Joanna Bieniek
Uniwersytet Mikołaja Kopernika w Toruniu

CYBERTERRORYZM ZAGROŻENIEM BEZPIECZEŃSTWA PAŃSTW WSPÓŁCZESNEGO ŚWIATA

STRESZCZENIE

Praca w szczególności dotyczy zagrożeń jakie wiążą się z cyberterroryzmem wielu państw na świecie. Żeby wyjaśnić to pojęcie najpierw trzeba się odnieść do samej definicji terroryzmu oraz jak w dobie globalizacji to zjawisko stało się problemem o międzynarodowym znaczeniu. W pierwszym rozdziale chciałabym przedstawić genezę powstania terroryzmu oraz opisać poszczególne zjawiska jakie temu towarzyszą. Rozdział drugi w całości poświęcony będzie cyberterroryzmowi oraz jak zinformatyzowanie życia wpływa na jego rozwój. W XXI wieku przestępczość komputerowa cały czas ewoluuje. Jest większa komputeryzacja w każdej dziedzinie życia, dlatego ważnym jest, aby starać się temu przeciwdziałać. Trzeci rozdział opisuje przykłady dzisiejszych ataków cyberterrorystycznych w różnych państwach. W każdej dziedzinie życia cyberataki stają się rzeczywistością, dlatego ważnym jest, aby pamiętać o bezpieczeństwie oraz stosować odpowiednie zabezpieczenia, które pomogą uchronić się przed cyberterroryzmem.

Słowa kluczowe:
terroryzm, cyberterroryzm, bezpieczeństwo

WSTĘP

Celem mojej pracy jest przedstawienie nowej formy zagrożenia terrorystycznego jakim jest cyberterroryzm. Ukazanie tej problematyki jest ważne, dlatego że wraz z postępem technologicznym i rozbudową infrastruktury informatycznej na całym świecie, zagrożenie cyberataków wciąż rośnie. W dzisiejszych czasach praktycznie każdy z nas ma dostęp do internetu. Jak każde narzędzie, internet może być przeznaczony do codziennego użytku, m.in. do komunikacji, nauki czy pracy. Niestety może również służyć do prowadzenia działań terrorystycznych. Coraz częściej w mediach pojawiają się informacje

o atakach w cyberprzestrzeni. Cyberterroryzm jest największym zagrożeniem współczesnego świata, ponieważ może uderzać w różne organizacje rządowe lub w wybrane instytucje. Może być tak samo niebezpieczny jak atak rakietowy na dane państwo.

TERRORYZM

Już od dawna terroryzm jest zjawiskiem, które towarzyszy społeczeństwu praktycznie na każdym kroku. W ostatnich czasach problem terroryzmu dynamicznie się rozwija, a środki masowego przekazu coraz częściej informują nas o nowym zagrożeniu. Na początek jednak należy zdefiniować samo pojęcie terroryzmu, aby wiedzieć jak je rozumieć. Sformułowanie to sprawia wiele problemów wśród naukowców, ponieważ źle podana definicja może całkowicie zmienić jego znaczenie[1].

„Terroryzm jest to różnie umotywowane ideologicznie, planowane i zorganizowane działanie pojedynczych osób lub grup, skutkujące naruszeniem istniejącego porządku prawnego, podjęte w celu wymuszenia od władz, państw i społeczeństw określonych zachowań i świadczeń, często naruszające dobra osób postronnych; działania te są realizowane z całą bezwzględnością za pomocą różnych środków (naciski psychologiczne, przemoc fizyczna, użycie broni i ładunków wybuchowych) w warunkach specjalnie nadanego im rozgłosu i celowo wytworzonego w społeczeństwie lęku"[2].

Terroryzm to nie tylko zagrożenie dla życia wydzielonych jednostek, ale jest on poważnym problemem współczesnego świata. Zagraża nie tylko społecznemu porządkowi, ale i również stosunkom międzynarodowym. Wraz z dynamicznym rozwojem terroryzmu w przyszłości może on być trudny do wyeliminowania. Jest to swoistego rodzaju narzędzie, które potrafi dostosować się do zmieniających się warunków. Dziś możemy sobie tylko wyobrazić jak w dobie globalizacji i coraz większego postępu technologicznego może to wszystko wyglądać[3].

Współczesny terroryzm jest nastawiony na ogrom zniszczeń oraz na coraz większą liczbę ofiar, co sprawia, że staje się on bardziej agresywny. Z tej perspektywy terroryzmu pojawia nam się obraz dzisiejszego terrorysty, który jest gotów działać w imię ustanowionych zasad i celów. Człowiek taki jest pełen przemocy i agresji[4].

---

[1] R. Kosta, *Terroryzm jako zagrożenie dla bezpieczeństwa cywilizacji zachodniej w XXI wieku*, Toruń 2012, s. 11.
[2] Ibidem, s. 13.
[3] K. Liedel, P. Piasecka, *Jak przetrwać w dobie zagrożeń terrorystycznych*, Warszawa 2008, s. 8.
[4] P. Dudczak, *Terroryzm we współczesnym świecie*, w: *Oblicza terroryzmu*, Kraków-Rzeszów-Zamość 2011, s. 233.

„Terrorystom nie chodzi przecież o zabijanie pana A ani pana B, ale o pokazanie siły i determinacji - tego, że są zdolni do wszystkiego. Ciągle jest to przemoc, bo choć stosują oni agresywne środki, to motywem pozostaje chęć podporządkowania sobie innych. Nam nie chodzi o zabijanie niewinnych, ale... - mówią często terroryści. Ci "lepsi" podkładają bomby tam, gdzie nie ma ludzi, albo detonują je w nocy"[5].

Terrorysta tak na prawdę jest podporządkowany idei grupy, do której należy. Niektórzy z nich są okłamywani i zagubieni. Nie wiedzą do końca, że dokonując zamachu, oni też muszą w nim zginąć. Jednak Ci terroryści, którzy zabijają dla swojego Boga lub dla swojej ideologii nie mogą być umieszczeni w jakiejkolwiek kategorii człowieka. Odnosząc się do podstawowych kryteriów jakimi posługują się terroryści na pierwszym miejscu możemy postawić ideologię, następnie cel do jakiego dążą, trzecim kryterium jest przemoc, a co za tym idzie liczne ataki na dane obiekty oraz historia z jaką wiąże się dana grupa terrorystyczna[6].

Wracając jednak do samego pojęcia terroryzmu możemy stwierdzić, że nie jest to zjawisko jednorodne. Dzieli się na różne kategorie oraz przybiera różne formy. Najbardziej rozpoznawalnym jest terroryzm tradycyjny, którego ideologia dąży do zdobycia przez terrorystów największego poparcia oraz na znalezieniu jak największej liczby osób, które będą z nimi sprzymierzeni oraz pomogą im w realizacji celów w danej grupie terrorystycznej. Grupy terrorystyczne zawsze mają swojego zarządcę, który znajduje się na najwyższym szczeblu. Terroryzm tradycyjny dzieli się również na podkategorie, do których należy terroryzm ideologiczny (prawicowy, lewicowy), socjalno-rewolucyjny oraz etniczno-nacjonalistyczny. Innym rodzajem terroryzmu, który dominuje w dzisiejszym świecie jest terroryzm religijny[7].

Wyróżniamy również terroryzm polityczny, który połączony jest z różnorodnymi poglądami politycznymi oraz terroryzm przestępczy, który często ma charakter kryminalny, a osoby, które dopuszczają się danego czynu mogą być zwykłymi przestępcami. Ze względu na cel ataku istnieje terroryzm ekonomiczny, których celem jest wyrządzenie jak największych szkód i zniszczeń, terroryzm indywidualny, który wymierzony jest w konkretne osoby (np. przywódcy polityczni) oraz terroryzm masowy, którego ofiarami są najczęściej przypadkowe osoby[8]. Wyodrębnienie jakie klasyfikuje terroryzm do kryterium postmodernistycznego jest określenie cyberterroryzmu. Jest on związany z używaniem technik informatycznych czego powodem jest ciągły rozrost sieci

[5] K. Brunetko, *Terrorysta - kto to taki?*, http://www.tygodnik.com.pl/kontrapunkt/28-29/kubacka.html, (dostęp: 29.03.2020r.)
[6] P. Dudczak, op. cit., s. 234.
[7] S. Pikulski*, Prawne środki zwalczania Terroryzmu*, Olsztyn 2000, s. 18.
[8] T. Aleksandrowicz, *Terroryzm międzynarodowy*, Warszawa 2008, s. 23.

internetowej. W przyszłości może to wiązać się z coraz większym zagrożeniem, ponieważ każde, nawet najmniejsze przedsiębiorstwo lub instytucja rządowa opiera się w większości o rozwiązania sieciowe[9].

Ze względu na taktykę walki wyróżniamy terroryzm represywny, który polega na zastraszeniu swojego lub okupowanego narodu. Celem tego jest w szczególności wymuszenie poparcia. Kolejnym jest terroryzm ofensywny, który za pomocą szantażu politycznego poszczególnych władz dąży do zmian obecnej sytuacji w kraju na inną, być może lepszą. Ze względu na taktykę walki wyróżniamy również terroryzm defensywny, który jest odpowiedzią na działanie nieprzyjaciela mająca ograniczyć jego atak[10].

Do rodzajów terroryzmu często przyporządkowany jest również terroryzm medialny. Jak wiemy terrorystom chodzi głównie o rozgłos, dlatego nie można mieć wątpliwości, iż to właśnie jest głównym czynnikiem strategii terrorystycznej. Samo słowo medialność dużo mówi o reklamie i marketingu, a w szczególności o rozgłosie danego produktu w mass mediach. Informacja medialna ma za zadanie przekazać wiadomość, która będzie miała wysoką oglądalność oraz będzie zarówno sensacyjna jak i spektakularna. Media niemal od zawsze posiadają nieograniczone środki, jeśli chodzi o przekazywanie informacji. Coraz częściej jesteśmy świadkami jak środki masowego przekazu mają większy udział w terroryzmie. Mamy do czynienia z demonstrowaniem siły oraz przedstawianiem charakteru przemocy w reklamach. Gdy tylko włączymy telewizor od razu wiemy co i gdzie się stało. Za pomocą mediów społeczeństwo ma dostęp do wszystkich informacji jakie dzieją się na świecie. Terroryści stosują swojego rodzaju strategię komunikacyjną, którą przekazują do opinii publicznej oraz do rządów. Celem zamachu nie jest sama przemoc, lecz wywołanie efektu użytej przemocy. Niestety jest to zjawisko, którego nie jesteśmy w stanie uniknąć[11].

Kluczową płaszczyzną, która służy przedstawieniu oraz zrozumieniu sensu i specyfiki współczesnego terroryzmu jest poznanie jego głównych celów. Jak już wcześniej zostało wspomniane podstawowym celem terroryzmu jest wzbudzenie strachu i zdobycie przewagi nad świadkami aktu terrorystycznego. Aby dotrzeć do publiczności, terroryści tak planują dany atak, aby zgromadzić wokół siebie prasę, telewizję czy radio. Takim sposobem chcą zwrócić na siebie uwagę oraz na ich postulaty i działalność. Innym celem terrorystów jest "uznanie istnienia". Starają się bowiem o rozgłos w celu uzyskania jak największego poparcia. Kolejnym aspektem jest "uznanie praw", w których sprawcom chodzi o uznanie akceptacji lub usprawiedliwienie dla własnych inicjatyw lub działań. Terroryści dążą również do społecznego przyzwolenia, w którym

[9] Ibidem, s. 24.
[10] S. Pikulski, op. cit., s. 19.
[11] T. Aleksandrowicz, op. cit., s. 27.

mogliby przeprowadzać zmiany w państwie. W głównej mierze może wiązać się to z przejęciem pełnej władzy w państwie[12].

W każdym ataku terrorystycznym cele pierwotne (główne) i cele instrumentalne (uboczne, pośrednie) są precyzowane. Cel pierwotny charakteryzuje się zmuszaniem do umotywowanych zachowań rządu, partii, różnych przedstawicieli władzy lub grupy społecznej. Do celu pierwotnego należy m.in. uzyskanie kompromisu lub korzyści, do których należy pokrycie okupu, zwolnienie zatrzymanych więźniów lub zamieszczenie orędzia terrorystów. Kolejnym jest wcześniej wspomniana "reklama", gdzie terrorystom chodzi o zwrócenie na siebie uwagi. Chcą oni w ten sposób dokładnie przedstawić sprawę, o którą walczą. Innym celem pierwotnym jest sianie zamętu, zastój istniejącego ustroju oraz wywołanie ucisków oraz szykanów ze strony rządu, co może być powodem utraty rozgłosu. Kolejnym celem jest wymuszenie posłuszeństwa i ustępliwości oraz wywołanie poczucia winy. Obok celów pierwotnych stoją cele pośrednie, które osiągane są przez terrorystów poprzez zachowania przestępcze skierowane na człowieka, środowisko lub rzecz. Ta strategia oparta jest na załamaniu psychologii odbiorców, która jest okazywana w sposób drastyczny. Oddziałuje na psychikę ofiar oraz sprawia, że sposób ten jest z reguły nieprzewidywalny. Do strategii celu pośredniego należy również wybór przypadkowych, często niewinnych osób. Kolejnym jest wybór miast jako zasadniczego teatru działań, ponieważ to w nich są wielkie skupiska ludności[13].

Formy przemocy jakie stosują terroryści to m.in. zamach na życie, który dokonywany jest najczęściej na osobach publicznych takich jak: policjanci, żołnierze, przywódcy partii politycznych oraz urzędnicy administracji rządowych. Inną formą jest zamach bombowy, który przyczynia się do wywierania presji na społeczeństwie. Następną formą jest uprowadzenie pojazdu lub samolotu wraz z zakładnikami, a w efekcie końcowym rozbicie go we wcześniej zaplanowanym miejscu. Następnie jest to uprowadzenie osoby (kidnaping), która ma być wykorzystana jako element przetargu dla spełnienia żądań sprawców. Ostatnią formą przemocy jest więzienie zakładników[14].

Terroryści w szczególności stosują broń konwencjonalną, najczęściej jest to automatyczna broń ręczna, granaty oraz ładunki wybuchowe. Wraz z rozwojem technicznym i technologicznym używana przez sprawców broń jest stale modyfikowana. Stosują oni coraz lepsze materiały wybuchowe, dokładniejsze zapalniki czasowe lub odpalane zdalnie detonatory. Wykorzystanie coraz nowszych rozwiązań technicznych przez terrorystów sprawia, że działania

[12] S. Wojciechowski, *Terroryzm na początku XXI wieku. Pojęcie, istota i przyczyny zjawiska*, Bydgoszcz-Poznań 2011, s. 83.
[13] K. Liedel, P. Piasecka, op. cit., s. 24, 25.
[14] S. Wojciechowski, op. cit., s. 90.

i akcje przez nich zaplanowane są dokładniejsze oraz bardziej zsynchronizowane. Co za tym idzie, iż służby antyterrorystyczne stale muszą doskonalić swoje środki, aby starać się zapobiegać działaniom terrorystów. W największym stopniu rozpowszechniony jest atak z użyciem tzw. "bomb samochodowych". Spełnia to podstawowe warunki, czyli umieszczenie ładunku we wcześniej ustalonym miejscu, ma dużą siłę rażenia oraz pochłania ogromną liczbę ofiar. Obecnie terroryści atakują po to, aby zademonstrować swoją siłę[15].

Cele ataków to nie tylko określenie stanu, jaki chcą osiągnąć, ale również cel fizyczny w jaki chcą uderzyć. Cele te są podzielone na twarde i miękkie. Cele twarde to takie, które są dobrze chronione przez infrastrukturę krytyczną państwa oraz są dobrze zabezpieczone. Uderzenie w taki cel może spowodować dla zaatakowanego przerwę w dostawie wody, prądu, a nawet żywności. Do infrastruktury krytycznej państwa zalicza się: władzę centralną, służbę zdrowia i system ratowniczy, surowce energetyczne, transport, energetykę, systemy wodociągowo-kanalizacyjne i dystrybucji żywności, sektor bankowo-finansowy oraz usługi informacyjne i łączność. Ważnym jest, aby ta infrastruktura była dobrze chroniona, ponieważ atak nawet na jedną z nich może przyczynić się do poważnych strat. Cele miękkie to takie, które nie wpływają bezpośrednio na funkcjonowanie systemu państwowego, lecz destabilizują działalność społeczeństwa. Do tego celu zalicza się wydarzenia lub obiekty, w których ofiarami są tysiące ludności oraz obiekty o znaczeniu symbolicznym lub historycznym z punktu widzenia państwa. Celami takich ataków są hipermarkety, obiekty religijne, węzły i środki transportu publicznego oraz budynki kulturalne, np. teatr, kino, stadion sportowy lub hala widowiskowa[16].

Działania terrorystyczne są często nieprzewidywalne, a ich rewolucyjność przyczynia się do intensyfikacji niebezpieczeństwa poprzez użycie broni masowego rażenia. Terroryści planując atak są w posiadaniu środków biologicznych, chemicznych oraz atomowych. Terroryzm ten wzbudza wśród ludności niepewność oraz strach. Terroryzm odnosi się również do zjawiska, które w XXI wieku jest coraz bardziej rozpowszechniane, a czasami nawet częściej stosowane niż zwyczajny atak terrorystyczny. Mowa tu o rzeczywistości wirtualnej. Żyjemy bowiem w świecie, który na przestrzeni lat coraz bardziej jest związany z przestrzenią internetową. To właśnie na działaniach sieci komputerowych opierają się m.in. szpitale, oczyszczalnie ścieków, ujęcie wody pitnej oraz elektrownie. Komputer w rękach terrorysty może stać się bronią masowego rażenia oraz jednym kliknięciem jest on w stanie zatrzymać sprawne działanie tych sieci[17].

[15] Ibidem, s. 92, 93.
[16] K. Liedel, P. Piasecka, op. cit., s. 27.
[17] Ibidem, s. 28.

CYBERTERRORYZM

Pod koniec XX i na początku XXI wieku gwałtownie zaczął się rozrastać postęp cywilizacyjny. Przemiany społeczne, polityczne i kulturowe nie są jedynymi jakie miały miejsce w XX wieku. Przede wszystkim są to zmiany z obszaru nowych technologii, komputerów oraz Internetu. Zmiany te wynikają z ogólnoświatowych narzędzi wytwarzania, przetwarzania i przekazywania informacji, które są respektowane za jeden z najważniejszych części przekształceń z obszaru nowych technologii. Wraz z postępem rozwoju informacji, komputerów i zaawansowanej technologii coraz więcej państw, które wcześniej nie miały dostępu do tego typu rozwiązań, zaczęły korzystać z tych dobrodziejstw.

W dobie globalizacji, gdzie rozwijają się procesy prowadzące do integracji państw jak i społeczeństwa, najpowszechniejszym i najbardziej wpływowym środkiem przekazu jest Internet. Jest to przyczyna, która uzależnia nas od postępujących technologii informatycznych. Praktycznie na co dzień jesteśmy z nim powiązani, czy to przez zakupy, sprawdzanie poczty elektronicznej, w usługach bankowych, czy nawet w pracy. Często, gdy chcemy zasięgnąć jakiejś rady lub nawiązać z kimś kontakt też korzystamy właśnie z Internetu. W dzisiejszych czasach nie musimy nawet wychodzić z domu, aby załatwić, np. sprawę urzędową. W sieci możemy nawet znaleźć naszą drugą połówkę. Jak widać Internet jest obecny we wszystkich sferach życia i korzystamy z niego praktycznie cały czas 24 h/7. Jednak fakt, iż każdy może mieć do niego dostęp jest niepokojący, ponieważ może to przysporzyć wiele niebezpieczeństw. Coraz częściej słyszymy o rozwijającej się działalności grup przestępczych[18]. Są to popularnie zwani włamywacze sieciowi, czyli hakerzy i crackerzy. Haker poszukuje sposobów dostępu do strzeżonych systemów w celu zwiększenia swojej wiedzy i zdobycia nowych doświadczeń. Jest to profesjonalista w dziedzinie bezpieczeństwa systemów komputerowych. Natomiast cracker łamie zabezpieczenia oprogramowania oraz włamuje się na serwery w sposób niezgodny z prawem. Różnica między hakerem, a crackerem jest dość spora, ponieważ haker to przede wszystkim pasjonat o dużej wiedzy, który nie wykorzystuje jest po to, by szkodzić innym. Cracker poprzez łamanie zabezpieczeń i kradzieży danych z serwera dokonuje przestępstwa. Jednak mimo odmiennej linii podziału między tymi dwoma znaczeniami, nie należy lekceważyć tego zagrożenia. Niekontrolowany przebieg współczesnej technologii, jak i informatyzacja spo-

[18] E. Szulc-Wałecka, *Znaczenie cyberterroryzmu we współczesnym świecie*, w: *Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja)*, pod. red. M. Marczewskiej-Rytko, Lublin 2014, s. 277.

łeczeństwa powodują, że większość państw na świecie musi liczyć się z coraz większym niebezpieczeństwem związanym z cyberterroryzmem[19].

Tabela 1. Światowe użytkowanie Internetu i statystyka populacji. Szacunki na koniec 2019r.

Lp.	Regiony świata	Ludność (szacunki 2020)	%Populacji na świecie	Użytkownicy Internetu 31 grudnia 2019r.	Współczynnik penetracji (% pop.)	Wzrost 2000-2020	Świat w Internecie %
1.	**Afryka**	1 340,598,447	17,2%	526,374,930	39,3%	11,559%	11,5%
2.	**Azja**	4 294,516,659	55,1%	2 300 469 859	53,6%	1,913%	50,3%
3.	**Europa**	834,995,197	10,7	727,814,272	87,2%	592%	15,9%
4.	**Ameryka Łacińska/Karaiby**	658,345,826	8,5%	453,702,292	68,9%	2,411%	10,0%
5.	**Bliski Wschód**	260 991 690	3,9%	180 498 292	69,2%	5,395%	3,9%
6.	**Ameryka Północna**	368,869,649	4,7%	348,908,868	94,6%	222%	7,6%
7.	**Australia/Oceania**	42 269 838	0,5 %	28 775 373	67,4%	277%	0,6%
8.	**World total**	7,796,615,710	100,0%	4,574,150,134	58,7%	1,167%	100,0%

Źródło: Internet World Status, www.Internetworldstats.com (02.04.2020).

Z powyższej tabeli wynika, iż nie ma już kontynentu, który nie jest podłączony do Internetu. Rozwój sieci internetowej jest gwałtowny, a wykorzystanie go jest coraz bardziej wszechstronne.

Tabela 2. Użytkowanie Internetu w Europie - Top 10. Stan na marzec 2019r.

Lp.	Państwo	Miliony użytkowników
1.	Niemcy	72,1
2.	Wielka Brytania	63,0
3.	Francja	60,4

[19] A. Gniadek, *Cyberprzestępczość i cyberterroryzm - zjawiska szczególnie niebezpieczne*, w: *Cyberterroryzm nowe wyzwania XXI wieku*, pod. red. T. Jemioły, J. Kisielnickiego, K. Rajchela, Warszawa 2009, s. 221.

4.	Włochy	54,8
5.	Hiszpania	42,9
6.	Polska	29,7
7.	Holandia	16,3
8.	Rumunia	14,3
9.	Belgia	10,8
10.	Szwecja	9,6

Źródło: Opracowanie własne na podstawie: Internet World Status, www.Internetworldstats.com (02.04.2020).

Wiemy już, że większy udział społeczeństwa w sieci i rozwój nowoczesnych technologii jest przyczyną rozwoju cyberterroryzmu. Aczkolwiek żeby dokładniej zrozumieć to zjawisko trzeba wyjaśnić jego pojęcie. Cyberterroryzm jest to połączenie słowa "terroryzm" i przedrostka "cyber", ponieważ należy do zaawansowanej technologicznie kategorii tradycyjnego terroryzmu. Określenie to nie jest zjawiskiem nowym, ponieważ pierwsze komunikaty o zagrożeniu zamachów terrorystycznych przy użyciu systemów komputerowych zaczęły pojawiać się w 1979 roku przez Szwedzkie Ministerstwo Obrony. Ministerstwo zalecało zaangażowanie rządu w nadzorowanie publicznych oraz prywatnych sieci komputerowych. Od tego momentu systematycznie mówiono o niebezpieczeństwie wymierzonym w społeczeństwo za pomocą systemów komputerowych. W latach 80., amerykańscy specjaliści w wywiadzie wojskowym również uprzedzali przed cybernetycznymi atakami na infrastrukturę teleinformatyczną Stanów Zjednoczonych[20].

W latach 90. XX wieku w Stanach Zjednoczonych coraz częściej zaczęto pisać o atakach cyberterrorystów. Obawa przed ich atakiem sprawiła, że w 1996 roku Prezydent Stanów Zjednoczonych Bill Clinton nakazał stworzenie ochrony "Krytycznej Infrastruktury". Działania cyberterrorystów zagrażały m.in. systemom bankowym, telekomunikacji, administracji rządowym, systemowi komputerowemu służb ratowniczych, transportowi wodnemu, lądowemu i powietrznemu oraz zagrażały instytucjom odpowiedzialnym za dostarczanie energii elektrycznej, gazu i wody. Zagrożenie dla bezpieczeństwa państwa przyczyniło się do powstania w 1998 roku Centrum Ochrony Infrastruktury Narodowej w centrali FBI, którego obowiązkiem było zabezpieczenie infrastruktury państwa przed zagrożeniami lub zamachami. Po 2001 roku zauważono wzrost zamachów na systemy komputerowe państw, które są w konflikcie politycznym lub zbrojnym. Cyberataki mogą modyfikować strony

[20] M. Szewczyk, *Cyberterroryzm jako zagrożenie współczesnego świata*, w: *Cyberterroryzm nowe wyzwania XXI wieku*, pod. red., T. Jemioły, J. Kisielnickiego, K. Rajchela, Warszawa 2009, s. 37, 38.

internetowe WWW lub rozpowszechniać wirusy. To właśnie komputer jest narzędziem, który umożliwia popełnienie przestępstwa[21].

Wracając jednak do meritum, cyberterroryzm to przede wszystkim:

„Groźba lub bezprawny atak wymierzony w system informatyczny lub zgromadzone dane, w celu zastraszenia czy wymuszenia na władzach państwowych lub jej przedstawicielach ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych celów (np. politycznych). Aby działania takie zostały zakwalifikowane jako terroryzm informacyjny, atak powinien powodować znaczne straty lub takie skutki, które wywołują powszechne poczucie strachu"[22].

Zatem atak cyberterrorystyczny to taki, który wyrządza szkody człowiekowi oraz wywołuje u niego strach. Inną definicją cyberterroryzmu jest:

"Akt kryminalny popełniony przy użyciu komputera i możliwości telekomunikacyjnych, powodujący użycie siły, zniszczenie i/lub przerwanie świadczenia usług dla wywołania strachu, poprzez wprowadzenie zamieszania lub niepewności w danej populacji, w celu wpływania na rządy, ludność tak, aby wykorzystać ich reakcje dla osiągnięcia określonych celów politycznych, społecznych, ideologicznych lub głoszonego przez terrorystów programu"[23].

Zgodnie z powyższymi definicjami można stwierdzić, że cyberterroryzm jest obecnie jednym z największych zagrożeń XXI wieku i występuje, gdy:

- celem ataku są systemy informacyjne, komputery, bazy danych,
- dochodzi do politycznie motywowanego ataku przeprowadzonego za pomocą sieci teleinformatycznych,
- dochodzi do destrukcji i dezorganizacji życia danej społeczności, jakim jest atak na Infrastrukturę Krytyczną Państwa (IKP),
- mamy do czynienia z atakiem na systemy energetyczne, zaopatrzenia w wodę, zdrowia, łączności, transportu, bankowości, zaopatrzenia w żywność,
- powoduje krytyczne skutki oraz zniszczenia.

Zjawisko to stanowi krytyczne położenie bezpieczeństwa informacyjnego dla jednostek organizacyjnych państwa lub węzła międzynarodowego[24].

[21] Ibidem, s. 39.
[22] E. Szulc-Wałecka, op. cit., s. 279.
[23] Ibidem, s. 280.
[24] E. Lichocki, *Cyberterroryzm państwowy i niepaństwowy - początki, skutki i formy*, w: *Ewolucja terroryzmu na przełomie XX i XXI wieku*, pod. red., K. Szalewskiej, Gdańsk 2009, s. 161.

Tabela 3. Powody, które mogą skłonić terrorystów do ataków w cyberprzestrzeni.

Powód terrorystycznego ataku w cyberprzestrzeni	**Wywierany wpływ na bezpieczeństwo informacyjne**	**Identyfikacja zagrożeń**
Niskie koszty przeprowadzenia ataku	Każdy może zostać cyberterrorystą. Wystarczy mieć komputer lub laptopa, odpowiedni program i trochę umiejętności.	Infrastruktura krytyczna państwa: - sektor energetyczny, - system zaopatrywania w wodę, - transport wodny, lądowy i powietrzny, - system i sieci teleinformatyczne, - łączność, - służby ratownicze, - zaopatrzenie w żywność, - bankowość i finanse, - urzędy państwowe, - przemysł istotny dla gospodarki, - narodowe pomniki i pamiątki.
Działania nad wyznaczonymi granicami państw	Nie wiadomo, skąd pochodzi atak i kto za nim stoi.	
Przewidywanie zagrożeń ataków	Nie wiadomo, które zagrożenie jest realne, a które tylko pozorne.	
Wykrycie i zlokalizowanie cyberataków	Nie wiadomo, jakie są zdolności i intencje atakujących.	
Cel ataku	Nie wiadomo, co będzie dokładnie celem ataku ani w jaki sposób będzie on wykonany.	
Budowa koalicji	Nie wiadomo, kto jest w koalicji, a kto jest nieprzyjacielem.	

Źródło: E. Lichocki, Cyberterroryzm państwowy i niepaństwowy - początki, skutki i formy, w: Ewolucja terroryzmu na przełomie XX i XXI wieku, pod. red., K. Szalewskiej, Gdańsk 2009, s. 162.

Należy zwrócić szczególną uwagę na coraz częstsze występowanie cyberataków ze względu na niskie straty terrorystów. Wiąże się to z wyższymi korzyściami niż w przypadku zwykłego ataku terrorystycznego. Żeby wykonać atak na sieć potrzebny jest jedynie komputer, dostęp do Internetu i trochę umiejętności technicznych. Zakłada się, iż doskonałe zaplecze do prowadzenia cyberterroryzmu stanowią studenci wielu europejskich i amerykańskich uczelni, którzy po zakończeniu studiów dysponują wiedzą, którą mogli by wykorzystać właśnie do ataku. Identycznie jak wiele innych organizacji przestępczych wykorzystują podsłuchy linii teleinformatycznych, transmisji internetowych itp. Jako ukierunkowane cele wybierają sobie systemy bankowe, centra elektroniki medycznej oraz węzły zasilania energią. Raport Zgromadzenia Parlamentarnego NATO przestrzega przed wzrostem ataków cyberterrorystycznych na systemy informatyczne[25].

[25] M. Białkowski, *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Warszawa 2016, s. 183.

Obiektem tradycyjnego ataku jest przede wszystkim oprogramowanie przeciwnika (software) oraz sprzęt komputerowy (hardware) i systemy informacyjne. Mając na uwadze rozmaite kryteria wyżej wymienionych zjawisk oraz ich metody funkcjonowania trzeba przyznać, iż nie istnieje jednoznaczna klasyfikacja, która wyczerpałaby wszystkie metody zainicjowania akcji w cyberprzestrzeni[26]. Formą działań w cyberprzestrzeni są niżej wymienione kategorie:

- Steal passwords – uzyskanie haseł dostępu do sieci,
- Social engineering – wykorzystanie niekompetencji osób mających dostęp do systemu,
- Bugs and backdoors – używanie systemu bez specjalnych zezwoleń bądź stosowanie oprogramowania pochodzącego z nielegalnych źródeł,
- Authentication failures – wykorzystanie luk w zbiorze reguł sterujących wymianą informacji pomiędzy dwoma lub wieoma niezależnymi urządzeniami lub procesami,
- Information leakage – zdobycie informacji dostępnych tylko dla administratora, niezbędne dla właściwego funkcjonowania sieci,
- Denial of Service – uniemożliwienie korzystania z systemu jego użytkownikom,
- Corruption – nieuprawniona zmiana informacji,
- Leakage – gdy informacja znalazła się tam, gdzie nie powinna,
- Denial – gdy komputer lub sieć nie nadają się do użytkowania,
- External Information Theft – przeglądanie oraz kradzież informacji przez osobę spoza systemu,
- External Abuse of Resources – zniszczenie twardego dysku,
- Masquerading – podawanie się za kogoś innego,
- Pest Programs – zainstalowanie złośliwego programu,
- Bypassins Authentication or Authority – złamanie haseł,
- Authority Abuse – fałszowanie danych,
- Abuse Through Inaction – celowe prowadzenie złego zarządzania,
- Indirect Abuse – używanie innych systemów do stworzenia złośliwych programów[27].

Wyżej wymieniona klasyfikacja pokazuje nam w pewnym świetle jakie mogą być zastosowane formy ataków cybernetycznych. Różnorodność pojęć dowodzi, że cyberprzestrzeń ma wielkie znaczenie. XXI wiek to przede wszystkim pojawienie się nowych technologii, w których formy coraz bardziej się po-

[26] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, Zeszyty Naukowe Akademii Marynarki Wojennej 2005, nr 1 (160), s. 180.
[27] Ibidem, s. 181.

szerzają i wzajemnie uzupełniają. Dzięki temu możemy zauważyć jak szybko rozwija się cyberterroryzm[28].

Analizując zagadnienia związane z cyberterroryzmem nie można pominąć metod jakie są związane z atakami w cyberprzestrzeni. Najważniejsze z nich to:

- phishing – czynność polegająca na wysyłaniu szkodliwych wiadomości e-mail (spamu) do danej osoby, które służą do kradzieży tożsamości,
- komputerowe robaki, bakterie oraz wirusy,
- bomby logiczne – uruchamiają one dodatkowe funkcje elementu logicznego komputera, a tym samym zakłócają jego działanie,
- konie trojańskie – programy wykonujące działania niezależnie od woli użytkownika,
- chipping – uzyskanie dostępu poprzez doinstalowanie dodatkowych chipów,
- "tylne drzwi" – wejście do systemu z ominięciem jego warstwy ochronnej,
- spoofing – podszywanie się,
- hijacking – polegający na przechwyceniu transmisji pomiędzy dwoma systemami,
- sniffing – śledzenie ruchów w sieci, podsłuchiwanie,
- receptor van Eycka – podglądanie repliki obrazów wyświetlanych na monitorze dzięki wykorzystywaniu efektu wysyłania przez monitor silnego sygnału elektromagnetycznego,
- DOS (Denial of Service) – odmowa usługi przez blokowanie pojedynczej usługi sieciowej lub też blokada pracy całego serwera, czasami za pomocą przeciążenia go niezliczoną ilością pytań,
- broń częstotliwości radiowej (radio frequency), czyli urządzenia emitujące promieniowanie elektromagnetyczne, które należy do tzw. widma radiowego używanego do niszczenia technicznych urządzeń elektronicznych, jak i zbiorów informatycznych,
- flooding – wysyłanie do atakowanego komputera takiej liczby żądań, której ten nie jest w stanie obsłużyć
- spamming[29].

Cyberterroryzm może to być zarówno podłożenie bomby w strategicznym miejscu, jak i atak na Infrastrukturę Krytyczną Państwa, zakłócając przy tym działania wszystkiego co oparte jest na łączach internetowych. Trzeba również pamiętać, iż im bardziej rozwinięte państwo to tym bardziej narażone

[28] E. Szulc-Wałecka, op. cit., s. 282.
[29] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2006, s. 38, 39, 40.

jest na niebezpieczeństwo, które płynie ze stale rozwijających się technicznych możliwości. W państwie wysoko rozwiniętym większość instytucji jest nadzorowana przez zintegrowane systemy łączności[30]. Faktem jest również powiązanie ze sobą systemów komputerowych, które są od siebie zależne. Włamanie lub uszkodzenie jednego z nich może spowodować tzw. reakcję łańcuchową. Jest to bardzo niebezpieczne, ponieważ systemy komputerowe danych instytucji, czy przedsiębiorstw przestaną działać tam, gdzie tylko to będzie możliwe[31].

DZISIEJSZE ATAKI CYBERTERRORYSTYCZNE

Aby zrozumieć zagrożenie jakie stanowią ataki cyberterrorystyczne, trzeba zaobserwować jak na przestrzeni lat ich liczba cały czas wzrasta. Pierwszy zmasowany cyberatak w historii był przeprowadzony przeciwko Estonii w 2007 roku, gdzie na kilka tygodni były zablokowane strony mediów estońskich, władz państwowych i banków[32]. W trakcie trwania ataków została utworzona jednostka Estonian Computer Emergency Response Team, której celem była obrona przed cyberatakami. Cel sprawców został spełniony, bowiem pokazali oni jak bezbronne w styczności z cyberterroryzmem może być społeczeństwo tak małego kraju. Ówczesny prezydent Estonii Toomas Hendrik Ilves powiedział „W obecnych czasach nie potrzeba pocisków, żeby zniszczyć infrastrukturę. Można to zrobić on-line"[33]. Te wydarzenie władze estońskie potraktowały poważnie. Gdyby atak był skoncentrowany za pomocą wszystkich środków danego państwa to skutki mogłyby być o wiele gorsze[34].

Innym przykładem cyberataku jest konflikt pomiędzy Rosją i Gruzją w 2008 roku o separatystyczną enklawę Osetii Południowej. Przed konfliktem zbrojnym doszło tam do ataku DDOS (distributed denial of service) na serwery publiczne w Gruzji. Były to serwery prezydenta, Ministerstwa Spraw Zagranicznych, Narodowego Banku Republiki Gruzji oraz środków masowego przekazu[35]. Jak podają wiadomości strona, z której korzystał gruziński prezydent Micheil Saakaszwili przez 24 godziny była unieruchomiona, a na stronie Narodowego Banku Gruzji widniały zdjęcia dyktatorów, w których znajdował się również ówczesny prezydent. Jak we wcześniejszej sytuacji z Estonią, do końca

[30] K. Liedel, P. Piasecka, *Jak przetrwać w dobie zagrożeń terrorystycznych*, s. 44.
[31] Ibidem.
[32] A. Gniadek, op. cit., s. 227.
[33] P. Bukalska, *Dni, które wstrząsnęły Estonią*, https://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html (dostęp: 03.04.2020).
[34] Ibidem.
[35] A. Podraza, *Cyberterroryzm jako wzrastające zagrożenie dla bezpieczeństwa międzynarodowego w XXI wieku*, w: *Cyberterroryzm zagrożeniem XXI wieku*, pod. red., A. Podrazy, P. Potakowskiego, K. Wiaka, Warszawa 2013, s. 39.

nie wiadomo kto był sprawcą cyberataków w Gruzji. Jak podaje amerykański dziennik New York Times sprawcą mógł być rosyjski gang Russian Business Network, który niejednokrotnie był zamieszany w przestępstwa w sieci. Ten atak jednak nie zaszkodził Gruzji, ponieważ jest to kraj, który nie jest aż tak związany z Internetem. Należy mieć jednak na uwadze, iż nie należy lekceważyć takich ataków[36].

Ataki cyberterrorystyczne mogą być również dokonywane przed dane państwo. Przykładem są Stany Zjednoczone. W 2010 roku na rządów prezydenta Baracka Obamy został kontynuowany program pod kryptonimem "Igrzyska Olimpijskie". W jego ramach Stany Zjednoczone przy pomocy Izraela opracowały komputerowego robaka "Stuxnet", który był użyty na irańskie wirówki uranu w ośrodku jądrowym Natanz. Celem było zastopowanie rozwoju irańskiego programu nuklearnego. Podaje się, iż był to pierwszy amerykański atak w cyberprzestrzeni, który miał na celu opanowanie infrastruktury innego państwa[37].

Kolejnym przykładem ataków w cyberprzestrzeni są ataki przeciwko instytucjom rządowym i dyplomatycznym w różnych częściach świata. W 2013 roku rosyjska instytucja zajmująca się tworzeniem oprogramowania, która zabezpiecza komputery Kaspersky Lab, wykryła operacje szpiegowskie. Były one skierowane przeciwko instytucjom badawczym, grupom energetycznym i jądrowym oraz wymierzone były w cele handlowe i lotnicze. Ataki były kierowane w szczególności na Europę Wschodnią, Europę Zachodnią oraz Amerykę Północną. Próbowano zidentyfikować sprawcę, jednak wiązało się to z pewną trudnością[38].

Analizując zagrożenia wynikające z cyberterroryzmu warto odnieść się do kilku faktów, przedstawiające dane dotyczące ataków na sieci informatyczne. Jak wynika z poniższej tabeli zjawisko cyberterroryzmu zdecydowanie się nasiliło. Znajduje się bowiem w czołówce największych zagrożeń XXI wieku.

Tabela 4. Globalna statystyka ataków na sieci informatyczne.

Lp.	Rok	Liczba ataków
1.	1995	4
2.	1996	18
3.	1997	34
4.	1998	269
5.	1999	4197

[36] *Cyberatak na Gruzję,* https://wyborcza.pl/1,75399,5586335,Cyberatak_na_Gruzje.html?disableRedirects=true (dostęp: 03.04.2020).
[37] A. Podraza, op. cit., s. 39.
[38] Ibidem, s. 40.

6.	2000	7821
7.	2001	31 323
8.	2002	87 525

Źródło: E. Szulc-Wałecka, Znaczenie cyberterroryzmu we współczesnym świecie, w: Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja), pod. red. Marii Marczewskiej-Rytko, Lublin 2014, s. 284.

W samym 2016 roku miało miejsce wiele zdarzeń, które można zaliczyć do cyberataków. Jednym z nich jest kradzież 81 mln dolarów z banku w Bangladeszu, poprzez wykorzystanie systemu SWIFT. Pieniędzy mogło zniknąć więcej, ale poprzez czujność instytucji finansowych sytuację dało się w porę opanować[39]. Kolejnym przykładem jest włamanie na serwery Narodowego Komitetu Demokratów z USA. Włamywacze działali z inicjatywy rosyjskiego rządu i wykradli większość dokumentów oraz analiz dotyczących przeciwników politycznych, a w szczególności Donalda Trumpa, ówczesnego kandydata na prezydenta[40]. Innym dowodem na działalność cyberterrorystów jest atak DDoS na firmę Dyn. Firma ta zarządza znanymi serwisami internetowymi, takimi jak Twitter, Spotify, Github, SoundCloud itp. Poprzez atak na tą firmę wyżej wymienione serwisy przestały działać przez pewien czas. Z powyższych przykładów wynika, że takie problemy powinny być przewidziane, aby im przeciwdziałać[41].

W roku 2017 wśród licznych ataków na sieć najbardziej odnotował się atak przy użyciu złośliwego oprogramowania NotPetya. Sparaliżował on Ukrainę oraz uderzył w instytucje rządowe, elektrownie i inne. Ofiarami ataku stały się również inne państwa, w tym również Polska i jej firmy takie jak: InterCars, czy Maersk. Jednak najgorsza sytuacja przedstawiała się na Ukrainie. Złośliwe oprogramowanie (ransomware) miało wpływ na wszystkie instytucje rządowe, bankomaty, firmy prywatne, czyli wszystko co składa się na Infrastrukturę Krytyczną Państwa. Sprawcy domagali się zapłaty w bitcoinach w zamian za ponowny dostęp do danych[42].

[39] *Jak zniknęło 81 milionów dolarów* - historia prawdziwa, https://zaufanatrzeciastrona.pl/post/jak-zniknelo-81-milionow-dolarow-historia-prawdziwa/, (dostęp: 03.04.2020).
[40] *Fatalna wpadka Rosjan, którzy włamali się na serwery amerykańskich polityków*, https://niebezpiecznik.pl/post/fatalna-wpadka-rosjan-ktorzy-wlamali-sie-na-serwery-amerykanskich-politykow/, (dostęp: 03.04.2020).
[41] *Duży atak DDoS powoduje problemy z dostępem do wielu usług*, https://zaufanatrzeciastrona.pl/post/duzy-atak-ddos-powoduje-problemy-z-dostepem-do-wielu-uslug/, (dostęp: 03.04.2020).
[42] K. Majdan, *Hakerzy wywołali chaos na Ukrainie. Jak doszło do ataku ransomware?*, https://businessinsider.com.pl/technologie/nowe-technologie/notpetya-atak-zlosliwym-oprogramowaniem-na-ukraine/s7bnll2, (dostęp: 03.04.2020).

Według raportu rocznego z działalności CERT, czyli zespołu który zajmuje się reagowaniem na naruszenia bezpieczeństwa w sieci, najczęściej występującym incydentem w Polsce w 2018 roku był phishing. Kolejnym była dystrybucja złośliwego oprogramowania oraz spam. W samej Polsce zostało zanotowanych 3 739 incydentów związanych z cyberatakami, co stanowi 17,5 procent więcej niż w porównaniu do roku 2017[43].

Tabela 5. Incydenty obsłużone przez CERT Polska w 2018r.

Lp.	Typ incydentu	Liczba incydentów	%
1.	Obraźliwe i nielegalne treści (w tym spam)	431	11,53
2.	Złośliwe oprogramowanie	862	23,05
3.	Gromadzenie informacji	101	2,70
4.	Próby włamań	153	4,09
5.	Włamania	125	3,34
6.	Dostępność zasobów	49	1,31
7.	Atak na bezpieczeństwo informacji	46	1,23
8.	Oszustwa komputerowe (w tym phishing)	1 878	50,23
9.	Podatne usługi	69	1,85
10.	Inne	25	0,67

Źródło: Opracowanie własne na podstawie: CERT Polska, www.cert.pl

W lutym 2018 roku miał miejsce cyberatak na ceremonię otwarcia zimowych igrzysk olimpijskich w Pjongczangu. Celem cyberterrorystów była strona internetowa igrzysk. Jednak problemy dotyczyły również transmisji telewizyjnych oraz kanałów internetowych. Dzięki reakcji odpowiednich służb wszystkie problemy zostały usunięte po 12 godzinach od pojawienia się zagrożenia[44]. Jak się okazuje sprawcami ataku byli rosyjscy szpiedzy z agencji Głównego Zarządu Wywiadowczego. Zainfekowali oni ponad 300 komputerów olimpijskich, zhakowali routery Korei Południowej oraz uruchomili złośliwe oprogramowanie. Przyczynili się do zaburzenia łączności z Internetem oraz systemów nadawczych. O zajście podejrzewa się Rosję, ponieważ przez afery

[43] *Krajobraz bezpieczeństwa polskiego internetu*, https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf?fbclid=IwAR0WOGdR8j82bIuw7XUd8JZiBlw2Pyd4zd4nAHtJtaFJgB8g3SdDpbWRLBc, (dostęp: 03.04.2020).

[44] P. Majchrzak, *Pjongczang 2018. Cyberatak na igrzyska olimpijskie*, https://www.sport.pl/zimowe/7,64996,23013732,pjongczang-2018-cyberatak-na-igrzyska-olimpijskie.html, (dostęp: 03.04.2020).

dopingowe, sportowcy nie mogli występować na Igrzyskach Olimpijskich w barwach swojego kraju[45].

W roku 2019 złośliwym oprogramowaniem okazał się Ryuk, czyli jeden z najgroźniejszych oprogramowań szyfrujących. Polska okazała się jednym z najczęściej atakowanych krajów. W kwietniu 2019 roku twórcy wirusa ulepszyli go do wersji 64-bitowej. Wirus powstał w 2018 roku i w początkach swojego istnienia zainfekował większość firm. Największa aktywność Ryuka przypada na wrzesień 2019 roku, kiedy to jego ofiarą padły większe firmy i instytucje publiczne[46].

W środowisku akademickim, w którym przebywam też miał miejsce cyberatak, m.in. mowa tu o znikomym podłożeniu bomby na Uniwersytecie Mikołaja Kopernika w Toruniu. W pierwszy dzień sesji na pocztę elektroniczną uniwersytetu ok. godziny 10:00 wpłynęła wiadomość, w której napisane było "w waszej szkole jest bomba". Przyczyniło się to do odwołania wszystkich egzaminów na uczelni oraz ewakuacji kilku tysięcy studentów. Co prawda bomby na uczelni nie znaleziono, aczkolwiek nie należy bagatelizować takiego wydarzenia. Mógł to zrobić zdesperowany student, który stwierdził, że nie poradzi sobie z egzaminami, ale mogła to również wykonać osoba, która specjalizuje się w cyberatakach. Kto wie jakby wyglądała ta sytuacja, gdyby nikt na nią nie zareagował. Może sprawca w przypadku braku reakcji planował wykraść dane uczelni lub zrobić coś innego co w wielkim stopniu mogłoby zaszkodzić tej instytucji[47].

Jak widzimy cyberterroryści działają w każdej dziedzinie naszego życia, czy to w sporcie, nauce, a nawet w pracy. Dlatego ważnym jest, aby z każdego nawet najmniejszego zajścia wyciągać wnioski. Atak dokonany w cyberprzestrzeni może spowodować niewyobrażalne szkody. Dlatego ważna jest obrona przed cyberatakami, współpraca międzynarodowa oraz rozwój sektora walki z cyberprzestępczością[48].

[45] D. Górecki, *To Rosjanie stali za cyberatakiem na otwarciu igrzysk olimpijskich*, https://ithardware.pl/aktualnosci/to_rosjanie_stali_za_cyberatakiem_na_otwarciu_igrzysk_olimpijskich-5336.html, (dostęp: 03.04.2020).
[46] *Ransomware Ryuk: Polska trzecim najbardziej atakowanym krajem*, https://avlab.pl/ransomware-ryuk-polska-trzecim-najczesciej-atakowanym-krajem, (dostęp: 03.04.2020).
[47] *Paraliż na UMK. Odwołano zajęcia i egzaminy z powodu informacji o bombie na uczelni*, https://torun.naszemiasto.pl/paraliz-na-umk-odwolano-zajecia-i-egzaminy-z-powodu/ar/c10-4972062, (dostęp: 03.04.2020).
[48] E. Szulc-Wałecka, op. cit., s. 289.

WNIOSKI

XXI wiek to przede wszystkim większe zinformatyzowanie życia. W coraz większym stopniu jesteśmy uzależnieni od komputera. Z powyższych przykładów cyberataków wynika, iż wraz z postępem technologicznym ilość ataków wciąż się zwiększa. W artykule przedstawione jest jak zwykły terroryzm na przestrzeni lat rozwinął się do cyberterroryzmu. Cyberatak może wykonać każdy kto ma dostęp do komputera oraz Internetu. Jak w przypadku terroryzmu, nie potrzebna jest broń lub materiały wybuchowe. Nie ma wątpliwości, że takie zjawisko jakim jest cyberterroryzm wymaga dalszych badań i powstawania nowszych źródeł. Społeczeństwo powinno posiadać większą wiedzę na ten temat, by w możliwy sposób ustrzec się przed cyberatakami.

BIBLIOGRAFIA

[1] Aleksandrowicz T., *Terroryzm międzynarodowy*, Warszawa 2008.

[2] Białkowski M., *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Warszawa 2016.

[3] Dudczak P., *Terroryzm we współczesnym świecie*, w: *Oblicza terroryzmu*, Kraków-Rzeszów-Zamość 2011.

[4] Gniadek A., *Cyberprzestępczość i cyberterroryzm - zjawiska szczególnie niebezpieczne*, w: *Cyberterroryzm nowe wyzwania XXI wieku*, pod. red. Tadeusza Jemioły, Jerzego Kisielnickiego, Kazimierza Rajchela, Warszawa 2009.

[5] Kosta Raul A., *Terroryzm jako zagrożenie dla bezpieczeństwa cywilizacji zachodniej w XXI wieku*, Toruń 2012.

[6] Lichocki E., *Cyberterroryzm państwowy i niepaństwowy - początki, skutki i formy*, w: *Ewolucja terroryzmu na przełomie XX i XXI wieku*, pod. red., Katarzyny Szalewskiej, Gdańsk 2009.

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

[8] Liedel K., Piasecka Paulina, *Jak przetrwać w dobie zagrożeń terrorystycznych*, Warszawa 2008.

[9] Pikulski S., *Prawne środki zwalczania Terroryzmu*, Olsztyn 2000.

[10] Podraza A., *Cyberterroryzm jako wzrastające zagrożenie dla bezpieczeństwa międzynarodowego w XXI wieku*, w: *Cyberterroryzm zagrożeniem XXI wieku*, pod. red., Andrzeja Podrazy, Pawła Potakowskiego, Krzysztofa Wiaka, Warszawa 2013.

[11] Szewczyk M.M., *Cyberterroryzm jako zagrożenie współczesnego świata*, w: *Cyberterroryzm nowe wyzwania XXI wieku*, pod. red., Tadeusza Jemioły, Jerzego Kisielnickiego, Kazimierza Rajchela, Warszawa 2009.

[12] Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, Zeszyty Naukowe Akademii Marynarki Wojennej 2005, nr 1 (160).

[13] Szulc-Wałecka E.*, Znaczenie cyberterroryzmu we współczesnym świecie*, w: *Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja)*, pod. red. Marii Marczewskiej-Rytko, Lublin 2014.

[14] Wojciechowski S., *Terroryzm na początku XXI wieku. Pojęcie, istota i przyczyny zjawiska*, Bydgoszcz-Poznań 2011.

Źródła internetowe:

[15] Brunetko K., *Terrorysta - kto to taki?*, http://www.tygodnik.com.pl/kontrapunkt/28-29/kubacka.html, (dostęp: 29.03.2020).

[16] Bukalska P., *Dni, które wstrząsnęły Estonią*, https://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html (dostęp: 03.04.2020).

[17] Cyberatak na Gruzję, https://wyborcza.pl/1,75399,5586335,Cyberatak_na_Gruzje.html? disableRedirects=true (dostęp: 03.04.2020).

[18] *Duży atak DDoS powoduje problemy z dostępem do wielu usług*, https://zaufanatrzeciastrona.pl/post/duzy-atak-ddos-powoduje-problemy-z-dostepem-do-wielu-uslug/, (dostęp: 03.04.2020).

[19] *Fatalna wpadka Rosjan, którzy włamali się na serwery amerykańskich polityków*, https://niebezpiecznik.pl/post/fatalna-wpadka-rosjan-ktorzy-wlamali-sie-na-serwery-amerykanskich-politykow/, (dostęp: 03.04.2020).

[20] Górecki Daniel, *To Rosjanie stali za cyberatakiem na otwarciu igrzysk olimpijskich*, https://ithardware.pl/aktualnosci/to_rosjanie_stali_za_cyberatakiem_na_otwarciu_igrzysk_olimpijskich-5336.html, (dostęp: 03.04.2020).

[21] Internet World Status, www.Internetworldstats.com (dostęp: 02.04.2020).

[22] *Jak zniknęło 81 milionów dolarów* - historia prawdziwa, https://zaufanatrzeciastrona.pl/post/jak-zniknelo-81-milionow-dolarow-historia-prawdziwa/, (dostęp: 03.04.2020).

[23] *Krajobraz bezpieczeństwa polskiego internetu*, https://www.cert.pl/wp-con-

tent/uploads/2019/05/Raport_CP_2018.pdf?fbclid=IwAR0WOGdR8j82bIuw7XUd8JZiBlw2Pyd4zd4nAHtJtaFJgB8g3SdDpbWRLBc, (dostęp: 03.04.2020).

[24] Majchrzak Piotr, *Pjongczang 2018. Cyberatak na igrzyska olimpijskie*, https://www.sport.pl/zimowe/7,64996,23013732,pjongczang-2018-cyberatak-na-igrzyska-olimpijskie.html, (dostęp: 03.04.2020).

[25] Majdan Krzysztof, *Hakerzy wywołali chaos na Ukrainie. Jak doszło do ataku ransomware?*, https://businessinsider.com.pl/technologie/nowe-technologie/notpetya-atak-zlosliwym-oprogramowaniem-na-ukraine/s7bnll2, (dostęp: 03.04.2020).

CYBERTERRORISM AS A THREAT TO THE SECURITY OF MODERN WORLD COUNTRIES

ABSTRACT

The work particularly addresses the threats posed by cyber-terrorism in many countries around the world. To clarify this concept, one first needs to refer to the very definition of terrorism and how, in the age of globalisation, this phenomenon has become a problem of international importance. In the first chapter I would like to present the origins of terrorism and describe the various phenomena that accompany it. The second chapter is entirely devoted to cyberterrorism and how the computerization of life affects its development. In the 21st century computer crime is still evolving. There is more computerisation in every area of life, so it is important to try to counteract it. The third chapter describes examples of today's cyberterrorist attacks in various countries. Cyber-attacks are becoming a reality in every area of life, so it is important to remember about security and apply appropriate safeguards to help protect against cyberterrorism.

Keywords: terrorism, cyberterrorism, security