https://doi.org/10.18778/8331-316-0.03

Bartosz Kurowski
0009-0008-9855-9318

Jaką rolę w działaniu terrorystów odgrywa technologia i jaką może odegrać w przyszłości?

Abstrakt
Celem artykułu jest podkreślenie znaczenia współczesnej technologii w działalności Państwa Islamskiego, które jako jedno z pierwszych ugrupowań terrorystycznych na świecie dostrzegło ogromny potencjał w mediach, jako gotowych narzędziach ułatwiających szerzenie propagandy czy wzbudzanie przerażenia wśród społeczeństwa. Coraz częściej pojawiające się zjawisko „elektronicznego dżihadu" – polegające na pozyskiwaniu nowych bojowników przy wykorzystaniu internetu – czy szerzenie dezinformacji na obszarach kontrolowanych przez terrorystów za pomocą gazet i ulotek propagandowych, to jedynie niewielki zarys całej machiny propagandowej dżihadystów. Szczególny priorytet został więc położony na wskazanie struktury medialnej, produktów propagandy, a także celów Państwa Islamskiego, które na przestrzeni lat zdają się ewoluować wraz ze zmieniającym się otoczeniem i postępującą globalizacją. W związku z tym współczesny terroryzm, coraz częściej określany mianem cyberterroryzmu, staje się jednocześnie zupełnie nowym zagrożeniem i wyzwaniem dla aparatu bezpieczeństwa.

Słowa kluczowe: Państwo Islamskie, współczesne media, propaganda, cyberprzestępczość, terroryzm

Wstęp

Właściwie już od początku XXI wieku społeczeństwo jest świadkiem imponującego skoku technologicznego, który opiera się przede wszystkim na rozwoju usług internetowych czy technologii dostępu mobilnego. Tak duże przemiany zrewolucjonizowały nie tylko media społecznościowe, ale nadały dyskursowi publicznemu zupełnie innej dynamiki. Nie pozostały również niezauważone

przez grupy terrorystyczne. Oczywiście technologia to nie tylko internet czy nowoczesne platformy multimedialne, a sam proces wytwarzania lub przetwarzania jakiegoś dobra lub informacji, od techniki malowania i projektowania, aż po technologię budowy maszyn.

W niniejszym artykule szczególny nacisk został położony przede wszystkim na wskazaniu, jaką rolę odgrywa i może odegrać w przyszłości wykorzystanie nowych technologii, a także technologii cyfrowej przez ISIS[1]. To właśnie Państwo Islamskie stało się swojego rodzaju prekursorem i pierwszą grupą terrorystyczną, która zaczęła wykorzystywać media społecznościowe czy komunikatory internetowe jako podstawowe narzędzia swojej szeroko zakrojonej działalności. W związku z tym, ramy czasowe przyjęte w niniejszym artykule to lata 2014–2016, kiedy po ogłoszeniu kalifatu na terenach Iraku i Syrii 29 czerwca 2014 roku Państwo Islamskie zaczęło szczególnie prężnie działać w przestrzeni medialnej[2]. Rok 2016 stanowi natomiast symboliczną datę pewnego zwrotu w rozważaniach nad cyberterroryzmem – po atakach na lotnisko w Brukseli – na które dżihadyści przygotowywali się szczególnie poprzez wykorzystanie nowych technologii.

Podstawowym problemem badawczym, który został podjęty w artykule jest wskazanie, iż współczesne media coraz częściej stają się głównym narzędziem wykorzystywanym przez ISIS do szerzenia propagandy i pozyskiwania nowych funduszy czy bojowników.

Hipotezą pracy badawczej jest stwierdzenie, że działalność terrorystyczna – w związku z globalizacją i cyfryzacją – coraz częściej odbywa się w przestrzeni internetowej, stanowiąc jednocześnie coraz większe wyzwanie dla służb bezpieczeństwa na całym świecie, nabierając tym samym wymiaru globalnego, opartego o tzw. nowe media.

Aby w pełni udowodnić postawioną hipotezę, autor stawia następujące pytania badawcze: Jak wygląda struktura medialna Państwa Islamskiego i podejmowane przez terrorystów działania psychologiczne? Jakie są cele i narzędzia propagandy ISIS? W jaki sposób nowe technologie przyczyniają się do ułatwienia komunikacji, cyberprzestępczości i pozyskiwania funduszy przez terrorystów?

---

[1] Skrót ISIS pochodzi od pełnej nazwy Islamic State of Iraq and Syria (Państwo Islamskie w Iraku i Syrii). W poniższej pracy zdecydowałem się wykorzystywać wiele skrótów na określenie Państwa Islamskiego, które na przestrzeni całej działalności terrorystów ulegały pewnym zmianom np. ISIL (Islamic State of Iraq and Lewant), ISI (Islamic State of Iraq) czy IS (Islamic State).

[2] M. M. Dziekan, R. Bania, K. Zdulski, *Państwo Islamskie – powstanie i działalność samozwańczego kalifatu*, 23.02.2020, https://histmag.org/Panstwo-Islamskie-powstanie-i-dzialalnosc-samozwanczego-kalifatu-20228 (dostęp: 13.07.2023).

By w sposób jak najbardziej spójny i przejrzysty przedstawić omawiane zagadnienie, praca została podzielona na trzy części. Część pierwsza opisuje organy medialne Państwa Islamskiego, a także podkreśla ich znaczenie dla szerzenia propagandy i chaosu na terenach okupowanych przez dżihadystów. Ponadto, autor przybliża także termin elektronicznego dżihadu, będącego nowoczesną formą rekrutacji bojowników.

W części drugiej opisane zostały cztery podstawowe cele ISIS, opracowane przez polskich badaczy – Tomasza Grzyba i Rafała Zgryziewicza – na podstawie analizy działalności Państwa Islamskiego. Autor podkreśla szczególne znaczenie tzw. Linii Wysiłku, na których opiera się współczesna strategia działalności terrorystów w sieci, odwołując się tym samym do konkretnych korzyści płynących dla dżihadystów z zastosowania elementu zastraszania czy informowania.

Ostatnia część skupia się przede wszystkim na analizie przypadków cyberprzestępczości, jakiej dopuszcza się Państwo Islamskie po zamachach na lotnisko w Brukseli w 2016 roku. Wydarzenie to stanowiło element zwrotny w rozważaniach nad działalnością grup terrorystycznych w sieci, o czym szczególnie przekonały się służby bezpieczeństwa zupełnie nieprzygotowane na tak rozwiniętą sieć medialną ISIS.

Praca opiera się przede wszystkim na metodzie analizy przypadku (*case study*) – jako badanie jakościowe polegające na analizie i ocenie wykorzystania nowych technologii przez Państwo Islamskie w XXI wieku. Dogłębna analiza pozwala stwierdzić, iż współczesne media coraz częściej stanowią najchętniej wykorzystywane przez terrorystów narzędzia do poszerzania swoich wpływów. Ponieważ temat artykułu w dużej mierze jest stosunkowo nowym zjawiskiem i porusza kwestię obecności dżihadystów w internecie, niezbędnym w niniejszej pracy było zastosowanie analizy treści źródeł dotyczących zagadnienia – w szczególności publikacji prasowych i internetowych, a także literaturze przedmiotu.

Struktura medialna i podejmowane przez Państwo Islamskie działania psychologiczne

Aby w pełni zrozumieć rolę nowoczesnych technologii w działalności terrorystów, niezbędne jest przedstawienie, jak bardzo rozbudowana i istotna jest struktura medialna Państwa Islamskiego. Działania dżihadystów, szczególnie na terenach przez nich zarządzanych, skupiają się bardzo często na walce informacyjnej bądź propagandowej. To właśnie w tym celu powstały takie organy jak Rada Medialna, Instytut Al-Furqan czy centrum medialne

Al-Hayat[3]. Wszystkie trzy przedsięwzięcia zaczęły funkcjonować w drugiej połowie 2014 roku w wyniku ogłoszenia przez Abu Bakra al-Bagdadiego powstania tzw. Państwa Islamskiego w Wielkim Meczecie w Mosulu. Powstanie IS (Islamic State) stało się momentem, w którym technologia i media zaczęły być wykorzystywane przez dżihadystów w bardziej profesjonalny sposób, a w ich szeregach pojawili się zagraniczni informatycy i tłumacze, dzięki którym propaganda okazywała się skuteczniejsza i trafiała do całego świata[4].

Rada Medialna ISI jest odpowiedzialna za działalność prasowo-informacyjną, ale także za nakreślanie sylwetki potencjalnych odbiorców i organizację operacji propagandowych[5]. Najbardziej charakterystycznym i popularnym działaniem Rady w ostatnich latach stało się prowadzenie tzw. elektronicznego dżihadu, czyli sposobu rekrutacji nowych bojowników (głównie z Europy) przy pomocy mediów społecznościowych[6]. Terroryści zamieszczają w internecie, w tym na różnych portalach społecznościowych, filmy czy posty, na których starają się ocieplić swój wizerunek, przedstawiając się na zdjęciach z popularnym kremem czekoladowym (Nutellą) czy małymi kotkami, jednocześnie opowiadając, jak dużą szansą i zaszczytem stał się dla nich wyjazd na „świętą wojnę" do Iraku czy Syrii i walka u boku „braci"[7]. W ten sposób wielu młodych muzułmanów z Europy, którzy nie widzą w swoim życiu perspektyw na przyszłość i nierzadko czują się wyalienowani ze społeczeństwa, ulegają manipulacji i wyjeżdżają na dżihad z nadzieją na lepsze życie, zasilając tym samym szeregi Państwa Islamskiego. Takie działania terrorystów określane są mianem działań psychologicznych, które w połączeniu z technologią cyfrową stanowią potężną broń w machinie propagandowej ISIS[8].

Jednak użycie technologii w procesie rekrutacji nowych bojowników online to jedno z wielu narzędzi jakimi dysponuje Rada Medialna, obok której stoi najstarszy organ medialny ISI – Instytut Al-Furqan. To właśnie jego zadaniem pozostaje przygotowywanie materiałów propagandowych takich jak plakaty,

---

3 H. Haniyeh, *Daesh's Organisational Structure*, Al Jazeera Center for Studies, 01.02.2017, http://studies.aljazeera.net/en/dossiers/decipheringdaeshoriginsimpactandfuture/2014/12/201412395930929444.html (dostęp: 30.03.2023).

4 M. Lakomy, *Internet w działalności tzw. Państwa Islamskiego: nowa jakość cyberdżihadyzmu?*, „Studia i Analizy" 2015, t. 38, s. 165–166.

5 K. Danielewicz (red.), *Państwo Islamskie (ISIS). Historia powstania i taktyka działania*, Napoleon V, Grojec 2019, s. 84.

6 H. Haniyeh, *Daesh's Organisational Structure*…

7 S. Campbell, *ISIS Using Kittens and Nutella to Lure Jihadi Wannabes*, „Mirror", 27.05.2016, http://www.mirror.co.uk/news/world-news/isis-using-kittens-nutella-lure-8061303 (dostęp: 30.03.2023).

8 K. Danielewicz (red.), *Państwo Islamskie*…, s. 84.

ulotki czy gazety, które następnie rozpowszechniane są na terenach okupowanych, wśród miejscowej ludności. Instytut Al-Furqan przy współpracy z dziennikiem arabskojęzycznym Al-Hayat – który posiada ok. kilkudziesięciu biur terenowych w Iraku i Syrii – zajmują się także produkcją i obróbką wszelkich materiałów wideo zamieszczanych przez Państwo Islamskie w sieci[9]. Warto także podkreślić, iż aby wszelkie materiały, zarówno prasowe jak i wideo, trafiały do jak największej liczby odbiorców na całym świecie, wydawane są w wielu językach, takich jak rosyjski, francuski czy angielski, a wśród najbardziej rozpoznawalnych pozostają magazyny „Dabiq", „Al-Kataib" czy „Rumiyah"[10].

Cel i narzędzia propagandy Państwa Islamskiego

Jak widać, struktura medialna IS jest bardzo rozbudowaną machiną, w której skład wchodzą tysiące bojowników, techników czy tłumaczy odpowiedzialnych za prawidłowe funkcjonowanie całego procesu działań psychologicznych stosowanych przez dżihadystów do osiągania konkretnych celów. Cele te, na podstawie działalności Państwa Islamskiego, zostały ściśle sprecyzowane przez polskich badaczy – doktora Tomasza Grzyba i Rafała Zgryziewicza i określone jako cztery główne Linie Wysiłku[11]:

- pozyskiwać wsparcie (*support*),
- jednoczyć (*unite*),
- przerażać (*frighten*),
- informować (*inform*).

Właściwie żaden z powyższych celów nie mógłby zostać spełniony nawet w najmniejszym stopniu, gdyby nie wykorzystanie współczesnych technologii i szybki przesył informacji, czy to za pomocą komunikacji bezpośredniej, jak przekazywanie ulotek, czy przy użyciu forów społecznościowych i blogosfery. Tym samym, wraz z rozwojem technologii, zaczęły zmieniać się cele i sposób działania Państwa Islamskiego[12].

O ile proces jednoczenia w pewnym stopniu wyjaśniłem w poprzednim punkcie, podając przykład „elektronicznego dżihadu", czyli rekrutacji nowych

[9] Ibidem, s. 84–85.

[10] A. Zelin, *A Clearinghouse for Jihādī Primary Source Material, Original Analysis, and Translation Service*, 2022, https://jihadology.net/ (dostęp: 30.03.2023).

[11] R. Zgryziewicz, J. Shaheen, T. Grzyb, S. Fahmy, *Daesh. Information Campaign and Its Influence – Executive Summary*, NATO StratCom COE, 15.12.2015, https://stratcomcoe.org/cuploads/pfiles/executive_summary_15-12-2015.pdf (dostęp: 30.03.2023).

[12] K. Danielewicz (red.), *Państwo Islamskie*…, s. 85.

bojowników online, o tyle w tym temacie należy podkreślić jeszcze jedną kwestię. W momencie, kiedy już potencjalny nowy dżihadysta zdecyduje się na dołączenie do Państwa Islamskiego, nierzadko zdarza się, że liderzy kalifatu, zamiast sprowadzać taką osobę do Iraku czy Syrii, wolą pozostawić ją w państwie europejskim jako swojego łącznika. Pozostają oni wtedy w kontakcie mailowym czy wymieniają się tweetami aż do momentu, kiedy taka osoba zostanie zmanipulowana do tego stopnia, że będzie mogła przeprowadzić atak terrorystyczny na miejscu[13]. Przywódcy Państwa Islamskiego szybko doszli do wniosku, że nie ma potrzeby wysyłać bojowników z Bliskiego Wschodu, aby przeprowadzali ataki na Zachodzie i ryzykować wykrycie ataku, skoro dzisiejsze technologie dają możliwość pozyskania nowych żołnierzy na miejscu, przy minimalnym zaangażowaniu.

Od razu widać tu olbrzymi skok technologiczny, jaki nastąpił w XXI wieku, a także łatwość, z jaką Państwu Islamskiemu udało się go wykorzystać w tak szybkim czasie, aby móc zjednoczyć swoich zwolenników niemal w każdym miejscu na świecie[14].

Ciekawszą kwestią pozostaje natomiast pozyskiwanie wszelkiego wsparcia przez ISIS. Mówiąc o wsparciu, należy wymienić zarówno pozyskiwanie nowych bojowników, ale także powszechną akceptację wśród społeczności lokalnej, zamieszkującej tereny kontrolowane przez Państwo Islamskie. W tym celu dżihadyści skupiają się na kontroli struktury regionalnej mediów. Od organizowania kampanii propagandowych, mających na celu przedstawiać telewizję satelitarną jako szkodliwą i zagrażającą religijnym wartościom, aż po promowanie telewizji lokalnej, będącej pod patronatem Rady Medialnej ISI[15]. Tym samym zdają się pomocne kampanie billboardowe czy rozwieszanie plakatów i wręczanie ulotek przedstawiających dżihadystów jako walecznych i nieustraszonych bohaterów walczących o swój kraj i wiarę[16]. Coraz częściej pojawiają się także – w szczególności na obszarach wiejskich – kioski i mobilne punkty informacyjne, które poprzez sprzedaż takich magazynów jak „Dabiq" czy „Rumiyah", a także rozpowszechnianie transmisji z przemówień liderów Państwa Islamskiego mają zachęcać miejscową ludność do współpracy i brania udziału w czynnym dżihadzie przeciwko państwom zachodnim[17].

---

[13] P. Engel, *The Orlando Attack Exposes the Biggest Blind Spot in the US Strategy Against ISIS*, Business Insider, 19.06.2019, https://businessinsider.com.pl/international/the-orlando-attack-exposes-the-biggest-blind-spot-in-the-us-strategy-against-isis/phv4zht (dostęp: 30.03.2023).

[14] R. Zgryziewicz, J. Shaheen, T. Grzyb, S. Fahmy, *Daesh*…

[15] K. Danielewicz (red.), *Państwo Islamskie*…, s. 73–74.

[16] P. Engel, *The Orlando Attack*…

[17] R. Zgryziewicz, J. Shaheen, T. Grzyb, S. Fahmy, *Daesh*…

Ostatnim z celów, które zostały przedstawione w badaniach, a który należy wyjaśnić jest wywoływanie przerażenia. Analizując wiele tekstów i historię działalności ISIS w mediach społecznościowych można dojść do wniosku, że to właśnie próby zastraszania, wzbudzania strachu czy siania paniki wśród społeczności międzynarodowej były pierwszymi celami przyświecającymi terrorystom.

Już sam Abu Musab az-Zarkawi – inicjator wojny sunnicko-szyickiej, pierwszy dowódca Al'Kaidy w Iraku, a także główny twórca ISIS – doceniał rolę oddziaływania współczesnych mediów i nowych technologii do osiągania swoich celów[18]. To właśnie Zarkawi był odpowiedzialny za nagranie i udostępnienie w sieci w 2004 roku krótkiego filmu z egzekucji amerykańskiego mechanika Nicka Berga. Na ok. pięciominutowym wideo można było zobaczyć klęczącego, związanego mężczyznę w pomarańczowym kombinezonie, za którym stało pięciu zamaskowanych dżihadystów. Jeden z nich przeczytał wiadomość, z której wynikało, że egzekucja jest zemstą za nadużycia wojsk amerykańskich wobec zakładników będących członkami ISI, po czym krzyknął: „Allah akbar" i odciął zakładnikowi głowę. W toku śledztwa władzom amerykańskim udało się ustalić, iż ofiarą rzeczywiście był Nick Berg, a osobą wykonującą egzekucję był sam Abu Musab az-Zarkawi[19]. Było to pierwsze nagranie z przeprowadzonej przez członków Państwa Islamskiego egzekucji, które zostało udostępnione w internecie opinii publicznej. Z jednej strony tak brutalne i bezpośrednie wideo wzbudziło niebywałą sensację i zainteresowanie, z drugiej jednak strony za takim działaniem kryła się bardzo sprecyzowana taktyka. Szybko okazało się bowiem, że wśród opinii publicznej film ten zaczął wzbudzać uczucie strachu i niepewności. Ludzie na całym świecie (przede wszystkim jednak w Stanach Zjednoczonych) zaczęli bać się o własne życie[20].

Należy także pamiętać o tym, iż wideo zostało opublikowane w internecie w 2004 roku, a więc trzy lata po wydarzeniach związanych z atakiem na World Trade Center i dwa lata po wygłoszeniu orędzia prezydenta Stanów Zjednoczonych George'a W. Busha, w którym wymienił trzy państwa należące do tzw. osi zła, a wśród których znalazł się Irak, jako siedziba grup terrorystycznych[21]. Był to więc okres, w którym takie organizacje jak ISI czy Al-Ka'ida

[18] K. Danielewicz (red.), *Państwo Islamskie*…, s. 23–25.

[19] B. Whitaker, L. Harding, *American Beheaded in Revenge for Torture*, „The Guardian", 12.05.2004, https://www.theguardian.com/world/2004/may/12/iraq.alqaida (dostęp: 30.03.2023).

[20] K. Danielewicz (red.), *Państwo Islamskie*…, s. 24.

[21] The United States Capitol, *President Delivers State of the Union Address*, 29.01.2002, https://georgewbush-whitehouse.archives.gov/news/releases/2002/01/print/20020129-11.html (dostęp: 30.03.2023).

wzbudzały wśród ludzi przerażenie czy strach, i dokładnie na tym miała opierać się ich taktyka. Zarkawi, poprzez udostępnienie nagrania z egzekucji w mediach społecznościowych, pokazał całemu światu (a dokładnie ludności cywilnej), że dżihadyści nie cofną się przed niczym, a ich ofiarą może zostać dosłownie każdy.

Po dziesięciu latach narracja Państwa Islamskiego właściwie nie uległa zmianie, natomiast znacznie rozwinęła się technika i sposób, w jaki przedstawiają przekaz. Film opublikowany w sieci we wrześniu 2014 roku pt. *Flames of War: Fighting Has Just Begun* został uznany za sztandarowy projekt ISIS. Jednocześnie jest idealnym przykładem tego, jak wraz z rozwojem współczesnych technologii ewoluuje działalność terrorystyczna[22]. Trwające 55 minut wideo jest relacją z zajęcia przez dżihadystów bazy 17. dywizji armii syryjskiej. Na nagraniu można zauważyć bawiących się bojowników, już po zajęciu bazy, a także syryjskich jeńców, którzy kopią swoje groby, a po kilku minutach zostają przy nich rozstrzelani. Cały film jest utrzymany w bardzo nowoczesnej konwencji, a do nagrań zostały użyte kamery GoPro, aby utrzymać widzów w pewnym poczuciu interaktywności. Sam operator kamery bierze czynny udział w masowej egzekucji, kadrując dokładnie każde spojrzenie czy gest – rodem z hollywoodzkich produkcji, a film zostaje przedstawiony w języku angielskim[23]. Wszystkie te zabiegi – idealnego wykadrowania scen egzekucji, stosowania techniki *slow motion*, dynamicznego montażu czy użycia języka angielskiego, mają na celu oddać przekaz jak najrealniej, a co za tym idzie sprawić, aby widz odczuwał każdą scenę jakby tam był, a więc aby odczuwał obrzydzenie, strach, poczucie lęku, niepewność, a na końcu przerażenie. W filmie pojawiają się także wstawki z przemówień George'a W. Busha po zakończeniu działań bojowych w Iraku, w których mówi, że „Stany Zjednoczone i nasi sojusznicy zwyciężyli", po czym głos operatora zza kamery stwierdza: „Zostaliście okłamani, ponieważ to był dopiero początek"[24].

Ten przykład pokazuje, jak odpowiednio zastosowana poprzez użycie stosownych technik montażowych manipulacja może przynieść oczekiwane skutki, a więc wzbudzić poczucie strachu, ale także wątpliwości, czy na pewno jesteśmy odpowiednio chronieni przez organy bezpieczeństwa. W tym miejscu należy dodać, że taka manipulacja ma zadziałać również w drugą stronę, a więc sprawić, abyśmy zaczęli odczuwać negatywne emocje wobec muzułmańskich mniejszości mieszkających w naszym otoczeniu. W ten sposób moglibyśmy

[22] K. Danielewicz (red.), *Państwo Islamskie*…, s. 87.

[23] K. Ruble, *Islamic State Documentary Style Video Says the „Flames of War" Have Just Begun*, „Vice", 19.09.2014, https://www.vice.com/en/article/d3jjga/islamic-state-documentary-style-video-says-the-flames-of-war-have-just-begun (dostęp: 30.03.2023).

[24] Ibidem.

zacząć stosować wobec nich przemoc, a także zacząć ich dyskryminować, jednocześnie się izolując, co doprowadziłoby do ich alienacji. W efekcie mniejszości te stałyby się podatne na manipulację ze strony terrorystów, którzy tylko czekają, aby zradykalizować kolejne europejskie społeczności[25].

Nie można nie zgodzić się, iż rzeczywiście taka taktyka grup terrorystycznych przynosi odpowiednie skutki, począwszy od faktu, że terroryści wciąż otrzymują wsparcie w postaci nowych bojowników z Europy i innych części świata, aż po wzbudzanie lęku i przerażenia. Przeciętna osoba przeglądająca wiadomości w internecie, która natknie się na film z egzekucji bądź zamachu samobójczego, z pewnością stwierdzi, iż Państwo Islamskie jest nieobliczalne i niedające się powstrzymać, skoro od tylu lat prowadzi skuteczne działania zbrojne na całym świecie, co jednak nie do końca okazuje się prawdą, jeśli przyjrzeć się bliżej sukcesom odnoszonym przez zachodnie wojska na terenach Iraku czy Syrii[26]. W tym kontekście nie ma to jednak żadnego znaczenia, ponieważ cel, jakim jest przekaz informacji i wzbudzenie lęku został osiągnięty.

Komunikacja, cyberprzestępczość i pozyskiwanie funduszy w użyciu nowych technologii

W poprzedniej części w dość szczegółowy sposób przedstawiłem cztery Linie Wysiłku, a więc najważniejsze cele, jakie przyświecają IS przy wykorzystaniu współczesnych technologii – jak się jednak okazuje nie są to jedyne cele. Obecna działalność terrorystyczna rzeczywiście w dużej mierze opiera się na propagandzie i budowaniu pozytywnego wizerunku, który ma służyć pozyskiwaniu nowych sojuszników. Nie mogłoby to jednak przynosić nawet najmniejszych efektów bez odpowiedniej komunikacji, a przede wszystkim środków finansowych, do pozyskiwania których Państwo Islamskie również używa współczesnej cybertechnologii.

Właściwie już od momentu, kiedy w przestrzeni publicznej zaczęły pojawiać się pierwsze smartfony, organy bezpieczeństwa zdawały sobie sprawę, że są one używane przez grupy terrorystyczne w celu komunikacji. Nie było jednak na to żadnych dowodów lub były one niewystarczające, aby móc się tej kwestii przyjrzeć bliżej – aż do momentu przeprowadzenia śledztwa po zamachach ISIS na lotnisku w Brukseli w 2016 roku[27]. W toku postępowania udało się

[25] K. Danielewicz (red.), *Państwo Islamskie*…, s. 95.
[26] Ibidem, s. 93.
[27] Ibidem, s. 99–101.

zdobyć laptop, który posłużył zamachowcom do komunikacji i zaplanowania ataku, jednak zanim udało się to potwierdzić, belgijscy technicy napotkali wiele przeszkód. Okazało się, że terroryści usunęli większość zawartości twardego dysku, a pozostała część danych została zabezpieczona za pomocą powszechnego programu szyfrującego. Ponadto zamachowcy użyli oprogramowania pozwalającego zachować anonimowość i usunąć wszelką działalność w sieci[28]. Ostatecznie śledczym udało się odzyskać jedynie pewną część danych z laptopa, lecz to wystarczyło, aby zrozumieć, jak wysoce rozwinięta jest działalność grup terrorystycznych na płaszczyźnie posługiwania się nowoczesną technologią. Na jaw wyszło, że na laptopie były zapisane informacje i plany dotyczące zamachu w Brukseli, który – jak się okazało – został zaplanowany już o wiele wcześniej[29]. Dodatkowo na dysku znajdowały się filmy propagandowe dotyczące przemówień Osamy bin Ladena, a także pewne dane świadczące o zainteresowaniu terrorystów obiektami jądrowymi czy TATP, który został użyty podczas ataku[30]. To co jednak najbardziej zszokowało śledczych, to plik o nazwie „cele", w którym znajdowały się podpliki: Groupe Omar, Groupe Francais, Groupe Iraqiens, Groupe Metro, Groupe Schiphol, które prawdopodobnie odnosiły się m.in. do zamachów na kawiarnię w Paryżu przez grupę Abu Omara, atak terrorystyczny na dyskotekę Bataclan w Paryżu, czy ataki samobójcze na Stade de France[31].

Dopiero ta sytuacja pokazała służbom bezpieczeństwa w Brukseli, ale i na całym świecie, że właśnie są świadkami wejścia na zupełnie inny poziom walki z terroryzmem. O ile Państwo Islamskie nadal używa tradycyjnych form przekazu w Iraku czy Syrii, takich jak billboardy, gazety czy ulotki, o tyle okazuje się, że jest to jedynie pewnego rodzaju zasłona dla ich dzisiejszej działalności terrorystycznej w przestrzeni międzynarodowej. Państwo Islamskie nie ogranicza się już jedynie do publikowania w sieci filmów z egzekucji czy działalności na forach internetowych. Sytuacja w Brukseli pokazała, że dżihadyści posiadają komórki świetnie wyszkolonych techników i informatyków właściwie w każdym miejscu na świecie[32]. Okazuje się, że jeden laptop zawierał w sobie tyle wartościowych danych, iż przejęcie go w odpowiednim czasie mogło

[28] P. Cruickshank, *Laptop Yields Revelations on Brussels Attacks*, „KSHB", 24.01.2017, https://www.kshb.com/news/national/discarded-laptop-yields-revelations-on-network-behind-brussels-paris-attacks (dostęp: 30.03.2023).

[29] K. Danielewicz (red.), *Państwo Islamskie*…, s. 101.

[30] P. Szymczak, *TATP, materiał wybuchowy zwany matką szatana. Czy można go wykryć?*, „Focus", 23.09.2019, https://www.focus.pl/artykul/czy-tatp-materia-wybuchowy-zwany-matk-szatana-mona-wykry (dostęp: 30.03.2023).

[31] P. Cruickshank, *Laptop Yields*…

[32] K. Danielewicz, *Państwo Islamskie*…, s. 99–102.

uchronić społeczeństwo od co najmniej pięciu ataków terrorystycznych. Dzięki użyciu oprogramowania szyfrującego i usuwaniu metadanych przez dżihadystów służby bezpieczeństwa na całym świecie nie przypuszczały nawet, jak niebezpieczną bronią stały się dzisiaj nowe technologie w rękach terrorystów.

Coraz większym problemem staje się jednak fakt, że im bardziej służby bezpieczeństwa starają się zbadać i zrozumieć jak dalece posunięta jest działalność Państwa Islamskiego w użyciu nowych technologii, za każdym razem dżihadyści są od nich o krok dalej, rozwijając i stosując coraz nowocześniejsze techniki kamuflażu. Często zdarza się, że dziennikarze czy śledczy starają się wkraść w sieci terrorystyczne poprzez tajną działalność na czatach czy forach internetowych. To właśnie w toku takich działań jednej z ekspertek, Rukmini Callimachi, udało się ustalić, że przed atakami w Paryżu zamachowcy posługiwali się czatem o nazwie „Kalafa", który miał być o wiele bezpieczniejszy od Twittera czy Messengera[33]. W tym miejscu należy dodać, że – według nieoficjalnych danych amerykańskich agencji wywiadowczych – ISIS stworzyło własną aplikację zapewniającą bezpieczną komunikację jej członkom, jednak wciąż nie ma oficjalnych dowodów na potwierdzenie tej tezy[34]. Powyższy przykład pokazuje jednak, iż zdobywane informacje są najczęściej szczątkowe, a cały proces ich pozyskiwania jest bardzo czasochłonny. Jest to spowodowane przede wszystkim tym, że członkowie IS bardzo dobrze zdają sobie sprawę z tajnej działalności organów ścigania w przestrzeni internetowej i prób inwigilacji poszczególnych platform internetowych i aplikacji[35]. Tym sposobem dżihadyści pozostają bardzo oszczędni w swoich wypowiedziach na forach internetowych, a także starają się używać tzw. protokołów OTR (Off The Record), które zapewniają pełne szyfrowanie danych w trakcie procesu komunikacji w sieci. Oznacza to tyle, że w momencie kiedy dwie osoby komunikują się ze sobą za pomocą jakiejś aplikacji, każda wiadomość zapisywana jest cyfrowym kluczem, do którego dostęp ma jedynie urządzenie, z którego została wysłana wiadomość[36]. Jest to tylko jedna z wielu technik wykorzystywanych przez Państwo Islamskie w użyciu nowych technologii, służąca do celów maskowania swojej działalności w przestrzeni internetowej.

Aby dokładniej wskazać, jak niebezpieczną bronią stają się nowe technologie w rękach terrorystów, można przytoczyć słowa byłego kanclerza skarbu

[33] P. J. Vogh, A. Goldman, *How ISIS Communicates In Secret*, „Digg", 22.04.2016, https://digg.com/2016/rukmini-callimachi-isis-reply-all (dostęp: 30.03.2023).

[34] K. Danielewicz (red.), *Państwo Islamskie*…, s. 103.

[35] S. Frenkel, *This Is How ISIS Uses The Internet*, „BuzzFeed News", 12.05.2016, https://www.buzzfeednews.com/article/sheerafrenkel/everything-you-ever-wanted-to-know-about-how-isis-uses-the-i (dostęp: 30.03.2023).

[36] K. Danielewicz (red.), *Państwo Islamskie*…, s. 103.

Wielkiej Brytanii – George'a Osborne'a, który w jednym z przemówień po atakach w Paryżu w listopadzie 2015 roku powiedział, że według jego wiedzy „bojownicy Państwa Islamskiego prowadzą badania nad możliwością przeprowadzania cyberataków na skalę globalną"[37]. Alan Woodward – ekspert ds. cyberprzestępczości sugeruje, że biorąc pod uwagę fakt, jak bardzo terroryści są obeznani z technologią, takie ataki mogą mieć miejsce już w niedalekiej przyszłości[38]. Wydaje się to tym bardziej realne, że w internecie można spotkać się z coraz większą liczbą informacji dotyczących przeprowadzania przez członków Państwa Islamskiego kampanii phishingowych czy ataków DDoS. Zdarzają się także przypadki, kiedy aktywiści działający w Iraku czy Syrii, próbując przedstawiać w sieci rzeczywiste realia z życia pod rządami kalifatu, otrzymują podejrzane maile, które zarówno w treści, jak i w samym wyglądzie są bardzo wiarygodne. W rzeczywistości jednak maile zawierają w sobie złośliwe oprogramowanie, które instaluje się na urządzeniu zaraz po otworzeniu wiadomości – w ten sposób nierzadko dżihadystom udaje się uzyskać dostęp do wszystkich danych z takiego urządzenia, a więc dotyczących działalności i nazwisk aktywistów z Iraku czy Syrii[39].

Podobnych cyberataków na przestrzeni ostatnich lat pojawia się coraz więcej nie tylko na Bliskim Wschodzie, ale także w Europie. Takie ataki są tym trudniejsze do wykrycia, im dalej znajduje się kraj, z którego atak został przeprowadzony. Amerykański wywiad, śledząc adresy IP, z których przeprowadzane były cyberataki, doszedł do wniosku, iż coraz częściej terroryści przemieszczają się do krajów sąsiednich, aby stamtąd przeprowadzić atak. Stanowi to dla nich kolejne zabezpieczenie, ponieważ przestrzeń internetowa w takich krajach jak Turcja czy Katar nie jest tak bardzo inwigilowana przez służby bezpieczeństwa jak w Iraku i Syrii[40].

Pozostając przy kwestii maskowania się w sieci i zabezpieczeń stosowanych przez członków Państwa Islamskiego, kluczowe zdaje się pytanie: Dlaczego, przy tak aktywnej działalności tylu zwolenników ISIS na całym świecie, służbom bezpieczeństwa tak trudno inwigilować przestrzeń internetową, w której poruszają się dżihadyści?

Odpowiedzią na nie wydają się być poradniki bezpieczeństwa w sieci dla zwolenników Państwa Islamskiego. Jeden z pierwszych takich dokumentów został odkryty zupełnie przypadkowo w 2015 roku przez zespół Aarona

[37] J. Wakefield, *How Does IS Communicate Securely?*, BBC News, 17.11.2015, https://www.bbc.com/news/technology-34842854 (dostęp: 30.03.2023).

[38] Ibidem.

[39] S. Frenkel, *This Is How ISIS…*

[40] K. Danielewicz (red.), *Państwo Islamskie…*, s. 101–103.

Brantly'a z Akademii Wojskowej West Point i, jak szybko udało się ustalić, docelowo był on stworzony dla dziennikarzy i działaczy politycznych ze Strefy Gazy. Państwo Islamskie jedynie przejęło ten dokument i przekształciło na własny użytek w taki sposób, że zawierał on nie tylko zbiór przydatnych porad dotyczących bezpiecznej komunikacji w sieci czy sposobów ochrony danych, ale określał także miejsca i położenia, w których obecnie znajduje się użytkownik[41]. Przykładowo, według poradnika wszelkie konta pocztowe powinny być tworzone poprzez podanie fałszywych danych, a korzystając z sieci powinno się zawsze używać wtyczek VPN i Tor, dzięki którym można zachować anonimowość. Zaleca się także mieć zawsze wyłączony GPS w smartfonach czy nieużywanie Instagramu, WhatsAppa i innych amerykańskich komunikatorów[42]. Zamiast tego w ostatnich latach członkowie Państwa Islamskiego szczególnie upodobali sobie niemieckie produkcje takie jak Telegram. Z informacji podanej do mediów jesienią 2015 roku przez jednego z założycieli aplikacji – Pawła Durowa – wynika, iż użycie Telegramu wśród zwolenników ISIS wzrosło w ostatnich latach, a filmy z egzekucji, przemówienia liderów i porady dotyczące wstąpienia do organizacji pojawiają się tam każdego dnia[43]. Ponadto, według opinii Aarona Brantly'a podpartej badaniami forów i mediów społecznościowych związanych z IS, najprawdopodobniej istnieje coś w rodzaju całodobowej informacji Państwa Islamskiego, która oferuje swoim zwolennikom wsparcie techniczne w przypadku problemów z bezpieczeństwem w sieci[44].

Podobny poradnik pojawił się już rok później w formie artykułu w internetowym magazynie „Dar Al-Islam" publikowanym przez ISIS – 16 stron poświęconych szczegółowym opisom, jak powinno postępować się w sieci, aby zwiększyć prawdopodobieństwo, że aktywność nie zostanie wykryta. Duża część artykułu nie różni się niczym od treści zamieszczonych w poprzednim poradniku, z tym, że ten drugi jest o wiele bardziej szczegółowy i „zaktualizowany". Profesor Thomas Rid z King's College London zauważa, że w pierwszym poradniku wtyczka Tor była polecana jako jedna z bardziej bezpiecznych do utrzymania anonimowości w internecie, zaś autor artykułu w magazynie „Dar Al-Islam" już zdecydowanie ją odradza, twierdząc, że najprawdopodobniej zaczęły nad nią pracować służby bezpieczeństwa[45].

---

41 K. Zetter, *Security Manual Reveals the OPSEC Advice ISIS Gives Recruits*, „Wired", 19.11.2015, https://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/ (dostęp: 30.03.2023).

42 K. Danielewicz (red.), *Państwo Islamskie*…, s. 104.

43 S. Frenkel, *This Is How ISIS*…

44 K. Zetter, *Security Manual*…

45 S. Frenkel, *This Is How ISIS*…

Jest to już kolejny przykład, który pokazuje, jak szybko i efektownie potrafią dzisiaj działać zwolennicy Państwa Islamskiego – po niecałym roku w sieci pojawił się nowy poradnik, który uwzględnił niemal wszystkie zmiany i postępy, jakie udało się uczynić informatykom śledczym, a wszystko po to, aby zapewnić swoim sojusznikom na całym świecie maksymalne bezpieczeństwo i anonimowość. Obecnie w internecie można znaleźć setki, jak nie tysiące mniejszych lub większych poradników dotyczących bezpieczeństwa w sieci, skierowanych do zwolenników ISIS. Wszystko to za sprawą innych zwolenników, którzy mieszkają głównie na Zachodzie i nie mają możliwości wspierania swoich „braci" na polu walki, robią to więc w mediach społecznościowych, zajmując się pisaniem poradników i udzielaniem wskazówek dotyczących bezpieczeństwa w internecie[46].

Ostatnią już kwestią, o której należy wspomnieć, choć w niewielkim zakresie, jest użycie współczesnej technologii (internetu) w celu dokonywania oszustw i gromadzenia funduszy przez Państwo Islamskie.

Jedna z takich sytuacji miała miejsce we wrześniu 2014 roku, kiedy ISIS oficjalnie otrzymało darowiznę z Zatoki Perskiej w wysokości 2 mln dolarów. W toku śledztwa okazało się, iż były to pieniądze z jednej ze zbiórek (przykrywek) charytatywnych prowadzonej w internecie przez prywatną osobę. Podobna sytuacja miała miejsce we Włoszech, gdzie na jedną z bardziej znanych organizacji charytatywnych otworzono konto, na które były zbierane kwoty od darczyńców z całej Europy. Po czasie okazało się, że osoba odpowiedzialna za prowadzenie zbiórki była powiązana z Państwem Islamskim, a pieniądze zniknęły i zostały przesłane do Turcji, a następnie do Syrii, gdzie posłużyły jako wsparcie finansowe dla działalności terrorystycznej[47].

Na przestrzeni ostatnich lat podobne zbiórki w internecie prowadzone były w Amsterdamie i Paryżu, gdzie pod przykrywką pięknie opisanej akcji charytatywnej „na pomoc humanitarną ofiarom z Syrii i Iraku" udało się uzbierać od 60 do 100 tys. euro, które później trafiały na konta bankowe liderów Państwa Islamskiego[48].

[46] K. Danielewicz (red.), *Państwo Islamskie*…, s. 104.

[47] Financial Action Task Force Report, *Financing of the Terrorist Organisation Islamic State in Iraq and Levant (ISIL)*, 02.2015, s. 35–36, https://www.fatf-gafi.org/content/dam/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf (dostęp: 30.03.2023).

[48] K. Danielewicz (red.), *Państwo Islamskie*…, s. 144.

Podsumowanie

Działalność Państwa Islamskiego, szczególnie po pierwszej dekadzie XXI wieku, pokazała, iż rozwój technologii okazał się tak samo potrzebny, jak i niebezpieczny. Wraz ze wzrostem znaczenia cyfryzacji łatwo dostrzec, jak na przestrzeni ostatnich 20 lat terroryści szybko i sprawnie zaadaptowali się w nowym otoczeniu. Ciągle rosnąca liczba zwolenników ISIS na całym świecie zdaje się tylko potwierdzać fakt, jak wiele nowych kanałów i metod przesyłania informacji, a także komunikowania się otworzyła technologia przed dżihadystami. Pewne różnice zauważyć można w celach, jakie stawiają przed sobą terroryści. Wraz z rozwojem technologii i uzyskaniem nowych narzędzi takich jak fora społecznościowe, blogosfery czy programy szyfrujące, a także wraz z uzyskaniem całkiem nowej, wykwalifikowanej fali zwolenników z Zachodu, ISIS nie poprzestaje już jedynie na wzbudzaniu przerażenia wśród społeczności międzynarodowej. Dzisiaj liderzy Państwa Islamskiego mogą sobie pozwolić na przeprowadzanie ataków terrorystycznych właściwie na całym świecie, nie ruszając się z Bliskiego Wschodu, przy swoim minimalnym zaangażowaniu. Zjawisko „elektronicznego dżihadu" staje się coraz bardziej powszechne i pozwala rekrutować nowych bojowników niemal z każdej części świata przy niewielkim ryzyku wykrycia, a nowe możliwości, jakie daje internet czy bankowość, są idealną przestrzenią do oszustw i pozyskiwania funduszy.

Można więc wysunąć stwierdzenie, iż wraz z rozwojem technologii, w drugiej dekadzie XXI wieku Państwo Islamskie dostało nowe życie i możliwości, i o ile instytucjom bezpieczeństwa w mniejszym lub większym stopniu udaje się hamować działalność ISIS w przestrzeni internetowej i wykorzystanie przez nich nowych technologii, o tyle wszystko wskazuje na to, że kolejna dekada będzie w dużym stopniu opierała się na walce z terroryzmem w cyberprzestrzeni.

Bibliografia

Campbell S., *ISIS Using Kittens and Nutella to Lure Jihadi Wannabes*, „Mirror", 27.05.2016, http://www.mirror.co.uk/news/world-news/isis-using-kittens--nutella-lure-8061303 (dostęp: 30.03.2023).

Cruickshank P., *Laptop Yields Revelations on Brussels Attacks*. „KSHB", 24.01.2017, https://www.kshb.com/news/national/discarded-laptop-yields-revelations-on-network-behind-brussels-paris-attacks (dostęp: 30.03.2023).

Danielewicz K. (red.), *Państwo Islamskie (ISIS). Historia powstania i taktyka działania*, Napoleon V, Grojec 2019.

Dziekan M., Bania R., Zdulski K., *Państwo Islamskie – powstanie i działalność samozwańczego kalifatu*, „Histmag", https://histmag.org/Panstwo-Islamskie-powstanie-i-dzialalnosc-samozwanczego-kalifatu-20228 (dostęp: 13.07.2023).

Engel P., *The Orlando Attack Exposes the Biggest Blind Spot in the US Strategy Against ISIS*, „Business Insider", 19.06.2019, https://businessinsider.com.pl/international/the-orlando-attack-exposes-the-biggest-blind-spot-in-the-us-strategy-against-isis/phv4zht (dostęp: 30.03.2023).

Financial Action Task Force Report, *Financing of the Terrorist Organisation Islamic State in Iraq and Levant (ISIL)*, 02.2015, https://www.fatf-gafi.org/content/dam/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf (dostęp: 30.03.2023).

Frenkel S., *This Is How ISIS Uses The Internet*, „BuzzFeed News", 12.05.2016, https://www.buzzfeednews.com/article/sheerafrenkel/everything-you-ever-wanted-to-know-about-how-isis-uses-the-i (dostęp: 30.03.2023).

Haniyeh H., *Daesh's Organisational Structure*, „Al Jazeera Center for Studies", 01.02.2017, https://studies.aljazeera.net/en/dossiers/decipheringdaeshoriginsimpactandfuture/2014/12/201412395930929444.html (dostęp: 30.03.2023).

Lakomy M., *Internet w działalności tzw. Państwa Islamskiego: nowa jakość cyberdżihadyzmu?*, „Studia i Analizy" 2015, t. 38, s. 156–184.

Ruble K., *Islamic State Documentary Style Video Says the „Flames of War" Have Just Begun*, „Vice", 19.09.2014, https://www.vice.com/en/article/d3jjga/islamic-state-documentary-style-video-says-the-flames-of-war-have-just-begun (dostęp: 30.03.2023).

Szymczak P., *TATP, materiał wybuchowy zwany matką szatana. Czy można go wykryć?,* „Focus", 23.09.2019, https://www.focus.pl/artykul/czy-tatp-materia-wybuchowy-zwany-matk-szatana-mona-wykry (dostęp: 30.03.2023).

The United States Capitol, *President Delivers State of the Union Address*, 29.01.2002, https://georgewbush-whitehouse.archives.gov/news/releases/2002/01/print/20020129-11.html (dostęp: 30.03.2023).

Vogh P. J., Goldman A., *How ISIS Communicates In Secret,* „Digg", 22.04.2016, https://digg.com/2016/rukmini-callimachi-isis-reply-all (dostęp: 30.03.2023).

Wakefield J., *How Does IS Communicate Securely?*, BBC News, 17.11.2015, https://www.bbc.com/news/technology-34842854 (dostęp: 30.03.2023).

Whitaker B., Harding L., *American Beheaded in Revenge for Torture*, „The Guardian", 12.05.2004, https://www.theguardian.com/world/2004/may/12/iraq.alqaida (dostęp: 30.03.2023).

Zelin A., *A Clearinghouse for Jihādī Primary Source Material, Original Analysis, and Translation Service*, 2022, https://jihadology.net/ (dostęp: 30.03.2023).

Zetter K., *Security Manual Reveals the OPSEC Advice ISIS Gives Recruits*, „Wired", 19.11.2015, https://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/ (dostęp: 30.03.2023).

Zgryziewicz R., Shaheen J., Grzyb T., Fahmy S., *Daesh. Information campaign and its influence – Executive summary*, 15.12.2015, https://stratcomcoe.org/cuploads/pfiles/executive_summary_15-12-2015.pdf (dostęp: 30.03.2023).