Cyberterroryści w cyfrowych czasach: profesjonalizacja i digitalizacja współczesnych organizacji terrorystycznych

Bogusław Węgliński

Bogusław Węgliński

Dolnośląska Szkoła Wyższa

Cyberterroryści w cyfrowych czasach – profesjonalizacja i digitalizacja współczesnych organizacji terrorystycznych

Słowa kluczowe: Al-Kaida, Państwo Islamskie, cyberterroryzm; terroryzm, Internet, media cyfrowe, ustawa antyterrorystyczna, drony.

Wprowadzenie: ewolucja instrumentarium terrorystycznego

Terroryści i przestępcy zawsze korzystali ze zdobyczy cywilizacji, także tych technicznych. Przejawem technologicznego zaawansowania terrorystów był choćby atak za pomocą gazu sarin w tokijskim metrze. Z drugiej strony możemy znaleźć mnóstwo przykładów na to, iż pomimo znaczących przeobrażeń współczesnego świata i rewolucji technologicznej oręż terrorystów nie zmienił się praktycznie w przeciągu ostatnich 150 lat. Pistolety, czy ładunki wybuchowe w dalszym ciągu stanowią groźny oręż w rękach terrorystów XXI w. i są dla społeczeństwa takim samym zagrożeniem jak dla pokoleń o wiek przynajmniej wcześniejszych. Zwracał na to uwagę w 1998 roku Zbigniew Brzeziński[1]. Niewiele później terroryści zrealizowali scenariusz użycia samolotów komunikacyjnych jako latających bomb. 11 września 2001 roku. Stał się on ponurą cezurą w historii ludzkości a widok walących się wież WTC w dalszym ciągu spędza sen z powiek służbom bezpieczeństwa na całym świecie. Jak na ironię, głównym zagrożeniem dla załóg porywanych w tym dniu samolotów były użyte przez terrorystów plastikowe noże do papieru oraz atrapy bomb. Renesans użycia broni białej widać także w serii palestyńskich ataków nożowników w Izraelu na przełomie ubiegłego i bieżącego roku. Alternatywną metodą ataków stało się jednak użycie samochodów i innych

[1] Z. Brzeziński, *Kłopoty dobrego hegemona*, źródło: http://szukaj.wyborcza.pl (dostęp: 06.05.2016).

pojazdów (używano także ładowarek) jako narzędzi do „rozjeżdżania" przystanków i grup przechodniów. Potwierdzeniem tej tezy stał się niestety atak z Nicei, gdzie niezależnie od inspiracji zamachowca, rozpędzona ciężarówka służyła jako narzędzie mordu[2]. Warto przy tym przypomnieć, że Francja była już celem tego typu ataków w grudniu 2014 roku, kiedy na szczęście skończyło się tylko na osobach rannych[3]. Obawiam się, że prostota działania i przerażająca „skuteczność" akcji może stać się inspiracją do przeprowadzania podobnych zamachów w przyszłości. Widać na tej podstawie, że działalność współczesnych organizacji terrorystycznych może się rozwijać wielotorowo. W dalszych fragmentach artykułu postaram się przybliżyć, te bardziej wyrafinowane technologicznie metody działań związanych z użyciem cyberprzestrzeni oraz pozwiązane z nimi wybrane rozwiązania ustawodawcze.

Technologie cyfrowe w służbie terrorystów

To nie wyposażenie, ale istota podejmowanych działań, która nie uległa zmianie świadczy o zagrożeniu jakie stwarzają współcześni terroryści. Trafnie zwraca na to uwagę Bartosz Bolechów[4].

W artykule postawiłem hipotezę, że współcześni terroryści wzorem swoich poprzedników wykorzystują instrumentarium swojej epoki, korzystając ze współcześnie dostępnych nowoczesnych technologii. Oprócz wyposażenia, czerpią oni także know how, czyli adaptują to co skuteczne w dzisiejszych metodach pracy i organizacji do funkcjonowania ugrupowań terrorystycznych. Hipotezie towarzyszy zestaw pytań badawczych:

[2] 14 lipca w godzinach wieczornych dokonano dwukilometrowego rajdu przez zatłoczoną promenadę nadmorską w Nicei. W jej wyniku 84 osoby zmarły, a ok. 200 odniosło różnego rodzaju obrażenia. Liczba ofiar nie musi być zamknięta, ponieważ część rannych w dalszym ciągu przebywa w stanie krytycznym. O ile władze francuskie sugerują powiązania sprawcy z islamskimi bojownikami, a ISIS „przyznało się" do przeprowadzenia zamachu, nie jest oczywiste, czy sprawca – 31-letni Mohamed Lahoualej Bouhlel, Tunezyjczyk, z prawem stałego pobytu we Francji rzeczywiście dokonał swego czynu w imię walki z „niewiernymi", czy po prostu przeszedł ostre załamanie psychiczne. Nie zmienia to faktu, że było to najkrwawsze dotychczas wykorzystanie samochodu jako narzędzia terroru; por. także *Zamach w Nicei. Francuska policja zatrzymała trzy osoby*, http://wiadomosci.gazeta.pl (dostęp: 17.07.2016).

[3] W grudniu 2014 odnotowano zamachy w Dijon i Nantes. Obaj sprawcy użyli samochodów do wjechania w tłum, wznosząc przy tym okrzyki związane z islamem. W Dijon rany odniosło 13 a w Nantes 10 osób. (*Francja: kolejny atak islamskiego radykała? Auto wjeżdża w tłum przechodniów w Nantes*, www.polskieradio.pl <<dostęp: 17.07.2016>>).

[4] B. Bolechów, *Terroryzm w świecie podwubiegunowym*, Toruń, 2002, s. 496-497.

1. Czy dzisiejsze organizacje terrorystyczne korzystają ze współczesnych osiągnięć technologicznych i organizacyjnych ?

2. Jak wygląda obecność organizacji terrorystycznych we współczesnych mediach cyfrowych? Na ile profesjonalna jest ich zawartość?

3. Czy współczesne państwa, w tym Polska są przygotowane na użycie nowoczesnych technologii, w tym dronów przez terrorystów?

Dzięki możliwościom, jakie stwarza jednak dzisiejsza technologia, użycie przez islamskich terrorystów miecza lub sztyletu, którym przed okiem kamery służącej do transmisji wydarzenia w sieci WWW dokonują oni egzekucji przedstawiciela naszej cywilizacji, nawet wydawałoby się przestarzała technologicznie biała broń może w dalszym ciągu służyć do zastraszania szerokich rzesz „niewiernych" odbiorców. Ten sam film oglądany przez inną grupę odbiorców wywoła euforyczne uniesienie dla toczonej przez nią walki, a niezdecydowanych może przekonać do wstąpienia w szeregi bojowników lub choćby sprowokować do wsparcia finansowego dzieła (oczywiście też przy pomocy nowoczesnych technologii bankowych). Niezależnie od etycznej wartości działań użyć możemy tych samych narzędzi. Tak krytykowany przecież za możliwość jego użycia w złych celach Internet może przecież służyć do propagowania idei demokratycznych w społeczeństwach zamkniętych[5], a nowe, cyfrowe technologie w rękach dyktatorów wydają się zagrożeniem porównywalnym z wykorzystaniem ich przez terrorystów[6].

Bruce Hoffman zauważa: „Narzędziami terrorystów są dzisiaj nie tylko bomby i rewolwery. Nowoczesny arsenał terrorysty obejmuje komputery i laptopy, nagrywarki CD i DVD, konta e-mailowe, Internet i sieć WWW. Terroryści dzięki nowym mediom mogą nie tylko kontrolować treść i kontekst przekazów, ale także środki, jakimi docierają do cyberprzestrzeni, i dobierać je stosownie do specyficznych grup odbiorców"[7].

Gabriel Weimann wyodrębnił typologię zastosowań Internetu przez grupy terrorystyczne. Najczęściej pełnione przez Internet role to :

1. sieć używana jako baza danych,
2. utrzymywanie kontaktu przez sieć WWW pomiędzy komórkami organizacyjnymi terrorystów,
3. internetowa rekrutacja i poszukiwania specjalistów,

[5] T. Danitz, W. P. Strobel, *Networking dissent: Cyber activists use the Internet to promote Democracy in Burma*, [w:] *Networks and Netwars*. red. Arquila J., Ronfeldt D, Santa Monica 2001, s. 129-169.
[6] D. Ronfeldt, J. Arquilla, *What next for networks and netwars?*, [w:] *Ibidem*, s. 314.
[7] B. Hoffman, *Foreword*, [w:] G. Weimann, *Terror on the Internet. The New Arena, the New Challenges*, Washington 2006, s. 9.

4. sieć jako miejsce przesyłania (zamieszczania) instrukcji i poradników,
5. sieć WWW jako narzędzie planowania i koordynacji działań,
6. miejsce zdobywania funduszy i zasobów,
7. internet jako miejsce walki z innymi organizacjami terrorystycznymi.[8]

Z zasobów i możliwości oferowanych przez wirtualną przestrzeń sieci chętnie korzystają obie strony konfliktu. W roku 2011, swoje konta na Twitterze uruchomili zarówno talibowie (@alemerahweb) jak i somalijskie Al-Shabaab (@HSM-Press). Jednocześnie konta utworzyli ich oponenci, kontyngent sił stabilizacyjnych NATO – (@ISAFmedia), czy mjr Emmanuel Chirchir (@MajorEChirchir), rzecznik kenijskiej armii w trakcie interwencji w Somalii[9]. Biorąc pod uwagę różnorodność proponowanych zastosowań, niewiele z dzisiejszych grup terrorystycznych może sobie pozwolić w kontekście ewolucji struktury, metod i celów działania na niekorzystanie z zaawansowanych technologii. Al-Kaida, czy jej współczesny sojusznik, a czasami konkurent - ISIS sprawnie wykorzystywały możliwości oferowane w wirtualnej przestrzeni. Obie organizacje nie stronią także od prowadzenia własnej polityki informacyjnej z wykorzystaniem mediów głównego nurtu. O ile Osama bin Laden chętnie przekazywał swoje przesłania telewizji Al Jazeera, o tyle wypowiedzi kalifa ISIS bez problemu można ściągnąć z sieci. Jak zauważa Patryk Cockburn „połowa świętej wojny toczy się w mediach. [...] Facebook, Twitter, YouTube oraz stacje telewizyjne codziennie przynoszą nowe informacje dotyczące idei, działań i celów sunnickich fundamentalistów. Mając dostęp do tak potężnych narzędzi propagandowych, ugrupowania w rodzaju Al-Kaidy nie muszą martwić się o napływ funduszy i ochotników”[10]. Nic dziwnego, że terroryści tak chętnie korzystają z Internetu skoro narzędzie to charakteryzuje:

- łatwy dostęp,
- niewielka (lub żadna) regulacja, cenzura albo inne formy kontroli państwowej,
- potencjalne wielkie audytoria rozproszone na całym świecie,
- anonimowość komunikowania,

[8] G. Weimann, *Terror on the Internet. The New Arena, the New Challenges*, Washington 2006, s. 111-146.
[9] D. Bennett, *Exploring the impact of an evolving war and terror blogosphere on traditional media coverage of conflict*, „Media, War & Conflict ” 2013, vol. 6, issue 1, s. 48.
[10] P. Cockburn, *Państwo Islamskie*, Warszawa 2015, s.168.

- szybki przepływ informacji,
- niezbyt kosztowne przygotowanie i utrzymanie portalu,
- multimedialność (możliwość łączenia tekstu, grafiki, słowa, muzyki filmu) oraz wymiana i ściąganie z sieci plików wideo, muzycznych itd.,
- zdolność podsuwania tematów tradycyjnym mass mediom, które coraz częściej traktują Internet jako źródło wiadomości[11].

Zachęcone możliwościami tkwiącymi w tym prostym narzędziu, organizacje terrorystyczne adaptują się do wymogów współczesnego świata. Al-Kaida, obecna w sieci od późnych lat 90-tych[12] ubiegłego wieku, dysponowała przez lata systemem informatycznym określanym przez służby jako Obelisk[13]. Do 2007 roku działał on na trzech, różnych płaszczyznach. Amerykańskie służby specjalne złamały

w pewnym momencie zabezpieczenia go chroniące, jednak przeciek medialny dotyczący nieujawnionego jeszcze przez organizację wystąpienia Bin Ladena musiał spowodować konsternację i potrzeby zmian w sieciowych zasobach i narzędziach organizacji[14]. Trzy poziomy zastosowań Internetu w Al-Kaidzie miały wyglądać następująco:

- na poziomie ścisłego kierownictwa organizacji funkcjonowała sieć do której dostęp miało tylko ok. 20 osób,
- na kolejnym stopniu, który obejmował krąg użytkowników średniego

  i niższego stopnia mogli się oni do niego dostać po wpisaniu haseł dostępu. Sam system pozostawał stosunkowo mobilny, co zabezpieczało go przed atakami służb na serwery go obsługujące,
- organizacja dysponowała także szeroką gamą, (ich liczba dynamicznie się zmieniała, jednak można mówić o 4-6 tys.) ogólnodostępnych stron internetowych skierowanych do sympatyków i osób „niezrzeszonych" pełniących funkcję propagandową, szkoleniową i rekrutacyjną[15].

[11] B. Hoffman*, op.cit.*, s. 9-11.
[12] D. E. Denning, *Terror`s Web: How the Internet Is Transforming Terrorism*, [w:] *Handbook of Internet Crime*, red. Y. Jewkes, M. Yar, London 2010, s. 195-196.
[13] B. Bolechów, *„Baza" w sieci. Wykorzystanie Internetu przez Al-Kaidę i jej zwolenników*, [w:] *Terroryzm w medialnym obrazie świata*, red. K. Liedel i S. Mocek, Warszawa 2010, s. 146-147.
[14] E. Lake, *Al Qaeda Breach Called 'Serious' but 'Reparable'*, źródło: www.nysun.com (dostęp: 19.07.2016).
[15] B. Bolechów, *„Baza" w sieci*… , s. 146-147.

Celem bojowników była także walka z infrastrukturą sieciowa i zawartością stron „niewiernych". Już w 2003 roku powstał Arabski Zespół Dżihadu Elektronicznego. Na szczęście główny, założony wtedy cel[16], którym było zniszczenie wszystkich izraelskich i amerykańskich witryn nie został dotychczas zrealizowany. Przedsięwzięcie wykraczało poza ramy Al-Kaidy, jednocząc wszystkich wokół wyznawanej idei. W ciągu zaledwie 7 lat od momentu kiedy meksykańscy zapatyści po raz pierwszy użyli Internetu do świadomej promocji i informowania o swoich działaniach[17] ten aspekt funkcjonowania organizacji terrorystycznej przeszedł gruntowną ewolucję. Cele działania e-dżihadystów zostały rozbudowane i obejmowały miedzy innymi:

- likwidację internetowych stron, które w jakikolwiek sposób obrażały muzułmanów,
- godne pomszczenie męczenników, którzy oddali swoje życie za Allaha a także innych prześladowanych jego wyznawców,
- ekonomiczne i moralne osłabienie użytkowników sieci WWW na Zachodzie,
- całkowity paraliż działalności infrastruktury komputerowej Zachodu doprowadzić ma do jego upadku[18].

Wobec prezentowanej, niewzruszonej postawy etycznej bojowników zaskakujące mogą być informacje jednego z byłych decydentów amerykańskiego wywiadu, który twierdzi, że komputery bojowników ISIS w większości wypełnione są treściami pornograficznymi[19]. Badający aktywność sieciowych bojowników Eli Alshech zauważa, że w początkowym okresie działania` w sieci (do roku 2006) ataki kierowano przeciwko trzem typom celów:

1. Atrakcyjnym celem były strony WWW propagujące niemuzułmańskie (w rozumieniu bojowników) ideologie: chrześcijaństwo, syjonizm, szyityzm(!).
2. Atakowano także strony promujące zakazane dla wyznawców Allaha aktywności (np. sportowe zaangażowanie kobiet).

[16] *Ibidem*, s. 147.
[17] D. E. Denning, *op. cit.*, s. 194-195; O zapatystach i ich działalności w sieci pisał także Michał Bogusz, por. M. Bogusz, *Ejército Zapatista de Liberación Nacional - wirtualna partyzantka*, [w:] *Terroryzm w medialnym obrazie świata*, red. K. Liedel i S. Mocek, Warszawa 2010, s. 162-172.
[18] B. Bolechów, *„Baza" w sieci* …, s. 150.
[19] L. Ferran, E. Brown, J.G. Meek, J. Fishel, *Jihadists' Computers '80 Percent' Full of Porn, Ex-Official Says*, źródło: http://abcnews.go.com (dostęp: 21.07.2016).

3. Na celowniku bojowników były także internetowe witryny, fora dyskusyjne i inne formy sieciowej aktywności, które urażały lub obrażały muzułmanów[20].

Al-Kaida wykorzystywała w swojej medialnej aktywności całą sieć mniej lub bardziej profesjonalnych producentów. Materiały ich produkcji zawierały zarówno logo wytwórcy, jak i zbrojnej grupy, którą promowały[21]. Interesującymi z punktu widzenia badacza było rozesłanie w maju 2008 roku przez Brygady Cyberdżihadu ponad 26 tys. maili do mieszkańców rejonu Zatoki Perskiej z informacją o celach działania organizacji, czy użycie do własnych celów neutralnych stron internetowych - znamienne było tu użycie arabskiej mutacji Wikipedii, na której umieszczano orędzia współpracującego jeszcze wtedy a Al-Kaidą Omara al-Baghdadiego[22]. Późniejsze dokonania cyfrowych mudżahedinów co pewien czas przykuwają uwagę światowych mediów. W 2015 roku skutecznie zakłócili oni funkcjonowanie stron francuskiej telewizji TV5[23]. Należy się spodziewać, że aktywność dżihadystów w sieci będzie narastała, choć oczywiście zdarzają się tez grupy hakerów, którzy atakują infrastrukturę sieciową bojowników[24].

W cyfrowy świat wpisują się także twórcy gier, w których gracze mogą się wcielać zarówno w przedstawicieli służb zwalczających terrorystów, jak i bojowników[25]. Widać w tym segmencie rynku zwiększającą się podaż produktów umożliwiających destrukcję świata, a nie jego obronę. Negatywni bohaterowie nie umierają w nich, lecz szybko wracają do kreowanej w grze rzeczywistości[26] Co więcej, możliwość szybkiego „odrodzenia" gracza po wirtualnej śmierci może wprowadzać zamieszanie w psychice młodych ludzi, co skutkuje atakami szalonych strzelców w Stanach Zjednoczonych i innych krajach, jak i terrorystycznymi atakami tzw. „samotnych wilków". Wpływ brutalnych gier komputerowych niewykluczony jest także w przypadku 18-letniego Niemca irańskiego pochodzenia, który 22 lipca

[20] E. Alshech, *Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad*, „Inquiry & Analysis Series Report" 2007, No. 329, s. 4-6.
[21] D. E. Denning, *op.cit*. s. 197-198.
[22] *Ibidem*, s. 198.
[23] *Francuska telewizja ofiarą cyberataku. Hakerzy podają się za dżihadystów*, źródło: http://www.newsweek.pl (dostęp: 22.07.2016).
[24] *Dżihadysta-gej? Zemsta hakera robi furorę*, źródło: http://tvn24bis.pl (dostęp: 22.07.2016).
[25] M. Schulzke, *Being a terrorist: Video game simulations of the other side of the War on Terror*, „Media, War & Conflict" 2013, vol. 6, issue 3, s, 218.
[26] M. Babecki M., *Funkcje epizodycznych gier internetowych w procesach modelowania wirtualnego wizerunku terrorysty i terroryzmu. Analiza aspektowa*, „Media – Kultura – Komunikacja Społeczna" 2013, nr 9, s. 49.

2016 zastrzelił w Monachium 9 osób i zranił kolejne 30, popełniając potem samobójstwo[27]. Argumenty przytoczone w podrozdziale wydają się potwierdzać hipotezę postawioną wcześniej, dając jednocześnie odpowiedź na część pytań badawczych tam zadanych.

Zastosowanie dronów – szanse i zagrożenia

Drony i BSL wykorzystywane są często do zwalczania organizacji terrorystycznych[28], z drugiej strony zagrożenie, jakie mogą one stanowić w rękach tych ugrupowań jawi się jako bardzo realne. Dobrze, że świadomość niebezpieczeństw jakie użycie dronów stwarza jest wśród przedstawicieli organów i służb odpowiedzialnych za utrzymanie naszego bezpieczeństwa w miarę wysoka, co przekłada sie na rozwiązania jakie zostały zawarte w nowej tzw. ustawie antyterrorystycznej. Dokument ten zakłada między innymi zmiany w dotychczas obowiązującym prawie lotniczym[29]:

Art. 126a. 1. Bezzałogowy statek powietrzny, w tym model latający, może zostać zniszczony, unieruchomiony albo nad jego lotem może zostać przejęta kontrola, w przypadku gdy:

1) przebieg lotu lub działanie bezzałogowego statku powietrznego: a) zagraża życiu lub zdrowiu osoby, b) stwarza zagrożenie dla chronionych obiektów, urządzeń lub obszarów, c) zakłóca przebieg imprezy masowej albo zagraża bezpieczeństwu jej uczestników, d) stwarza uzasadnione podejrzenie, że może zostać użyty jako środek ataku terrorystycznego;

2) bezzałogowy statek powietrzny wykonuje lot w przestrzeni powietrznej w części której państwowy organ zarządzania ruchem lotniczym wprowadził ograniczenia lotów albo znajdującej się nad terytorium Rzeczypospolitej Polskiej, w której lot statku powietrznego jest zakazany od poziomu terenu do określonej wysokości[30].

[27] *„Nienawiść do ludzi". Kolega ze szpitala psychiatrycznego o zamachowcu* . źródło: http://www.tvn 24.pl (dostęp: 25.07.2016).

[28] Pomimo tego, iż drony coraz częściej używane są zarówno przez siły porządkowe jak i regularną armię pozostaje cały wachlarz wątpliwości etycznych i prawnych towarzyszących tego typu działaniom. Zob. E. Schwarz, *Prescription drones: On the techno-biopolitical regimes of contemporary 'ethical killing'*, „Security Dialogue" 2016, vol. 47(I) , s. 56 i n.; P. Sheets, C.M. Rowling, T. M. Jones, *The view from above (and below): A comparison of American, British, and Arab news coverage of US drones*, „Media, War & Conflict" 2015. vol. 8, issue 3, s. 1-23 .

[29] *Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze, Dz.U. 2002, Nr 130, poz. 1112.*

[30] Art. 39, *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, Dz.U. 2016, poz. 904.*

Ten sam projekt dokumentu określa katalog służb i formacji, które mogłyby nadzorować egzekwowanie prawa w przypadku jego łamania. Zniszczyć, unieruchomić bądź przejąć kontrolę nad lotem BSP może:

- Policja,
- Straż Graniczna,
- Biuro Ochrony Rządu,
- Agencja Bezpieczeństwa Wewnętrznego,
- Agencja Wywiadu,
- Centralne Biuro Antykorupcyjne,
- Służba Kontrwywiadu Wojskowego,
- Służba Wywiadu Wojskowego,
- Służba Celna,
- Służba Więzienna
- żołnierze Żandarmerii Wojskowej i Sił Zbrojnych
- pracownicy specjalistycznych uzbrojonych formacji ochronnych[31].

Lista ta jest nieznacznie mniejsza w przypadku imprez masowych, a siły zbrojne RP maja prawo do działań tego typu w przypadku naruszania przez urządzenie i jego operatora stref zastrzeżonych. Wszystko zależy oczywiście od tzw. zimnej krwi funkcjonariuszy, ale istnieją duże szanse na pełne dramatyzmu artykuły w tabloidach piętnujące „nadgorliwych" obrońców prawa niszczących zabawki dzieciom. Jest to tym bardziej prawdopodobne, iż lot drona kierowanego przez niewprawnego operatora może budzić wątpliwości u postronnych obserwatorów. W kontekście powtarzających się jednak incydentów w okolicach lotnisk oraz zgłaszanych naruszeń stref zakazanych dotyczących najważniejszych osób i instytucji w państwie działania tego typu należy uznać za uprawnione. Nie dotarłem do tej pory do opisu użycia drona jako narzędzia zamachu, ale poprawiające się szybko charakterystyki osiągów tych urządzeń predestynują je do zastosowań terrorystycznych. Wydawało sie przez chwilę, że to siły porządkowe użyły sterowanej, latającej bomby do unieszkodliwienia „snajpera" w Dallas[32], ale okazało się, że wykorzystano urządzenie naziemne, które pozwoliło dostarczyć ładunek wybuchowy

[31] *Ibidem*.

[32] W nocy 8 lipca, doszło przy okazji demonstracji potępiającej brutalność białych funkcjonariuszy policji wobec czarnoskórych zatrzymanych do ataku na funkcjonariuszy policji w Dallas. Snajper (lub kilku sprawców) zabił 5 i ranił kolejnych kilku (od 6 do 9) policjantów. Po wymianie ognia z policjantami sprawca został zabity. por. *Snajperski ostrzał w Dallas. Napastnik chciał wymordować białych policjantów*, http://www.rmf24.pl (dostęp: 12.07.2016).

blisko przestępcy[33]. Jak bardzo wrażliwy na wszelkie, nawet niezamierzone zakłócenia jest cały funkcjonujący dzisiaj system lotnictwa cywilnego świadczyć może „współzawiniona" przez obce oprogramowanie katastrofa lotnicza w Madrycie w 2008. Osłabiony przez działanie tzw. trojana system bezpieczeństwa nie zareagował na wysyłane z samolotu informacje o awarii, co doprowadziło do śmierci 154 osób[34]. Zamach w Dallas po raz kolejny pokazuje użyteczność nowoczesnych technologii w zwalczaniu zagrożeń dla porządku publicznego. W tej części artykułu udało się odpowiedzieć na zadane wcześniej kolejne z pytań badawczych. Polskie państwo zauważyło potencjał zagrożeń, jaki niesie ze sobą użycie dronów w celach terrorystycznych. Przygotowane na tą okoliczność prawodawstwo umożliwia sprawne reagowanie przez przeznaczone do tego agendy państwa, dając obywatelom większe poczucie bezpieczeństwa.

Zakończenie

Jeszcze niecałe 200 lat temu, informacje Europy do obu Ameryk płynęły ok. 6 tygodni. Transmisje z zamachu na WTC 11 czerwca 2001 roku zaczęły się ok. 15 minut po uderzeniu pierwszego samolotu, a atak na drugą wieżę można już było oglądać na niemal całym świecie „na żywo"[35]. Nie inaczej jest dzisiaj. Liczne telewizje informacyjne rywalizują ze sobą, o to która z nich przekaże informację o zamachach, wypadkach i katastrofach najszybciej, najdrastyczniej i najskuteczniej. W obliczu wyścigu z czasem i konkurencją we współczesnych mediach często brakuje weryfikacji doniesień, czy też innych elementów właściwych dla profesjonalnego i odpowiedzialnego dziennikarstwa. Sensacyjne informacje wypierają inne przekazy, ponieważ audytorium odbiorców oczekuje „prawdziwego" obrazu rzeczywistości. Nic więc dziwnego, że we współczesnym świecie o wiele więcej uwagi przywiązujemy do nie tak popularnego w końcu zjawiska cyberterroryzmu, co do mogącego nas statystycznie spotkać o wiele bardziej prawdopodobnie przestępstwa w Internecie[36]. To przecież tam odbywa się nieustanne polowanie na nasze hasła

[33] D. Beres *This Is The Robot Dallas Police Used To Kill Shooting Suspect*, źródło: http://www.huffingtonpost.com (dostęp: 12.07.2016).

[34] R. Heickerö, *Cyber Terrorism: Electronic Jihad*, „Strategic Analysis" 2014, vol. 38, no.4, s 556.

[35] P. Wojtunik, J. Bartoszek, G. Biskupska, *Strategie i cele wykorzystywania mediów przez organizacje terrorystyczne*, [w:] *Polityka medialna instytucji państwowych w obszarze zagrożeń terrorystycznych. Materiały z II edycji międzynarodowej konferencji z cyklu Przeciwdziałanie terroryzmowi. Warszawa, 18 listopada 2008 r.*, Warszawa 2009, s. 10.

[36] por. Y. Jewkes , M. Yar , *Introduction: the Internet, cybercrime and the challenges of the twentyfirst century*, [w:] *Handbook of Internet Crime*, red. Y. Jewkes , M. Yar , London 2010, s. 4-7.

dostępu, dane osobowe, czy choćby informacje o naszych internetowych preferencjach zakupowych. ONZ prognozuje, że już w 2020 roku trudno będzie o przestępstwo nie powiązane w żaden sposób ze sferą Internetu[37].

Przerażeni cyberdżihadystami zapominamy też o terrorystach działających w imieniu, czy też na zamówienie legalnych rządów. Potwierdzono tego typu aktywność Północnej Korei[38], Chin, a tajemnicą poliszynela są działający na zlecenie Rosji sprawcy ataków na infrastrukturę krytyczną Ukrainy[39]. Również do Rosji prowadzą ślady najnowszej afery związanej z ujawnieniem potencjalnych nadużyć w sztabie Partii Demokratycznej w USA[40]. Ta sama cyberprzestrzeń stwarza zagrożenia dla krajów niedemokratycznych, które nie zawsze są w stanie zapanować nad jej zawartością. Satelity i Facebook jawią się notablom w Iranie jako narzędzia „miękkiej wojny"[41] Epatowani na co dzień mrożącymi krew w żyłach obrazami i relacjami przejmujemy wizję świata złego i zagrażającego nam, nie zauważając, że przyjmujemy tylko jedną z jego sztucznych kreacji, która przywiąże nas do nadawców informacji i ew. sprzedawców/promotorów kolejnych metod na zapewnienie nam bezpieczeństwa. Te same media utrudniają czasami działania służb ujawniając zbyt wiele szczegółów ich działań, a czasem same biorą na siebie rolę śledczych[42].

Dostosowanie miast do zagrożeń terrorystycznych otwiera także szeroką drogę do zleceń dla szeroko rozumianego sektora budowlanego, z którego niewątpliwie wygeneruje się specjalistyczna odnoga budownictwa (dla) bezpieczeństwa. Takie są nasze czasy i zagrożenia im towarzyszące, co zmusza nas do uwzględniania ich

[37] *Comprehensive Study on Cybercrime, Draft, February 2013*, United Nations Office on Drugs and Crime, New York 2013, s. 4-50, por także S. Tripathi, *Cyber: Also a Domain of War and Terror*, „Strategic Analysis" 2015, vol. 39, issue1, s. 1-2.

[38] R. Heickerö, *Cyber Terrorism…*, s 556.

[39] Taką informację udostępniła telewizja CNN powołując się na wypowiedź wiceszefowej Departamentu Energii USA Elizabeth Sherwood-Randall. Por także: *USA unikają oficjalnego oskarżenia Rosji o atak hakerski na Ukrainę*, źródło: http://biznesalert.pl (dostęp: 21.07.2016).

[40] A. Phillips, *Clinton campaign manager: Russians leaked Democrats' emails to help Donald Trump*, źródło: https://www.washingtonpost.com (dostęp: 25.07.2016).

[41] Tak wypowiadał się Minister Spraw Wewnętrznych Iranu –Mostafa Najjar, a szef Irańskich Strażników Rewolucji - Abdollah Araghi zapewniał, że jego formacja posiada juz narzędzia do walki z tego typu zagrożeniami , które mogą być groźniejsze niż wojna fizyczna. Zob. J.A. Lewis, *National Perception of Cyber Threats,* „Strategic Analysis" 2014, vol. 38, issue 4, s.574.

[42] Po zamachu w Bostonie w 2013 roku internauci i media ochoczo typowali potencjalnych sprawców, publikując ich wizerunki w ogólnokrajowych/globalnych (?) mediach. zob. także B. Węgliński, *Analiza wybranych aktów terrorystycznych w roku 2013. Odrodzenie Al-Kaidy?*, „Rocznik Bezpieczeństwa Międzynarodowego" 2014, vol.8, nr 1, s.186-187.

w codziennych przedsięwzięciach, jakie podejmujemy, a listy gończe z podobiznami domniemanych terrorystów możemy zobaczyć w mediach, czy na słupach i wystawach sklepowych.

Podsumowując, udało mi się potwierdzić postawioną w tekście hipotezę. Współcześni terroryści zarówno korzystają z nowoczesnych rozwiązań technologicznych jak i organizacyjnych. W profesjonalny sposób prowadzone media społecznościowe, a także inne cyfrowe kanały przekazu to potwierdzają. Obecność w strukturach organizacji terrorystycznych wykwalifikowanych specjalistów z zakresu dziennikarstwa cyfrowego, logistyki czy choćby budowy ładunków i planowania nie dają cienia wątpliwości, co do procesu profesjonalizacji we współczesnym terroryzmie. Można mówić wręcz o ich korporacyjnym modelu działania. Zaskakujący jest jednoczesny, zauważalny w ostatnich latach trend do delegowania części działań na poziom jak najbardziej "amatorski" - przykładem tego będzie aktywność "samotnych wilków". Nie zmienia to faktu, że "amatorów" motywuje do akcji działalność profesjonalistów. Pozytywna jest także odpowiedź na pytanie o stopień przygotowania do użycia przez terrorystów dronów i innych BSL. Na poziomie prawodawstwa problem jest rozstrzygnięty, a rozwojowi tej technologii towarzyszą badania nad wytworzeniem urządzeń je neutralizujących.

Należy oczywiście założyć, że wraz z dalszym rozwojem cywilizacji i technologii, terroryści będą je adaptowali do swoich celów na podobnych zasadach, jak robią to już dziś. Ważne jest jedynie to, aby służbom zwalczającym terrorystów udawało się być zawsze krok przed nimi.

Bibliografia

„Nienawiść do ludzi". Kolega ze szpitala psychiatrycznego o zamachowcu, źródło: http://www.tvn24.pl (dostęp: 25.07.2016).

Alshech E., *Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad*, „Inquiry & Analysis Series Report" 2007, No. 329.

Babecki M., *Funkcje epizodycznych gier internetowych w procesach modelowania wirtualnego wizerunku terrorysty i terroryzmu. Analiza aspektowa*, „Media – Kultura – Komunikacja Społeczna" 2013, nr 9.

Bennett D., *Exploring the impact of an evolving war and terror blogosphere on traditional media coverage of conflict*, „Media, War & Conflict " 2013, vol. 6, issue 1.

Beres D., *This Is The Robot Dallas Police Used To Kill Shooting Suspect*, źródło: http://www.huffingtonpost.com (dostęp: 12.07.2016).

Bogusz M., *Ejército Zapatista de Liberación Nacional - wirtualna partyzantka*, [w:] *Terroryzm w medialnym obrazie świata*, red. K. Liedel, S. Mocek, Warszawa 2010.

Bolechów B., *„Baza" w sieci. Wykorzystanie Internetu przez Al-Kaidę i jej zwolenników*, [w:] *Terroryzm w medialnym obrazie świata*, pod red. K. Liedel i S. Mocek, Warszawa 2010.

Bolechów B., *Terroryzm w świecie podwubiegunowym*, Toruń, 2002.

Brzeziński Z., *Kłopoty dobrego hegemona*, źródło: http://szukaj.wyborcza.pl (dostęp: 06.05.2016).

Cockburn P., *Państwo Islamskie*, Warszawa 2015.

Comprehensive Study on Cybercrime, Draft, February 2013, United Nations Office on Drugs and Crime, New York 2013

Danitz T., Strobel W. P., *Networking dissent: Cyber activists use the Internet to promote Democracy in Burma*, [w:] *Networks and Netwars*. red. Arquila J., Ronfeldt D., Santa Monica 2001.

Denning D. E., *Terror`s Web: How the Internet Is Transforming Terrorism*, [w:] *Handbook of Internet Crime*, red. Y. Jewkes, M. Yar, London 2010.

Dżihadysta-gej? Zemsta hakera robi furorę, źródło: http://tvn24bis.pl (dostęp: 22. 07.2016).

Ferran L., Brown E., Meek J. G., Fishel J., *Jihadists' Computers '80 Percent' Full of Porn, Ex-Official Says*, źródło: http://abcnews.go.com (dostęp: 21.07.2016).

Francja: kolejny atak islamskiego radykała? Auto wjeżdża w tłum przechodniów w Nantes, źródło: www.polskieradio.pl (dostęp: 17.07.2016).

Francuska telewizja ofiarą cyberataku. Hakerzy podają się za dżihadystów, źródło: http://www.newsweek.pl (dostęp: 22.07.2016).

Heickerö R., *Cyber Terrorism: Electronic Jihad*, „Strategic Analysis" 2014, vol. 38, no.4.

Hoffman B., *Foreword*, [w:] G. Weimann, *Terror on the Internet. The New Arena, the New Challenges*, Washington 2006.

Jewkes Y., Yar M., *Introduction: the Internet, cybercrime and the challenges of the twentyfirst century*, [w:] *Handbook of Internet Crime*, red. Y. Jewkes, M. Yar , London 2010.

Lake E., *Al Qaeda Breach Called 'Serious' but 'Reparable'*, źródło: www.nysun.com (dostęp: 19.07.2016).

Lewis J. A., *National Perception of Cyber Threats,* „Strategic Analysis" 2014, vol. 38, issue 4.

Phillips A., *Clinton campaign manager: Russians leaked Democrats' emails to help Donald Trump*, źródło: https://www.washingtonpost.com (dostęp: 25.07.2016).

Ronfeldt D., Arquilla J., *What next for networks and netwars?*, [w:] *Networks and Netwars*. red. Arquila J., Ronfeldt D, Santa Monica 2001.

Schulzke M., *Being a terrorist: Video game simulations of the other side of the War on Terror*, „Media, War & Conflict" 2013, vol. 6, issue 3.

Schwarz E., *Prescription drones: On the techno-biopolitical regimes of contemporary 'ethical killing'*, „Security Dialogue" 2016, vol. 47(I).

Sheets P., Rowling C. M., Jones T. M., *The view from above (and below): A comparison of American, British, and Arab news coverage of US drones*, „Media, War & Conflict" 2015. vol. 8, issue 3.

Snajperski ostrzał w Dallas. Napastnik chciał wymordować białych policjantów, http://www.rmf24.pl (dostęp: 12.07.2016).

Tripathi S., *Cyber: Also a Domain of War and Terror*, „Strategic Analysis" 2015, vol. 39, issue1

USA unikają oficjalnego oskarżenia Rosji o atak hakerski na Ukrainę, źródło: http://biznesalert.pl (dostęp: 21.07.2016).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, Dz.U. 2016, poz. 904.

Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze, Dz.U. 2002, Nr 130, poz. 1112.

Weimann G., *Terror on the Internet. The New Arena, the New Challenges*, Washington 2006.

Węgliński B., *Analiza wybranych aktów terrorystycznych w roku 2013. Odrodzenie Al-Kaidy?,* „Rocznik Bezpieczeństwa Międzynarodowego" 2014, vol.8, nr 1.

Wojtunik P., Bartoszek J., Biskupska G., *Strategie i cele wykorzystywania mediów przez organizacje terrorystyczne*, [w:] *Polityka medialna instytucji państwowych w obszarze zagrożeń terrorystycznych. Materiały z II edycji międzynarodowej konferencji z cyklu Przeciwdziałanie terroryzmowi. Warszawa, 18 listopada 2008 r.*, Warszawa 2009.

Zamach w Nicei. Francuska policja zatrzymała trzy osoby, źródło: http://wiadomosci.gazeta.pl (dostęp: 17.07.2016).