(Cyber)Terroryzm w Polsce

Autor tekstu: **Tomasz Mróz**

Zamachy terrorystyczne z 11 września 2001 roku pokazały, iż kraje Zachodu nie mogą czuć się bezpiecznie, nawet w czasie pokoju. Ataki w Madrycie i Londynie, które nastąpiły po zniszczeniu dwóch wież World Trade Center, tylko to potwierdzały. Zachodnie państwa będące sojusznikiem USA stały się atrakcyjnym celem dla organizacji Al-Kaida. Jednak ta siatka terrorystyczna zapomina o innych partnerach Stanów Zjednoczonych, szczególnie z rejonu Europy Środkowo-Wschodniej, które są pomijane jako cel ataków terrorystycznych. W tym szczęśliwym gronie państw jest również Polska. Na tle zachodnich krajów, Polska jawi się jako kraj wręcz nietknięty aktami terroru, mimo, iż jest sojusznikiem USA i aktywnym uczestnikiem wojny w Iraku i Afganistanie. Skoro Polska wspomagała Stany Zjednoczone w wojnie w Iraku podobnie jak Anglia czy Australia, to dlaczego siły Al-Kaidy nie odpowiedziały atakiem terrorystycznym wymierzonym w nasz kraj? Choć pojawiają się nieudane próby zamachów bombowych[1] to wydawać się może, iż Polska częściej jest celem cyberterroryzmu[2]. Tego typu ataki miały już wielokrotnie miejsce. Czy jednak stanowiły one zagrożenie dla bezpieczeństwa państwa? Dlaczego Polska jest częstszym celem ataków hakerów niż zamachowców? W związku z tym pojawia się pytanie, czy Polska jest „odpowiednim" celem dla ataków terrorystycznych w ogóle?

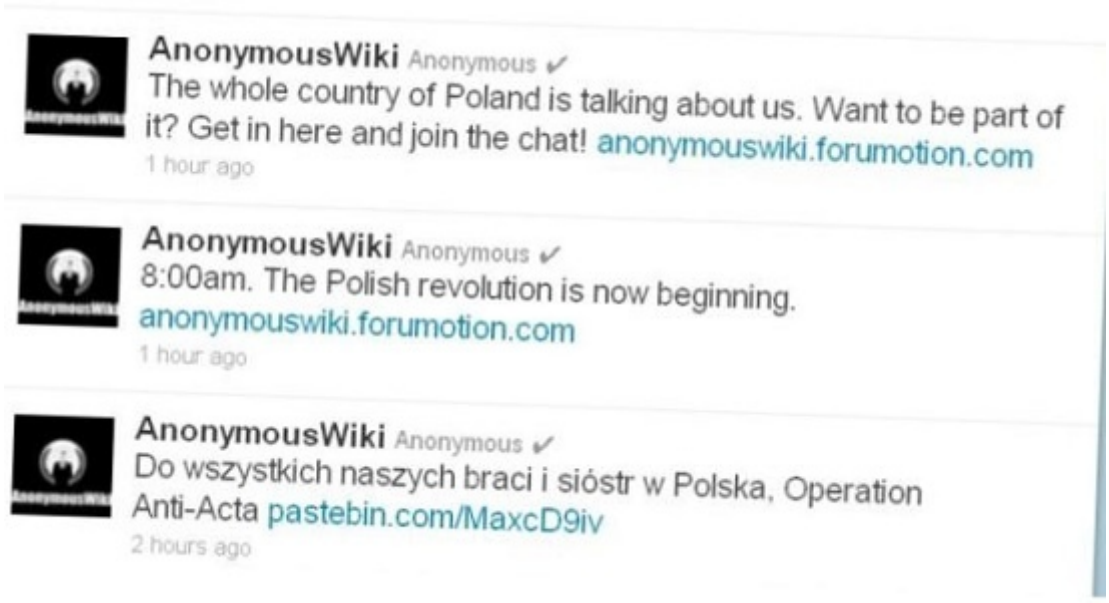
By lepiej zrozumieć czym jest cyberterroryzm, najpierw trzeba zapoznać się z samym pojęciem terroryzmu. Terroryzm posiada wiele definicji [3]. Jedną z nich zaproponowała Organizacja Narodów Zjednoczonych[4]:

„Stanowczo potępiamy wszelkie akty, metody i praktyki terrorystyczne jako nieusprawiedliwione, niezależnie od tego kiedy i przeciwko komu zostały popełnione, zwłaszcza te, które zagrażają międzynarodowemu pokojowi i bezpieczeństwu."

ONZ wskakuje, iż dla niego aktem terrorystycznym jest czyn, który zagraża życiu i zdrowiu ludzi. Nie tylko w wymiarze lokalnym, państwowym, lecz także globalnym. Inną definicję terroryzmu proponuje encyklopedia PWN:

„...różnie umotywowane, najczęściej ideologicznie, planowane i zorganizowane działania pojedynczych osób lub grup, podejmowane z naruszeniem istniejącego prawa w celu wymuszenia od władz państwowych i społeczeństwa określonych zachowań i świadczeń, często naruszające dobra osób postronnych; działania te są realizowane z całą bezwzględnością, za pomocą różnych środków[...]w warunkach specjalnie nadanego im rozgłosu i celowo wytworzonego w społeczeństwie lęku." [5]

Powyższa definicja zaznacza ważny cel zamachu terrorystycznego jakim jest wywołanie społecznego strachu i niepokoju oraz wymuszenie określonych decyzji politycznych. Bardziej lakoniczną, aczkolwiek podobną definicję stworzył Tomasz Aleksandrowicz:



„Terroryzm to akt przemocy zaplanowany tak, aby zwrócić uwagę i dzięki zdobytemu rozgłosowi przekazać odpowiednie przesłanie." [6]

W tej definicji brakuje uściślenia czym dokładnie jest akt przemocy i jakiej grupy ma on dotyczyć. Ta nieścisłość wymaga dookreślenia, w przeciwnym razie za akt terroru będzie można uznać np. walki uliczne czy stadionowe. Terminologiczna propozycja Aleksandrowicza zawiera kolejny istotny element ataku terrorystycznego. Mianowicie akt terroru jest komunikatem, wiadomością, która ma za zadanie dotrzeć do szerokiego grona odbiorców. Skuteczność ataku można zweryfikować na podstawie ilości medialnych doniesień i komentarzy, tym samym replikując główne przesłanie jakie za sobą nosi. Wspomniane powyżej definicje wystarczająco precyzują środki, cel i efekt ataku terrorystycznego na potrzeby niniejszego opracowania[7].

Na tej podstawie można podjąć próbę określenia ram znaczeniowych cyberterroryzmu. Próbę zdefiniowania tej formy terroryzmu podjęło się polskie Ministerstwo Spraw Wewnętrznych[8]. Nie uczyniło tego przypadkiem, bowiem w 2009 roku ministerstwo opublikowało dokument pt.: „Założenia do Rządowego programu ochrony cyberprzestrzeni RP na lata 2009-2011". Raport opisuje cele, status prawny i technologiczny oraz metody obrony polskich witryn i komputerów rządowych (oraz prywatnych, mających strategiczne znaczenie dla państwa). Zasadnicza jednak dla niniejszego opracowania jest zawarta w dokumencie definicja:

„Cyberterroryzm, czyli terroryzm wymierzony przeciwko newralgicznym dla państwa systemom, sieciom i usługom teleinformatycznym(...)." [9]

Według polskiego MSW za cyberterroryzm uznaje się takie ataki, które mają za zadanie sparaliżować funkcjonowanie stron internetowych czy systemów komputerowych. W takim wypadku na celowniku organizacji cyberterrorystycznych mogą znaleźć się banki, korporacje, urzędy oraz wojsko. W literaturze funkcjonuje inna definicja cyberterroryzmu zaproponowana przez agenta FBI Marka Pollita:

"(...)cyberterroryzm jako celowy motywowany politycznie atak przeciw informacji, systemom komputerowym, programom komputerowym i danym, który skierowany jest przeciw cywilnym i wojskowym celom przez państwowych i niepaństwowych aktorów."[10]

Powyższe określenie cyberterroryzmu dokładniej precyzuje tę formę terroryzmu. Znamienne jest określenie strony atakującej, otóż nie musi to być grupa terrorystyczna w przykładzie Al-Kaidy, lecz równie dobrze może nim być taki kraj jak USA, Chiny czy Rosja. W przeciwieństwie do polskiej definicji, ta wskazuje na militarne aspekty cybernetycznego ataku. Formuła Pollita na tle definicji zaprojektowanej przez polskie MSW wydaje się dokładniej prezentować charakter cyberterroryzmu[11].

Przebadawszy dostępne sformułowania dotyczące terroryzmu i cyberterroryzmu można zastanowić się czy w rzeczy samej Polska częściej jest celem ataków terrorystycznych czy cybernetycznych. Co do tych pierwszych można mieć pewne obiekcje, bowiem miały miejsce ataki bombowe, jednak były one w większości autorstwa Polaków. Ostatnimi czasy media prezentowały główną postać udaremnionego ataku bombowego, Brunona K. Miał on przygotowywać zamach na Sejm RP, jednak odpowiednie służby w porę udaremniły przygotowywany przez niego atak. Inny zamach bombowy zrealizowali bracia Kowalczyk, którzy podłożyli ładunek w auli Wyższej Szkoły Pedagogicznej w Opolu w 1971 roku. Ten incydent ma jednak charakter ambiwalentny. Z jednej strony był niebezpiecznym atakiem (mimo iż bomba eksplodowała w pustej auli), z drugiej był formą protestu wobec krwawo stłumionych protestów na Wybrzeżu w grudniu 1970 roku. Innym zamachem bombowym, jaki miał miejsce w Polsce, był ten w Cytadeli Warszawskiej z 13 października 1923 roku. Wybuch uszkodził budynki Cytadeli i jej okolic. W wyniku zamachu zginęło dwadzieścia osiem osób a osiemdziesiąt dziewięć zostało rannych.

Powyższe zamachy były jednak realizowane przez Polaków, a nie przez organizacje zewnętrzne czy obce kraje (choć niejasne podejrzenia padają co do zamachu na Cytadeli Warszawskiej, które przypisuje się agentom ZSRR). W tym świetle Polska pozostaje nietknięta przez działalność grup terrorystycznych. Tym nie mniej istnieją inne formy działalności terrorystycznej, które mogą zagrozić bezpieczeństwu kraju, a mianowicie cyberterroryzm. Ta forma terroryzmu została nie raz skierowana na państwo polskie. Skoro nie ma przejawów terroryzmu w klasycznym jego rozumieniu, to dlaczego Polska jest celem cyberterroryzmu? Czy Polska tym samym nie jest „atrakcyjnym" celem ataków terrorystycznych?[12] Jeżeli nie było w Polsce ataków terrorystycznych to może i nie ma cyberterroryzmu, tzn. Polskę atakują nie organizacje, lecz konkretne państwa?

W celu znalezienia odpowiedzi na powyższe pytania warto przyjrzeć się statystykom jakie podają państwowe placówki zajmujące się kwestią bezpieczeństwa cybernetycznego. Jednostką ochraniającą i publikującą dane na temat ataków w polskiej cyberprzestrzeni jest Rządowy Zespół

Reagowania na Incydenty Komputerowe CERT.GOV.PL. Ta instytucja działająca w ramach MSW zdaje kwartalne raporty na temat bezpieczeństwa oraz incydentów w cyberprzestrzeni. Analizując wspomniane raporty od trzeciego kwartału 2009 r. do drugiego kwartału 2010 r., można zauważyć systematyczny wzrost alarmów o priorytecie wysokim [13]. W publikacjach brakuje jawnego stwierdzenia czy dane incydenty były atakami cyberterrorystycznymi, czy może atakami hakerskimi. Stwierdza się jedynie wysoką szkodliwość wskazanych ataków. Mimo to, niepokojący jest dwukrotny wzrost liczby incydentów w ciągu niespełna roku. Kolejną ważną informacją zamieszczoną w raportach CERT.GOV.PL są źródła niektórych ataków. We wszystkich raportach wymienia się Stany Zjednoczone oraz Chiny jako jedne z głównych lokalizacji wykonawców ataków[14]. Regularność w odnotowywaniu tych dwóch krajów jako miejsc ataków na polskie witryny i serwery jest zastanawiająca.

Lakoniczne dane państwowych instytucji nie pozwalają szerzej spojrzeć na problematykę cyberterroryzmu w Polsce. Tłumaczyć to można tajemnicą państwową czy zaangażowaniem rządu oraz wojska, które nie chcą upubliczniać tak poufnych informacji. Nie mniej pojawiają się spektakularne ataki na strony internetowe polskich instytucji, których nie sposób nie zauważyć, jak np. ten z września 2009 roku[15]. Ustalono, iż atak przeprowadzony został z Rosji oraz miał on zorganizowany charakter. Inne szczegóły dotyczące tego incydentu zostały utajnione.

Analizując raporty CERT.GOV.PL należy zwrócić uwagę na fakt, iż brak w nich rozróżnienia na ataki terrorystów cybernetycznych, hakerów czy haktywistów [16]. Polskie strony internetowe należące do władz państwowych szczególnie pamiętają działalność tej ostatniej grupy. Ataki znanej grupy The Anonymous z przełomu marca i kwietnia 2012 roku zablokowały witryny internetowe polskiej administracji. Działanie The Anonymous związane było z propozycją przyjęcia ogólnonarodowego porozumienia handlowego pod nazwą ACTA[17]. Porozumienie miało na celu ograniczenie nielegalnego pobierania dokumentów, utworów i książek w celu ochrony praw autorskich. Pomysł ratyfikacji ACTA spotkał się ze społecznym sprzeciwem. W odpowiedzi na podpisanie przez Polskę ACTA, The Anonymous dokonali ataków na rządowe strony www[18].

Reasumując, Polska, pomimo aktywnego udziału w wojnach na Bliskim Wschodzie, czy bliskiego sojuszu z posiadającym wielu wrogów USA, najwyraźniej nie jest atrakcyjnym obiektem ataków terrorystycznych. Być może wynika to z naszej mało istotnej pozycji na świecie i niskiego zainteresowania zagranicznych mediów Polską. Ze względu na to, że coraz więcej ważnych dla bezpieczeństwa państwowego informacji przechowuje się w postaci cyfrowej, wojny i terroryzm przenoszą się w świat wirtualny. Cyberataki nie wymagają tak dużych kosztów i wysiłku jak terroryzm w klasycznym ujęciu. Być może dlatego statystyki MSW wykazują stale rosnącą liczbę cyberataków na rządowe witryny internetowe (które jednak nie zawsze muszą nosić znamiona cyberterroryzmu — przykład ACTA). Wraz z postępem techniki i cyfryzacji możemy się spodziewać, że ta tendencja wzrostowa się utrzyma. Nie wiadomo jednak, jak duża część cyberataków pozostanie nigdy niewykryta lub na zawsze utajniona.

---

[1] Za przykład polskich terrorystów mogą posłużyć Brunon K., który chciał zaatakować Sejm RP, oraz Adam K. i Mikołaj G, którzy zasłynęli atakami bombowymi na markety sieci Ikea, jednak ich działalność omijała Polskę. Braci Kowalczyk, którzy wysadzili w powietrze budynek wyższej uczelni w Opolu, trudno zaklasyfikować jako terrorystów, tym bardziej, iż jednemu z braci decyzją prezydenta Lecha Wałęsy przysłużyło zatarcie skazania.

[2] Witryny i komputery polskich urzędów w samym 2008 roku stały się celem ataków około 500 tysięcy razy. Zob.: http://www.altair.com.pl/news/view?news_id=3500 , dostęp: 21.01.2014.

[3] Istnieje ponad 100 definicji tego pojęcia, zob. http://encyklopedia.pwn.pl/haslo.php?id=3986796 , dostęp: 12.01.2014.

[4] Rezolucja Rady Bezpieczeństwa S/RES/1269(1999 r.).

[5] http://encyklopedia.pwn.pl/haslo.php?id=3986796 , dostęp:21.01.2014.

[6] T. R. Aleksandrowicz, „Terroryzm międzynarodowy", Warszawa 2008, s. 21.

[7] Dokładniejsza analiza definicji terroryzmu zob.: http://konkursy.byd.pl/userfiles/files/Majczak.pdf , dostęp: 21.01.2014.

[8] Dalej skr. MSW.

[9] „Założenia do Rządowego programu ochrony cyberprzestrzeni RP na lata 2009-2011", Warszawa 2009, s.4.

[10] Cyt. za: „Terroryzm cybernetyczny — zagrożenia dla bezpieczeństwa narodowego i działania amerykańskiej administracji", Biuro Bezpieczeństwa Narodowego, Warszawa 2009, s. 2.

[11] Michał Majczak cyberterroryzm określa jako „próbę zastraszania za pośrednictwem narzędzi internetowych". Takie ujęcie terroryzmu cybernetycznego jednak pauperyzuje problem, bowiem ta forma terroryzmu była użyta w konflikcie miedzy Rosją a Gruzją. Zob.: „Terroryzm cybernetyczny — zagrożenia dla bezpieczeństwa narodowego i działania amerykańskiej administracji", Biuro Bezpieczeństwa Narodowego, Warszawa 2009, s. 5.

[12] Wspomnieć należy o porwaniu i zabiciu polskiego geologa Piotra Stańczaka. Jednak ten akt terroru miał na celu wymianę za uwięzionych współtowarzyszy porywaczy. Mimo, iż to morderstwo nosi ślady działań terrorystycznych, to nie miało miejsca na terenie Polski. Zob.: K. Liedel, A. Mroczek, „Terror w Polsce — analiza wybranych przypadków", Wydawnictwo Difin, Warszawa 2013.

[13] W trzecim kwartale 2009 roku zanotowano 56 incydentów o wysokim priorytecie, w drugim kwartale 2010 odnotowano już 122. W trzecim kwartale 2010 wykryto najmniej incydentów o wysokim priorytecie, bowiem 55, lecz w czwartym kwartale 2010 już 127. Zob.: http://www.cert.gov.pl/cer/publikacje , dostęp:26.01.2014.

[14] Polskie strony atakowano również z Japonii, Kanady, Turcji, Hiszpanii, Litwy, Federacji Rosyjskiej i Tajwanu. Co ciekawe ataki odnotowywano na terenie samej Polski. Zob: http://www.cert.gov.pl/cer/publikacje/raporty-z-dzialalnosci/385,Raport-z-dzialalnosci-zespolu-CERTGOVPL-za-IV-kwartal-2010.html , dostęp: 26.01.2014.

[15] http://prawo.rp.pl/artykul/375962.html , dostęp: 26.01.2014.

[16] Więcej o haktywizmie zob.: http://winntbg.bg.agh.edu.pl/skrypty2/0095/445-450.pdf , dostęp:27.01.2014.

[17] Anti-Counterfeiting Trade Agreement, (pol. Umowa handlowa dotycząca zwalczania obrotu towarami podrabianymi).

[18] http://www.cert.gov.pl/cer/publikacje/raporty-z-dzialalnosci/561,Raport-z-dzialalnosci-zespolu-CERTGOVPL-za-II-kwartal-2012.html , dostęp: 27.01.2014.

Tomasz Mróz
Magister kulturoznawstwa w Instytucie Kulturoznawstwa Wydziału Nauk Społecznych Uniwersytetu im. Adama Mickiewicza w Poznaniu. Członek i wolontariusz Stowarzyszenia "Lepszy Świat" w Poznaniu.

Pokaż inne teksty autora

(Publikacja: 28-08-2014)
Oryginał.. (http://www.racjonalista.pl/kk.php/s,9721)

i nie korzystać z jego zasobów.

Informacje zawarte na tym portalu przeznaczone są do użytku prywatnego osób odwiedzających te strony. Można je pobierać, drukować i przeglądać jedynie w celach informacyjnych, bez czerpania z tego tytułu korzyści finansowych lub pobierania wynagrodzenia w dowolnej formie. Modyfikacja zawartości stron oraz skryptów jest zabroniona. Niniejszym udziela się zgody na swobodne kopiowanie dokumentów portalu Racjonalista.pl tak w formie elektronicznej, jak i drukowanej, w celach innych niż handlowe, z zachowaniem tej informacji.

Plik PDF, który czytasz, może być rozpowszechniany jedynie w formie oryginalnej, w jakiej występuje na portalu. **Plik ten nie może być traktowany jako oficjalna lub oryginalna wersja tekstu, jaki prezentuje**.

Treść tego zapisu stosuje się do wersji zarówno polsko jak i angielskojęzycznych portalu pod domenami Racjonalista.pl, TheRationalist.eu.org oraz Neutrum.eu.org.

Wszelkie pytania prosimy kierować do redakcja@racjonalista.pl