wszystkim Tamilskich Tygrysów (LTTE – *Liberation Tigers of Tamil Elam*) czy Kurdyjska Partia Pracy/Kurdyjski Kongres Ludowy (PKK/KONGRA – GEL), a nawet południowoamerykańskiej FARC (*Fuerzas – Armadas Revolucionares Colombiana*).

Raporty TE-SAT zwracają także uwagę na rosnące powiązania pomiędzy organizacjami terrorystycznymi a zorganizowanymi grupami przestępczymi. Zorganizowana przestępczość zaczyna stanowić coraz istotniejsze źródło finansowania działalności terrorystycznej, dotyczy to zwłaszcza handlu bronią i narkotykami, handlu ludźmi, oszustw finansowych, prania brudnych pieniędzy i wymuszeń. Dotyczy to szczególnie organizacji kurdyjskich i Tamilskich Tygrysów; charakterystyczne wydają się być powiązania np. pomiędzy baskijską *ETA* a wspomnianą kolumbijską organizacją *FARC*.

Kończąc ten krótki przegląd należy także wspomnieć o zagrożeniach związanych z tzw. *single – issue terrorism*, który w Europie przybiera głównie postać organizacji obrońców praw zwierząt. Według autorów Raportu europejskie ugrupowania tego typu zaczynają tworzyć sieć, której najsilniejsze ogniwa znajdują się w Wielkiej Brytanii. Co więcej, obrońcy praw zwierząt, anarchiści i radykalni obrońcy środowiska naturalnego zaczynają tworzyć wspólną ideologię, która staje się powoli spoiwem łączącym różne z pozoru grupy.

Nowe środowisko – cyberprzestrzeń

W ciągu minionego dziesięciolecia cyberprzestrzeń stała się areną działań zarówno o charakterze wojskowym (ataki na systemy dowodzenia i łączności przeciwnika), jak i wywiadowczym, sabotażowym czy wręcz przestępczym (np. kradzieże komputerowe), a nawet chuligańskim, nie wspominając o działaniach propagandowych czy politycznych. Konflikt cybernetyczny może przybrać

formę aktywizmu (niedestrukcyjna działalność informacyjno-propagandowa, np. na forach internetowych, czatach, portalach społecznościowych), haktywizmu (stanowiącego kombinację aktywizmu i działań zakłócających funkcjonowanie określonych systemów komputerowych, np. poprzez blokowanie dostępu do serwerów) lub cyberterroryzm politycznie motywowanego ataku na komputery, sieci lub systemy informatyczne w celu zniszczenia infrastruktury i wymuszenia na rządzie lub organizacji określonego działania lub zaniechania). Stwarza to nowe zagrożenia dla bezpieczeństwa narodowego, bowiem w coraz większym stopniu elementy infrastruktury krytycznej państw funkcjonują w oparciu o technologie informacyjne i są podatne na zagrożenia z cyberprzestrzeni. Istotne znaczenie ma też fakt, iż znaczna część infrastruktury krytycznej znajduje się w rękach podmiotów pozapaństwowych (komercyjnych), co w oczywisty sposób rozszerza zakres podmiotowy bezpieczeństwa narodowego.

Cyberprzestrzeń jest zatem sferą działania zarówno przestępczości wymierzonej przeciwko interesom obywateli, państwa i podmiotów gospodarczych, jak też działań wymierzonych w obronność i bezpieczeństwo państwa; jest także przestrzenią, w której toczy się walka informacyjna. Najpoważniejsze zagrożenia związane są z pozyskiwaniem danych dostępowych do kont bankowych, przejmowaniem kontroli nad komputerami i atakami typu DDoS. W praktyce zastosowano także próbę przejęcia kontroli nad systemem komputerowym sterującym pracą obiektu przemysłowego (atak na instalacje jądrowe w Iranie). Funkcjonowanie nowoczesnego, rozwiniętego ekonomicznie państwa nieodłącznie wiąże się z zapewnieniem stałego i prawidłowego funkcjonowania systemów gromadzenia i transmisji danych, monitorowania i sterowania. Do działań o charakterze agresji cybernetycznej mogą się uciekać zarówno władze i służby państw wrogich, gotowych prowadzić swego rodzaju wojnę informacyjną, jak i wielkie koncerny, organizacje o charakterze pozarządowym i ponadnarodowym, w tym przestępcze. Jak wykazują doświadczenia ostatnich lat, ataki w sferze cybernetycznej mogą mieć zarówno podłoże polityczne i religijne, jak i biznesowe. Nie można wykluczyć, że w niedalekiej przyszłości cyberataki, skierowane zwłaszcza na elementy infrastruktury krytycznej, staną się narzędziem szantażu w rękach przestępczości zorganizowanej. Elementem sprzyjającym takim atakom jest duża trudność w udowodnieniu jego sprawstwa. W efekcie żaden z dotychczasowych ataków na państwa (Estonia 2007, Litwa 2008, Gruzja 2008) lub organizacje międzynarodowe (np. na MFW w 2011 r.) nie zakończył się formalnym wskazaniem jego sprawcy[35]. Nakazuje to traktowanie współczesnych

[35] Na temat zagrożeń cyberterroryzmem zob.: *Cyberterroryzm. Nowe wyzwania XXI wieku*, praca zbiorowa pod redakcją T. Jemioły, J. Kisielnickiego i K. Rajchela, Warszawa 2009, passim.

zagrożeń terrorystycznych również w kategoriach walki/wojny informacyjnej, prowadzonej również w cyberprzestrzeni[36].

Podsumowanie

Najnowsze dane statystyczne dostępne w chwili pisania tych słów (grudzień 2014 r.)[37] nie napawają optymizmem.

Rok 2013 przyniósł wzrost zagrożeń terrorystycznych. W porównaniu do roku poprzedzającego liczba zamachów wzrosła o 44%, liczna ofiar śmiertelnych – 61%. Ponad 80% ofiar śmiertelnych straciło życie w zamachach dokonanych na terytorium Iraku, Afganistanu, Pakistanu, Nigerii i Syrii; 90% zamachów miało miejsce w państwach, na terytorium których dochodzi do masowych naruszeń praw człowieka. Największe zagrożenia niesie ze sobą działalność ugrupowań talibów, Boko Haram, Państwa Islamskiego i Al Kaidy. Terroryzm, mimo, że podlega jako zjawisko daleko idącemu zróżnicowaniu i dynamicznym zmianom, nadal stanowi realne i poważne zagrożenie zarówno dla bezpieczeństwa narodowego, jak i bezpieczeństwa poszczególnych państw. Z punktu widzenia Zachodu, a więc i Polski, analiza minionych dziesięciu lat pozwala na sformułowanie następujących konstatacji:

– gros zamachów terrorystycznych ma miejsce na terytorium państw będących tzw. punktami zapalnymi na mapie świata. Nie może to jednak stanowić powodu do samouspokojenia, bowiem konflikty te wpływają na bezpieczeństwo międzynarodowe. Co więcej, stanowią one zagrożenie dla wszystkich osób znajdujących się w tych rejonach. Odrębną kwestią jest udział obywateli państw zachodnich w walkach m.in. w Syrii, ich daleko postępująca radykalizacja i perspektywa powrotu do Europy;

---

[36] T. Aleksandrowicz, *Terroryzm jako walka informacyjna*, [w:] *Zarządzanie informacją i energią w systemie bezpieczeństwa Unii Europejskiej*", B. Sitek, R. Trzaskalik (red.), Warszawa 2010, s. 341 i nast. Zob.: N. Robinson, *Cybersecurity Strategies Raise Hopes of International Cooperation*, RAND Review, Summer 2013, http://www.rand.org/pubs/periodicals/rand-review/issues/2013/summer/cybersecurity-strategies-raise-hopes-of-international-cooperation.html, dostęp 19.11.2014.

[37] *Global Terrorism Index 2014*. Measuring and Understanding the Impact of Terrorism. Institute of Econimics&Peace, http://www.visionofhumanity.org/sites/default/files/Global%20Terrorism%20Index%20Report%202014_0.pdf, dostęp 19.11.2014. Omówienie raportu zob.: A. Taylor, *These 5 Countries Accounted for Nearly All the World's Terrorism Death Last Year*, The Washington Post, November 18, 2014, http://www.washingtonpost.com/blogs/worldviews/wp/2014/11/18/these-5-countries-accounted-for-nearly-all-the-worlds-terrorism-deaths-last-year, dostęp 19.11.2014.

– zagrożenia terrorystyczne nie wiążą się jedynie z aktywnością organizacji islamistycznych. Jest to widoczne szczególnie w państwach członkowskich Unii Europejskiej. Po metody terrorystyczne sięgają zarówno radykalne grupy lewackie, skrajnie prawicowe czy np. ekologiczne (*terroryzm jednej sprawy*). Bardzo aktywne są także terrorystyczne ugrupowania separatystyczne. Uwagę musi zwracać także fakt powiązań pomiędzy organizacjami terrorystycznymi a zorganizowanymi grupami przestępczymi;
– najczęściej stosowanym *modus operandi* sprawców pozostają zamachy bombowe. W znakomitej większości są one dokonywane z wykorzystaniem improwizowanych urządzeń wybuchowych, wytwarzanych z powszechnie dostępnych komponentów, co w znacznej mierze utrudnia działania prewencyjne służb antyterrorystycznych;
– tendencją rosnącą wydaje się być aktywność typu *lone wolf/solo terrorism*. Wzrastające zdolności destrukcyjne pojedynczych osób powodują, że tego typu zamachy stają się coraz groźniejsze, by wspomnieć choćby o zamachach w Oslo czy podczas maratonu w Bostonie, a także – *pro domo sua* – casus Brunona K.

Wydaje się, że mamy do czynienia z procesem radykalnej zmiany zagrożeń terrorystycznych, przynajmniej w odniesieniu do państw Zachodu. Zagrożenia terrorystyczne drugiej dekady XXI wieku przybierają postać *czarnego łabędzia*: sytuacji, która nie wpisuje się w modele i zawsze pozostaje poza marginesem obserwowanej i analizowanej rzeczywistości. *Czarny łabędź* to sytuacja nieprzewidywalna, niosąca za sobą poważne konsekwencje, wymykające się prognozowaniu[38].

Zamachy bombowe dokonywane przez pojedyncze osoby przy użyciu improwizowanych urządzeń wybuchowych należy uznać za *czarne łabędzie*. Aktywność organizacji, nawet niewielkiej, zawsze pozostawia za sobą ślady, które mogą zwrócić uwagę służb antyterrorystycznych. Pojedyncza osoba pozostawia takich śladów znacznie mniej, szczególnie, jeśli nie manifestuje swoich przekonań, nie ogłasza planów i manifestów, a przygotowania do zamachu zachowuje wyłącznie dla siebie[39]. Wykorzystanie improwizowanych urządzeń wybuchowych, wytwarzanych z komponentów powszechnie dostępnych na rynku, umożliwia uniknięcie przez sprawcę ryzyka wpadki podczas prób zakupu broni/materiałów wybuchowych na czarnym rynku bądź też ich kradzieży. Dla służb

---

[38] Teoria czarnego łabędzia została opracowana przez N.S. Taleba i zaprezentowana w książce *The Black Swan: the Impact of the Highly Improbable*, New York 2007. Na temat zastosowania teorii czarnego łabędzia do analizy środowiska bezpieczeństwa zob. Adamczuk, *op. cit.*, s. 37–41.

[39] Brunon K. nie zachował swoich planów i podejmowanych przygotowań w poufności, stąd skuteczna interwencja Agencji Bezpieczeństwa Wewnętrznego i niedopuszczenie do wykorzystania zgromadzonych przez sprawcę materiałów wybuchowych.

antyterrorystycznych taki sprawca jest zatem w praktyce nie do wykrycia aż do chwili zamachu. Wymusza to gruntowną rewizję postrzegania zagrożeń terrorystycznych, a przede wszystkim skłania do podjęcia badań naukowych mających na celu zastosowanie teorii *black swan* do analizy środowiska bezpieczeństwa, w tym zagrożeń terrorystycznych[40].

[40] Zob.: *Zagrożenia terrorystyczne w drugiej dekadzie…*, *op. cit.*, s. 136–137.