EDUKACJA HUMANISTYCZNA nr 2 (39), 2018
Szczecin 2018

Grzegorz Gronowicz
Marek Woś
Wyższa Szkoła Humanistyczna
Towarzystwa Wiedzy Powszechnej w Szczecinie

ZAGROŻENIA CYBERTERRORYSTYCZNE W ŚWIADOMOŚCI MŁODZIEŻY

Wstęp

Człowiek żyjący w społeczeństwie włączony jest w jego rytm. Wszystko, co go otacza, ma swoje odniesienie do jego życia. Obecnie zauważalny jest coraz większy rozwój myśli, technologii, napór trendów, które z jednej strony zwalczają się, z drugiej zaś wzajemnie się korygują. Społeczeństwa na różnych kontynentach rzadziej współcześnie dochodzą do stabilnych wniosków, które by ukazywały drogi wyjścia z trudnych sytuacji. Jest to być może związane z gwałtownym rozwojem technologii informacyjnej i komunikacyjnej, ponieważ zachodzące zmiany są bardzo skomplikowane. Jednocześnie dokonująca się w różnych aspektach życia człowieka globalizacja jest złożoną rzeczywistością, która niejako wywraca dotąd znany świat[1].

Od wydarzeń w Stanach Zjednoczonych, jakie miały miejsce 11 września 2001 roku (WTC), znane jest powszechnie nowe zjawisko terroryzmu, wymierzone przede wszystkim w ludność cywilną[2]. Tym samym w wiktymologicznym ujęciu ofiarą terroryzmu zostaje się z powodu polityki lub ideologii, kiedy jednostki lub też grupy społeczne łamią ustalony ład i porządek, nie tylko podczas ataku fizycznego na jednostkę, lecz przede wszystkim przejmując kontrolę nad umysłem drugiej osoby. Dlatego niezbędne wydaje się przyjrzenie się używanym przez terrorystów narzędziom, aby zadać sobie pytanie o ich rodzaj: czy są to tylko bomby, broń, środki transportu, czy może coś więcej?

[1] M. Woś, *Wychowanie i edukacja chrześcijańska wobec wyzwań socjoglobalistyki*, „Seminare" 2014, nr 2 (35), s. 83, 99.
[2] R.B. Woźniak, *U podstaw socjoglobalistyki. Koncepcje i zagrożenia,* Szczecin 2009, s. 203–208.

1. Aspekty bezpieczeństwa użytkowania Internetu

Wiele osób rozumie obecnie globalizację jako proces intensywnych powiązań oraz wszelkiego rodzaju zależności pod względem ekonomicznym, politycznym, ideologicznym, społecznym, prawnym, informacyjnym i ekologicznym. Według nich odzwierciedla ona nowy ład społeczny. Zawiera w sobie obszar wolności, bezpieczeństwa oraz sprawiedliwości, które nie mogą być pominięte w kontekście budowania bezpieczeństwa publicznego[3].

Mnogość możliwości komunikacji jaką oferuje cyberprzestrzeń czyni ją idealną bronią w rękach terrorystów, która może zostać skierowana zarówno przeciwko poszczególnym jednostkom, jak i różnym grupom społecznym. Mechanizm kopiowania i ponownego udostępniania treści w Internecie zwiększa liczbę odbiorców informacji, która krąży w sieci na różnych portalach i mediach społecznościowych. Dzięki zastosowaniu odpowiednich zabezpieczeń źródło informacji może zostać anonimowe lub trudne do ustalenia.

Na początku omawiania zagadnienia bezpieczeństwa użytkowania Internetu należy stwierdzić, że sam termin „bezpieczeństwo" definiowany jest bardzo szeroko[4]. Jedni uważają, że jest to między innymi stan pewności, spokoju, zabezpieczenia oraz istnienie obszaru porządku i ochrony bezpieczeństwa. Drudzy są zdania, że odzwierciedla brak zagrożeń i polega na ścisłej, obejmującej możliwie wiele dziedzin życia współpracy państw. Stanowi instrument odstraszania, który charakteryzuje brak określonego wroga, przy czym wymaga współpracy wszystkich zainteresowanych podmiotów przy zastosowaniu koncepcji równowagi sił[5].

Bezpieczeństwo w Internecie w głównej mierze zależy od świadomości korzystającego z niego użytkownika. Dlatego ważna jest wiedza dotycząca zagrożeń, jakie czyhają w cyberprzestrzeni. Jej zastosowanie w odpowiednim zakresie pomaga zminimalizować ryzyko związane z zagrożeniami w sieci, którego nie należy rozpatrywać jedynie jako zagrożenia *sensu stricto*, lecz również jako stopień świadomości użytkowników na temat samego pojęcia zagrożenia, nieraz bagatelizowanego i bywającego obiektem żartów. Każda podatność na zagrożenia w cyberprzestrzeni jest bezpośrednio powiązana z konkretną osobą, z użytkownikiem lub administratorem.

Medium, jakim jest Internet, należy traktować z dystansem, ostrożnie podchodząc do jego zasobów. Należy być świadomym w korzystaniu z wiarygodnych źródeł dostarczających treści. Aby chronić także oczy i uszy najmłodszych użytkowników systemów informatycznych, trzeba zdawać sobie sprawę z tego, że są osoby włamujące się do sieci i systemów[6].

Włamania dotyczące systemów i sieci informatycznych mogą być niezwykle groźn, nie tylko dla jednostek, lecz także dla organizacji i państw. Ze względu na swoje funkcje oraz rodzaj przechowywanych i przetwarzanych danych kwestia bezpieczeństwa systemów i sieci informatycznych jest sprawą wagi państwowej. Stąd też opracowania i wdrożenia dotyczące

---

3 Ibidem, s. 220.

4 K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2006, s. 19.

5 Ibidem, s. 222–223.

6 *Konwencja Rady Europy o cyberprzestępczości*, Dz. U. poz. 728, Warszawa, dnia 27 maja 2015 r., s. 4.

polityki ochrony cyberprzestrzeni Rzeczypospolitej Polskiej[7] i państw Unii Europejskiej. Należy przy tym nadmienić, że według danych statystycznych GUS z roku 2016 dostęp do cyberprzestrzeni ma większość gospodarstw domowych w Polsce[8].

2. Zagrożenia w cyberprzestrzeni

Przy zakupie nowego tabletu, komputera lub smartfonu albo podczas uruchamiania łącza internetowego rozpatrywane są korzyści, jakie płyną z używania wymienionego sprzętu w sieci. Wiele osób miało okazję się przekonać, o ile uboższe są możliwości sprzętu komputerowego bez połączenia internetowego. Niestety Internet to nie tylko same korzyści, lecz również realne zagrożenia, które mają swoje odniesienie do rzeczywistości. Do najważniejszych z nich należą:

a) *cyberbullying* (ang.) – cyberprzemoc: znęcanie się nad słabszymi, terroryzowanie, tyranizowanie, zastraszanie, prześladowanie, szykanowanie i dokuczanie[9];
b) pedofilia – relacja tworzona pomiędzy dorosłym a dzieckiem, oparta na manipulacji; uwodzenie dzieci w celach seksualnych przez Internet[10];
c) sekty – grupy destrukcyjne oraz zjawiska patologiczne związane z ich działalnością[11];
d) *sexting* – zagrożenie polegające na tym, że materiały przesyłane przez nadawcę mogą zostać udostępnione innym osobom lub wręcz opublikowane w Internecie. Mogą stać się narzędziem szantażu i doprowadzić do cyberprzemocy;
e) cyberseks – motywowana seksualnie interakcja z drugą osobą za pośrednictwem komputera[12];
f) pornografia – zamieszczona w różnych formach w sieci może doprowadzić do przyswajania prymitywnej wizji seksualności i uprzedmiotowienia drugiej osoby;
g) działalność terrorystów w Internecie – szerzenie ideologii, prowadzenie internetowego dżihadu, werbunku, szkoleń, komunikacji oraz zamieszczanie brutalnych materiałów wideo z egzekucji przeprowadzanych przez państwo islamskie (ISIS);
h) uzależnienie od sieci – komputer i Internet zaspokajają potrzeby człowieka, jego wrodzoną ciekawość, nagradzając go znalezieniem szukanej informacji. Oferują przy tym poczucie bezpieczeństwa i przyjemności, co doprowadza często do zaniedbania obowiązków życia codziennego;

7 *Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*, Dz.U. 2002 nr 156, poz. 1301; *Polityka ochrony cyberprzestrzeni Rzeczpospolitej Polskiej*, Warszawa, 25.06.2013.

8 GUS, *Opracowanie sygnalne. Społeczeństwo informacyjne w Polsce w 2016 r.*, Warszawa 2016, s. 4, http://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/2/6/1/si__sygnalna_2016.pdf [28.04.2017].

9 *Bullying*, http://pl.bab.la/slownik/angielski-polski/bullying [4.04.2017].

10 M. Wawrzak-Chodaczek, I. Jagoszewska, *Komunikacja wobec wyzwań współczesności*, Toruń 2011, s. 53.

11 *Raport o niektórych zjawiskach związanych z działalnością sekt w Polsce*, Warszawa 2000, s. 16.

12 R. Mysior, *Cyberseks – ciemna strona mediów*, „Problemy opiekuńczo-wychowawcze" 2013, nr 9, s. 34–38.

i) zagrożenia finansowe – dotyczą przede wszystkim płatności bezgotówkowych, gdzie płatność odbywa się z wykorzystaniem środków teleinformatycznych;
j) złośliwe oprogramowanie – „uciążliwy lub szkodliwy typ oprogramowania, który ma na celu potajemnie uzyskać dostęp do urządzenia bez wiedzy użytkownika”[13];
k) piractwo – na przykład zagrożenie finansowe dla twórcy lub dystrybutora oraz zagrożenie dla osób korzystających z pirackich źródeł. Pirackie oprogramowanie zdobyte z nieoficjalnego źródła, może być wyposażone w dodatkowe malware.

3. Dane statystyczne

Dane statystyczne dotyczące cyberprzestępczości podane przez polską policję nie podają informacji, które przestępstwa miały znamiona cyberterroryzmu. Należy jednak mieć świadomość, że prócz danych podanych w raporcie istnieje również nieznana liczba przestępstw. Są to zazwyczaj przestępstwa niewykryte bądź niezgłoszone.

Tabela 1. Liczba przestępstw stwierdzonych przez Policję w Polsce z wybranych artykułów k.k. dotyczących cyberprzestępczości w latach 2009–2015

Artykuł	2010	2011	2012	2013	2014	2015
art. 200a §1–2 k.k. (przestępstwa związane z pedofilią)	6	62	74	132	151	286
art. 269 §1–2 k.k. (atak na zasoby lub urządzenia informatyczne instytucji państwowych lub samorządowych)	0	5	5	9	7	4
art. 269a k.k. (atak na system komputerowy lub sieć teleinformatyczną)	18	30	30	34	52	111
art. 269b k.k. (udostępnianie urządzeń, programów lub danych służący popełnianiu przestępstw)	71	29	27	28	43	44

Źródło: Ministerstwo Spraw Wewnętrznych i Administracji, „Raport o stanie bezpieczeństwa w Polsce w 2015 roku”, s. 264.

4. Konsekwencje udanego cyberataku

Badania firmy Deloitte *Beneath the surface of a cyberattack. A deeper look at business impacts* uzmysłowiły odbiorcom sieci skutki cyberataków. W tabeli numer 2 zebrano je i podzielono na dwie płaszczyzny: nad i pod powierzchnią.

[13] *Malware*, https://www.avast.com/pl-pl/c-malware [18.04.2017].

Tabela 2. Skutki udanego cyberataku w przypadku firm, różnego rodzaju instytucji i organizacji

Skutki nad powierzchnią, które są dobrze znane i bezpośrednio widoczne: • śledztwo techniczne; • powiadomienie klienta o naruszeniu; • ochrona klienta po naruszeniu; • zgodność z przepisami – jej brak może prowadzić do poniesienia konsekwencji finansowych; • PR – pogorszenie wizerunku firmy i relacji z klientami; • spory sądowe, wynagrodzenia dla prawników i opłaty związane z postępowaniem sądowym; • poprawa cyberbezpieczeństwa.
Skutki pod powierzchnią, ukryte i mniej widoczne: • wzrost wysokości składek ubezpieczeniowych; • wzrost uzyskania kapitału dłużnego; • zakłócenie działalności; • zmniejszenie się wartości relacji z klientem; • utrata zysku z umów, które mogłyby zostać zawarte; • utrata reputacji firmy; • utrata własności intelektualnej.

Źródło: Deloitte, „Beneath the surface of a cyberattack. A deeper look at business impacts", 2015, s. 3, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf [10.07.2017].

Skutków cyberataków nie należy bagatelizować. Jedną z najbardziej odczuwanych konsekwencji jest zakłócenie działalności, które należy rozpatrywać indywidualnie, ponieważ inna jest skala następstw awarii pracy elektrowni atomowej lub włamanie i skasowanie bazy PESEL w porównaniu do utraty wypracowania licealisty. Skala strat i skutków udanego cyberataku zależy także od ważności danych czy też funkcji, jaką pełni system komputerowy oraz stopnia zabezpieczenia się na sekwencje po nim wynikłe.

Na podstawie opublikowanych przez GUS[14] danych dotyczących zdarzeń związanych z bezpieczeństwem podczas korzystania z Internetu można wyciągnąć następujące wioski: najczęstszym skutkiem cyberataku jest utrata danych i czasu (24,6%), następnie naruszenie prywatności (2,8%), później zaś straty finansowe wynikające z pishingu (0,7%) lub fałszywych płatności z wykorzystaniem karty (0,2%).

5. Unikanie i zabezpieczenie się przed atakiem cyberterrorystycznym

Aby uniknąć czy też zminimalizować straty związane z cyberatakiem, powinno tworzyć się i rozpatrywać różne scenariusze w celu podniesienia poziomu zabezpieczeń i zminimalizowaniu strat. Na bazie doświadczeń można i należy rozpatrywać dokonane już cyberataki oraz ich skutki i tworzyć nowe środki zaradcze, które dotyczyć będą nie tylko

[14] GUS, *Jak korzystamy z Internetu? 2015*, s. 2, http://szczecin.stat.gov.pl/download/gfx/szczecin/pl/defaultaktualnosci/843/6/30/1/jak_korzystamy_z_internetu_2015.pdf [10.09.2017].

sprzętu, lecz także korelacji sprzętu komputerowego (szeroko rozumianego) z użytkownikami.

Pomocna w podniesieniu bezpieczeństwa jest wymiana informacji pomiędzy ekspertami z dziedziny cyberbezpieczeństwa. Przykładem tego może być spotkanie ekspertów z sektora finansowego, zrealizowane przez redakcję Itwiz i Intel Security, producenta popularnego oprogramowania antywirusowego McAfee oraz procesorów, podczas którego zwrócono uwagę na biznesowe aspekty technologii[15].

Nie tylko firmy i banki powinny mieć opracowany system ciągłości działania. Choć w przypadku zwykłych użytkowników komputerów i smartfonów termin „system ciągłości działania" wydaje się czymś na wyrost, to założenia w obu przypadkach są podobne:

1) Należy robić kopię bezpieczeństwa.
2) Należy zmniejszać podatność na cyberatak poprzez przestrzeganie kilku zasad:
   a) używanie legalnego i aktualnego oprogramowania;
   b) posiadanie aktualnego oraz aktywnego programu antywirusowego i zapory sieciowej;
   c) przeprowadzanie okresowego skanowania w celu wyszukania i likwidacji szkodliwego oprogramowania;
   d) korzystanie z sprawdzonych (przeskanowanych) nośników danych, nieotwieranie nieznanych załączników maili, znajomość prawidłowych adresów internetowych swojego banku i innych używanych stron oraz szczególna uwaga przy korzystaniu z poczty email, aby nie paść ofiarą *phishingu*;
   e) używanie oprogramowania wykrywającego spam i *spyware*;
   f) unikanie korzystania z niesprawdzonych połączeń, na przykład z publicznych sieci Wi-Fi;
   g) używanie bezpiecznych, haseł logowania o odpowiednim stopniu skomplikowania;
   h) niepodawanie haseł osobom trzecim i nielogowanie się na swoje konta z niesprawdzonych cudzych komputerów, na przykład w bibliotece, kawiarence;
   i) okresowe zmienianie haseł, zgodnie z polityką bezpieczeństwa;
   j) posiadanie konta online skonfigurowanego tak, aby otrzymywać powiadomienia o naruszeniu bezpieczeństwa w postaci sms lub wiadomości email;
   k) skanowanie pamięci przenośnych przed użyciem.

Należy jednak pamiętać, że wymienione zasady pomogą w zmniejszeniu podatności na cyberatak, lecz nie zapewnią całkowitego bezpieczeństwa, gdyż są przede wszystkim ogólnymi poradami dla użytkowników cyberprzestrzeni.

[15] Szerzej na ten temat: P. Okopień, *Informatyka śledcza w obronie przed i po cyberataku*, http://itwiz.pl/informatyka-sledcza-obronie-przed-po-cyberataku/ [4.07.2017].

6. Pojęcie cyberterroryzmu

Używanie szeroko pojętej cyberprzestrzeni do aktów terroryzmu nazywamy cyberterroryzmem. Jest to bardzo sugestywna nazwa, gdyż wskazuje na narzędzie, sposób jego użycia oraz na zdobycze technologii cyfrowej służące do przekazywania i przetwarzania danych w cyberprzestrzeni jako narzędzia terroru. Pojęcie cyberterroryzm jest ściśle związane z terminami cyberprzestrzeni i terroryzmu. Jako pierwszy połączenia tych pojęć dokonał w połowie lat 80. XX wieku Bary Collin z Institute of Seciurity and Intelligence z Kaliforni: cyberprzestrzeń + terroryzm = cyberterroryzm[16]. Należy zatem zwrócić uwagę na to, że często różne zjawiska występujące w Internecie są określane mianem cyberterroryzmu, lecz jest to zabieg upraszczający, który ma na celu ułatwienie prowadzenie debaty publicznej.

Brak jednolitej definicji rozdzielającej działania cyberprzestępcze od cyberterrorystycznych powoduje, że granica pomiędzy nimi jest trudna do ustalenia. Należy również podkreślić, że osoby zajmujące się tym zjawiskiem mają trudności w poznaniu, które działania są internetowym przestępstwem, a które cyberterroryzmem. Nie ułatwia tego fakt, że cyberprzestępcy mają możliwość dobrego kamuflażu w cyberprzestrzeni, a za tym idzie, bycia anonimowymi.

Tabela 3. Składowe cyberterroryzmu

Cyberterroryzm Cyberterroryzm należy rozumieć jako wykorzystywanie technologii, sprzętu elektronicznego (komputerów, smartfonów, oprogramowania) oraz infrastruktury sieciowej do sterowania i przekształcania informacji w cyberprzestrzeni tak, aby kierując się pobudkami terrorystycznymi, wywrzeć wpływ na jednostki i społeczeństwa.		
Cyberprzestrzeń (jako przestrzeń przetwarzania informacji)		Terroryzm
Cyber (w nawiązaniu do cybernetyki jako nauki o przetwarzaniu i przekazywaniu informacji).	Przestrzeń (wirtualna, sieciowa, ale mająca bezpośrednie odniesienie do rzeczywistości).	Zjawisko szeroko rozumianego (ze względu na brak jednej uniwersalnej definicji) terroryzmu jako aktu przemocy, mającego na celu wymuszenie określonych zachowań wobec społeczeństw.

Źródło: opracowanie własne.

7. Problematyka badawcza

Ze względu na styczność młodzieży z nieustannie rozwijającą się technologią, w tym z Internetem i cyberprzestrzenią, a także towarzyszącymi jej zjawiskami, zasadnym wydaje

[16] A. Podraza, P. Potakowski, K. Wiak, *Cyberterroryzm zagrożeniem XXI wieku: perspektywa politologiczna i prawna*, Warszawa 2013, s. 27.

się postawienie pytania: jaki jest poziom wiedzy młodzieży na temat zagrożeń cyberterrorystycznych? W celu uzyskania odpowiedzi posłużono się w badaniu kwestionariuszem ankiety, który zawierał pytania zamknięte (alternatywne, koniunktywne, dysjunktywne), otwarte i półotwarte. Badanie zostało zrealizowane we wrześniu 2017 roku (uczniowie Zespołu Szkół Prywatnych nr 1 oraz gimnazjum) w Stargardzie na populacji 50 osób.

Młodzież na początku kwestionariusza ankiety została zapytana o znajomość pojęcia cyberterrozyzmu w celu sprawdzenia, czy rozumie zagadnienie, które stanowi główny przedmiot badania. Pomiar wykazał, że 84% uczniów deklaruje znajomość tego pojęcia, a 16% brak. Większość także odpowiadających mężczyzn (89%) ma lepsze rozeznanie w tym problemie w porównaniu z odpowiadającymi kobietami (78%). Szczegółowy wynik, po zsumowaniu danych, z rozkładem respondentów na płeć, miejsce zamieszkania oraz doświadczenie płynące z użytkowania Internetu, przedstawia się następująco:

Tabela 4. Deklaracja znajomości pojęcia cyberterroryzmu

			Płeć		Miejsce zamieszkania		Użytkownik Internetu	
Odpowiedź	Odpowiedzi ogółem	Ogółem %	Kobiety	Mężczyźni	Wieś	Miasto	Od 3 do 6 lat	Powyżej 6 lat
tak	42	84%	18	24	14	28	11	31
nie	8	16%	5	3	2	6	4	4

Źródło: opracowanie własne.

Na kolejne pytanie wielokrotnego wyboru (tabela nr 5): „Czym jest według Ciebie cyberterroryzm?", 35 ankietowanych (70%) odpowiedziało, że cyberterroryzm to przestępczość komputerowa. Jednocześnie 23 osoby (46%) podkreśliły, że jest to hakerstwo; 5 osób (10%) było przekonanych o tym, że cyberterroryzm to również wyszukiwanie dziur w oprogramowaniu komputerowym, a 24 osoby (48%) wskazały na neologizm opisujący dokonywanie aktów terroru przy pomocy zdobyczy technologii informacyjnej. 12 osób (24%) myślało, że są to też wirusy i zagrożenie w Internecie, zaś 12% badanych (6 osób) uważało, że cyberterroryzm jest atakiem konwencjonalnym, który polega na fizycznym uszkadzaniu elementów systemu komputerowego. W zbiorczym podsumowaniu uwzględniono także wszystkie poprzednie parametry, które dają szczegółowy obraz respondentów:

Tabela 5. Cyberterroryzm według młodzieży

			Płeć		Miejsce zamieszkania		Użytkownik Internetu	
Odpowiedź	Odpowiedzi ogółem	Ogółem %	Kobiety	Mężczyźni	Wieś	Miasto	Od 3 do 6 lat	Powyżej 6 lat
przestępczość komputerowa	35	70%	14	21	12	23	12	23
neologizm opisujący dokonywanie aktów terroru przy pomocy zdobyczy technologii informacyjnej	24	48%	12	12	6	18	4	19
hakerstwo	23	46%	5	18	5	18	5	18
wirusy i zagrożenie w Internecie	12	24%	2	10	4	8	1	11
atak konwencjonalny, który polega na fizycznym uszkadzaniu elementów systemu komputerowego	6	12%	2	4	1	5	1	5
wyszukiwanie dziur w oprogramowaniu komputerowym	5	10%	1	4	1	4	1	4
nie wiem	0	0%	0	0	0	0	0	0

Źródło: opracowanie własne.

Skoro większość uczniów nie wykazała się znajomością pojęcia „cyberterroryzm" oraz nie potrafiła wskazać, czym on jest, w kolejnym pytaniu zostali oni poproszeni o wskazanie przyczyny tego zjawiska: „Co jest według Ciebie przyczyną zagrożeń cyberterrorystycznych?". Według przeważającej części – 29 osób (58%) – przyczyną zagrożeń cyberterrorystycznych jest przestępczość komputerowa. 18 uczniów (36%) wskazało na politykę rządów, a 13 respondentów (26%) na wirusy komputerowe. Tyle samo osób (26%) było zdania, że przyczyną zagrożeń cyberterrorystycznych jest szybki rozwój technologii, a 24% (12 osób) opowiadało się za piractwem jako przyczyną zagrożeń cyberterrorystycznych. Fundamentalizm religijny wskazało 11 osób (22%). Najmniej osób, 3 (6%), uznało, że nie wie, co jest przyczyną zagrożeń cyberterrorystycznych.

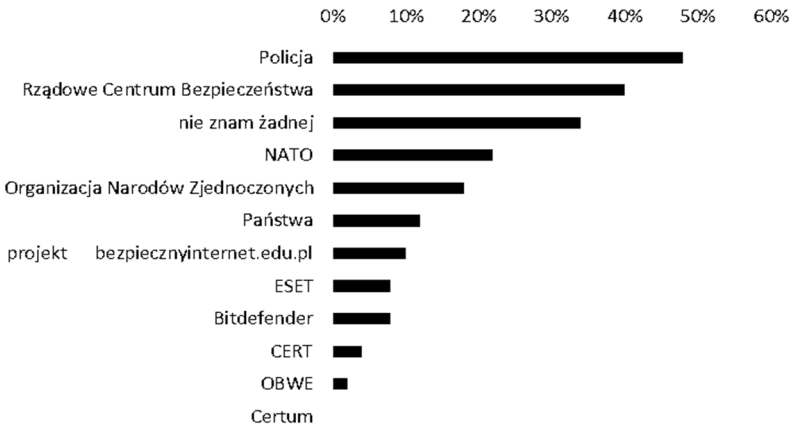
Następne pytanie zawarte w kwestionariuszu ankiety miało za zadanie sprawdzenie, czy młodzi ludzie orientują się, kto może stać się ofiarą działań wynikający z cyberterroryzmu: „Co lub kto według Ciebie może stać się ofiarą cyberterroryzmu?". 33 osoby (66%) stało na stanowisku, że są to przede wszystkim komputery rządowe. 64% respondentów (32 osoby) uważało, że ofiarami mogą być również portale społecznościowe, a 27 osób (54%) podkreśliło, że zagrożone są strony internetowe. 19 respondentów (38%) podkreśliło, że możliwą ofiarą cyberterroryzmu może być przypadkowa osoba, a według 18 osób

(36%) – komputer osobisty. Tylko 9 osób (18%) jako możliwą ofiarę cyberterroryzmu wskazało infrastrukturę krytyczną. Na samym końcu podsumowania wyników (8 osób – 16%) znalazły się organizacje edukacyjne, które są zagrożone tym przestępstwem.

Spośród skutków ataku cyberterrorystycznego (pytanie: „Jakie mogą być według Ciebie skutki ataku cyberterrorystycznego?") najczęściej podkreślonym aspektem – przez 46 osób (92%) – był wyciek tajnych danych, w następnej kolejności była to destabilizacja funkcjonowania państwa – 18 osób (36%). Najrzadziej wybieraną odpowiedzią było przekonanie, że skutkiem ataku może być przetrzymywanie zakładników (3 osoby, czyli 6%) oraz utrata gwarancji na sprzęt komputerowy (6%).

Jedno z ostatnich pytań sprawdzało orientację uczniów dotyczącą organizacji zajmujących się zwalczaniem cyberterroryzmu: „Wymień znane Tobie organizacje, instytucje odpowiedzialne za zwalczanie cyberterroryzmu". Instytucją najbardziej znaną uczniom (wskazało ją 24 respondentów, czyli 48%), która zajmuje się tym procederem, jest policja. Na drugim miejscu znalazło się Rządowe Centrum Bezpieczeństwa (11 osób – 22% ankietowanych). Niepokojącym może wydawać się to, że 17 uczniów (34%) uważa, że nie zna żadnej instytucji lub organizacji odpowiedzialnej za zwalczanie cyberterroryzmu.

Wykres 1. Organizacje i instytucje odpowiedzialne za zwalczanie cyberterroryzmu według młodzieży



Źródło: opracowanie własne.

11 uczniów (22%) zakładało, że za zwalczanie cyberterroryzmu odpowiedzialne jest NATO, a 9 osób (18%) reprezentowało pogląd, że za zwalczanie cyberterroryzmu odpowiedzialne jest ONZ. Tylko 6 ankietowanych, czyli 12%, było zdania, że państwo jest odpowiedzialne za zwalczanie cyberterroryzmu.

Na podstawie badań przeprowadzonych wśród uczniów ze Stargardu można zaryzykować stwierdzenie, że znają oni zagadnienie dotyczące cyberterroryzmu. Większość pytanych prawidłowo wskazała na źródło jego pochodzenia. Jednakże, jak się wydaje, uczniowie

mają małą świadomość tego, że sami mogą być narażeni na atak w cyberprzestrzeni. Pocieszającym jest zaś to, że prawie co drugi uczeń zdaje sobie sprawę z możliwości poszukiwania pomocy u funkcjonariuszy policji, którzy pracują w wyspecjalizowanych komórkach do spraw zwalczania przestępczości i terroryzmu w cyberprzestrzeni.

Zakończenie

Temat użytkowania Internetu i bezpieczeństwa w sieci oraz płynących zagrożeń ze strony cyberterroryzmu jest od kilkunastu lat szczególnie aktualny między innymi na łamach publikacji naukowych. Żyjemy w okresie, w którym tworzy się społeczeństwo informacyjne. Każdy z sektorów gospodarczych jest w coraz szerszym zakresie uzależniony od sieci i systemów informatycznych. Sama dostępność technologii zmienia życie wielu społeczeństw i narodów oraz przyczynia się do popełniania nowych form przestępstw w cyberprzestrzeni.

Bezpieczeństwo w Internecie w głównej mierze zależy od świadomości korzystającego z niego użytkownika, ponieważ skutków ataków cyberprzestępców nie można przewidzieć. Dlatego ważne jest rozpowszechnianie, między inymi wśród młodzieży, wiedzy dotyczącej czyhających w cyberprzestrzeni zagrożeń, tak by w niektórych sytuacjach móc je przynajmniej zminimalizować. Idealny użytkownik sieci to użytkownik świadomy. Problem jednak w tym, że takich użytkowników jest niewielu, ponieważ z Internetu ma prawo korzystać każdy, niezależnie od wieku. Należy zatem już od najmłodszych lat tak edukować użytkowników, aby budować kulturę bezpieczeństwa w sieci, ponieważ najsłabszym ogniwem według ekspertów nie jest sprzęt, tylko człowiek.

Internet to nie tylko same korzyści, lecz również realne zagrożenia mające odniesienie do rzeczywistości. Najbardziej dotkliwym skutkiem cyberataku jest zakłócenie działalności, przy czym należy zwrócić uwagę, że przypadki udanych cyberataków należy rozpatrywać indywidualnie, a ich skutków nie należy bagatelizować.

Aby uniknąć strat albo je zminimalizować, powinno się tworzyć i rozważać różne scenariusze, które usprawnią zabezpieczenie się przed udanym cyberatakiem lub też osłabiają jego skutki. Należy zatem znać zagrożenia oraz środki zaradcze, dzięki którym można osiągnąć bezpieczeństwo danych oraz funkcjonowanie sytemu.

W ramach działalności dotyczącej bezpieczeństwa cyberprzestrzeni Polski, w tym walki z cyberterroryzmem w Polsce, realizuje się między innymi następujące programy:

- Rządowy program ochrony cyberprzestrzeni;
- Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej;
- Krajowy System Reagowania na Incydenty Komputerowe w CRP (CRP – Cyberprzestrzeń Rzeczypospolitej Polskiej).

Oprócz programów powołany został również Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL (www.cert.gov.pl).

Brak odczuwania przez niektóre osoby lub instytucje skutków terroryzmu nie powinien być powodem nieznajomości zagrożenia, tym bardziej że ono narasta. W związku z tym forma terroryzmu, jaką jest cyberterroryzm, powinna stać się obiektem debaty publicznej z udziałem ekspertów, którzy nie powielają błędnych schematów, te bowiem prowadzą do tego, że zwykła przestępczość komputerowa mylona jest z cyberterroryzmem, a sama wiedza na temat cyberterroryzmu jest znikoma lub żadna.

Na podstawie przeprowadzonych badań należy stwierdzić, że powinno się dalej podejmować systematyczne działania edukacyjne nad wdrożeniem programów, które skutkować będą coraz większą odpowiedzialnością uczniów jako użytkowników Internetu i sieci. Szkolenia oraz ćwiczenia przyczynią się do zwiększenia ochrony przed cyberterroryzmem nie tylko wśród uczniów, lecz także wśród innych osób z ich otoczenia. Na koniec nie można zapominać także o uświadamianiu młodzieży, że jakakolwiek działalność w Internecie lub sieci podlega odpowiedzialności karnej.

Bibliografia

Bullying, http://pl.bab.la/slownik/angielski-polski/bullying [4.04.2017].

Deloitte, *Beneath the surface of a cyberattack. A deeper look at business impacts*, 2015, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/ risk/us-risk -beneath-the-surface-of-a-cyber-attack.pdf [10.07.2017].

GUS, *Jak korzystamy z Internetu? 2015*, http://szczecin.stat.gov.pl/download/gfx/ szczecin/pl/defaultaktualnosci/843/6/30/1/jak_korzystamy_z_internetu_2015.pdf [10.09.2017].

GUS, *Opracowanie sygnalne. Społeczeństwo informacyjne w Polsce w 2016 r.*, Warszawa 2016, http://stat.gov.pl/download/gfx/portalinformacyjny/ pl/ defaultaktualnosci/5497/2/6/1/si__sygnalna_2016.pdf [28.04.2017].

Konwencja Rady Europy o cyberprzestępczości, Dz. U. poz. 728, Warszawa, dnia 27 maja 2015 r.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2006.

Malware, https://www.avast.com/pl-pl/c-malware [18.04.2017].

Ministerstwo Spraw Wewnętrznych i Administracji, „Raport o stanie bezpieczeństwa w Polsce w 2015 roku".

Mysior R., *Cyberseks – ciemna strona mediów*, „Problemy opiekuńczo-wychowawcze" 2013, nr 9.

Okopień P., *Informatyka śledcza w obronie przed i po cyberataku*, http://itwiz.pl/ informatyka-sledcza-obronie-przed-po-cyberataku/ [4.07.2017].

Polityka ochrony cyberprzestrzeni Rzeczpospolitej Polskiej, Warszawa, 25.06.2013.

Podraza A., Potakowski P., Wiak K., *Cyberterroryzm zagrożeniem XXI wieku: perspektywa politologiczna i prawna*, Warszawa 2013.

Raport o niektórych zjawiskach związanych z działalnością sekt w Polsce, Warszawa 2000.

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz.U. 2002 nr 156, poz. 1301.

Wawrzak-Chodaczek M., Jagoszewska I., *Komunikacja wobec wyzwań współczesności*, Toruń 2011.

Woś M., *Wychowanie i edukacja chrześcijańska wobec wyzwań socjoglobalistyki*, „Seminare" 2014, nr 2 (35).

Woźniak R.B., *U podstaw socjoglobalistyki. Koncepcje i zagrożenia,* Szczecin 2009.

Grzegorz Gronowicz, Marek Woś

Zagrożenia cyberterrorystyczne w świadomości młodzieży

Rozwój technologiczny, a w tym rozwój Internetu, daje swoim użytkownikom możliwości szybkiej, taniej i globalnej komunikacji, wymiany informacji dzięki systemom teleinformatycznym. W obecnej dobie globalizacja jest procesem intensywnych powiązań oraz wszelkiego rodzaju układów pod względem ekonomicznym, politycznym, ideologicznym, społecznym, prawnym, informacyjnym i ekologicznym.

Młodzież, w coraz większym stopniu uzależniająca się od Internetu i sieci, może stać się ofiarą cyberterroryzmu. Znajomość prawa karnego i zagrożeń ze strony innych użytkowników technologii komunikacyjnej i informacyjnej może przyczynić się do jej bezpieczeństwa. Wiedza na temat instytucji, które specjalizują się niesieniem pomocy w tym zakresie, jest takim gwarantem.

Słowa kluczowe: Internet; cyberterroryzm; młodzież; technologia informacyjna; bezpieczeństwo.

Cyberterroristic threat in teenagers' consciousness

Technological development, including the Internet advance, gives its users possibility of quick, cheap and global communication, exchanging information due to communication and information system. Nowadays, globalization is a strenuous process of connection and various dependents such as: economical, political, ideological, social, legal, informational and ecological.

Teenagers being more addicted to the Internet may become victims of cyberterrorism. Knowing criminal law and threats from other information and communication technology users may cause their safeness. Awareness of institutions which are specialized in giving a hand with this issue is the guarantor.

Keywords: the Internet; cyberterrorism; teenagers; information technology; safety.

Translated by Grzegorz Gronowicz, Marek Woś