Studia Bezpieczeństwa Narodowego
Zeszyt 25 (2022)
ISSN 2028-2677, s. 11-24
DOI: 10.37055/sbn/151907

Instytut Bezpieczeństwa i Obronności
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

National Security Studies
Volume 25 (2022)
ISSN 2028-2677, pp. 11-24
DOI: 10.37055/sbn/151907

Institute of Security and Defense
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

BEZPIECZEŃSTWO W CYBERPRZESTRZENI

SECURITY IN CYBERSPACE

Katarzyna Przestrzelska
Akademia Nauk Stosowanych w Łomży

Abstrakt. Temat artykułu skupia się na cyberbepieczeństwie. Celem badawczym niniejszego artykułu jest przybliżenie działalności haktywistów. W artykule zostały opisane działania popularnej grupy haktywistycznej – Anonymous. Postawione zostało pytanie badawcze: jakie narzędzia i techniki hakerskie stosowane są w cyberprzestrzeni. W celu odpowiedzenia na te pytanie, została zbadana historia i działalność grup haktywistycznych. W artykule została przedstawiona charakterystyka haktywistów oraz metody ich działań. Podjęto próby oceny działań haktywistycznych, a także szanse i zagrożenia, jakie niesie dla obywateli. W cyberprzestrzeni występują działania, które tworzą dla niej zagrożenie, są to: cyberterroryzm i cyberprzestępstwa. Poczucie bezkarności sprawiło, że coraz więcej osób zaczęło aktywnie działać w cyberprzestrzeni. Wyniki badań wskazują, że haktywistyczne przedsięwzięcia mogą mieć różne zamiary – niektórzy kierują się dobrem ogółu, a inni za cel cyberataków stawiają swoje indywidualne korzyści m. in. majątkowe. Wśród cyberprzestępców wyróżnia się hakerów, haktywistów, krakerów i cyberterrorystów. Cyberterroryzm niewątpliwie jest zagrożeniem dla państwa, powoduje zniszczenia infrastruktury i jest zagrożeniem dla życia ludzi. Natomiast cyberbezpieczeństwo jest także zagrożone mniejszymi, mniej szkodliwymi działaniami, takimi jak: ataki hakerskie, włamania, pozyskiwanie danych, czy też poprzez wirusowanie stron. Z niniejszego artykułu można wywnioskować, że działania hakerskie są niejednoznaczne i nie zawsze wiążą się z niebezpieczeństwem wobec państwa i obywateli. Wyniki analizy wskazują, że bardzo często hakerzy dbają także o dobro ogółu i przeciwstawiają się łamaniu praw i wolności. Należy jednak mieć na uwadze fakt, że nie wszyscy działają w ten sam sposób i nie wiadomo, jak bardzo zagrożona może być nasza przyszłość.
Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, cyberprzestępstwo, cyberterroryzm, haktywizm

Abstract. The theme of the article focuses on cyber security. The research goal of this article is to present the activities of hacktivists. The article describes the activities of the popular hacktivist group - Anonymous. The research question is: what hacking tools and techniques are used in cyberspace? In order to answer this question, the history and activities of hacktivists have been researched. The article presents the characteristics of hacktivists and the methods of their activities. It also attempts to assess this phenomenon in terms of the opportunities and threats posed to citizens and state institutions. In cyberspace there are also activities that pose a threat to this term, these are: cyberterrorism and cybercrime. The feeling of

impunity means that more and more people are actively working in cyberspace. Their undertakings may have different intentions - some are guided by the common goods, while others target their individual benefits e.g. wealths, as a target of cyberattacks. Among cybercriminals there are hackers, hacktivists, crackers and cyberterrorists. Undoubtedly, cyberterrorism is a threat to the state, it destroys infrastructure and is a threat to people's lives. This is a threat to the real reality. What is more, cybersecurity is also threatened by smaller, less harmful activities, such as: hacking attacks, hacking, data extraction, or by virusing websites. From this article it can be concluded that hacking activities are ambiguous and not always associated with a danger to the state and citizens. The results of the analysis indicate that hackers very often care about the public good and oppose the violation of rights and freedoms. However, it should be borne in mind that not all act in the same way and it is not known how much our future may be at risk.
Keywords: cyberspace, cybersecurity, cyberterrorism, cyber crime, hacktivism

Wstęp

Obecna rzeczywistość związana jest z powszechnym korzystaniem z Internetu. Niemożliwy do wyobrażenia jest współczesny świat bez różnorodnych portali, serwisów, stron internetowych, usług komunikacyjnych, handlowych, a także instytucji działających online, czy też e-bankowości. Wzrost technologii sprawił, że cyberprzestrzeń stała się wręcz niemożliwa do odpowiedniego zabezpieczenia. Eksperci do spraw hakingu z łatwością odnajdują luki w systemach, co wiąże się z pozaprawnym przechwytywaniem tajnych danych.

Poczucie bezpieczeństwa w cyberprzestrzeni jest trudne do utrzymania m.in. dlatego, że sprawcy cyberprzestępstw są niemal niemożliwi do zidentyfikowania. Poczucie bezkarności sprawia, że coraz więcej osób aktywnie działa w cyberprzestrzeni. Ich przedsięwzięcia mogą mieć różne zamiary – niektórzy kierują się dobrem ogółu, a inni za cel cyberataków stawiają swoje indywidualne korzyści m. in. majątkowe. Wśród działaczy cybernetycznych wyróżnia się hakerów, terrorystów i haktywistów.

Działania zwykłych hakerów i terrorystów wiążą się z naruszeniem bezpieczeństwa społeczności, natomiast przedsięwzięcia haktywistów są niejednoznaczne. Celem niniejszej publikacji jest przybliżenie działalności haktywistów (w tym grupy Anonymous). Podjęte analizy posłużą do odpowiedzenia na następujące pytanie: jakie narzędzia i techniki hakerskie stosowane są w cyberprzestrzeni?

Pojęcie cyberprzestrzeni

Gwałtowny rozwój technologiczny świata przyczynił się do zmiany trybu życia, pracy i rozrywki społeczeństw. Rozpowszechniła się globalizacja środowiska internetowego i cyfryzacja systemów teleinformatycznych. Trudno sobie wyobrazić życie bez korzystania z portali internetowych, poczt elektronicznych, ogólnoświatowego przepływu informacji lub też bankowości online. Rozpowszechnienie cyfryzacji spowodowało, że obecnie coraz więcej codziennych spraw dokonuje się w Internecie,

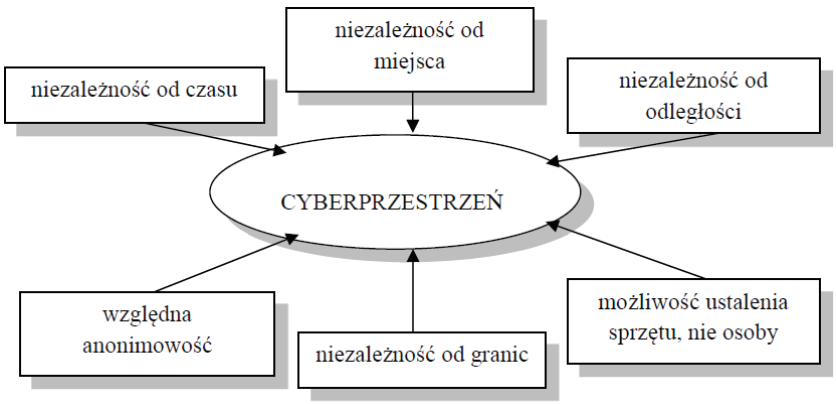
począwszy od robienia zakupów, rekrutacji do szkół, pracy online, a skończywszy na udzielaniu usług bankowych drogą elektroniczną, czy też wykorzystywaniu elektronicznego podpisu. Internet towarzyszy ludziom we wszystkich sferach ich życia. Skutkiem tego jest powszechne przetwarzanie danych, pozostających w cyberprzestrzeni.

W celu zdefiniowania zjawiska cyberprzestrzeni warto określić pojęcie systemu teleinformatycznego. Zgodnie z definicją zawartą w art.3 ust. 3 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, systemem teleinformatycznym jest zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2021 r. poz. 576). System teleinformacyjny jest ściśle powiązany z cyberprzestrzenią.

Termin cyberprzestrzeni nie ma jednoznacznej, stałej definicji. Można ją definiować w różnorodny sposób. Nienaukowo po raz pierwszy cyberprzestrzeń spopularyzował William Gimbson w 1982 r., który wskazał na charakterystyczne elementy umożliwiające opisanie tego zjawiska. Wśród nich wyróżnia się: rozciągłość na cały świat i wszechstronna baza danych. Autor tego zjawiska uznał, że cyberprzestrzeń jest niemożliwa do porównania z fizycznymi wymiarami (Wasilewski, 2013, s. 226). W. Gibson scharakteryzował cyberprzestrzeń, jako zjawisko *since fiction*. Wówczas nie zdawano sobie sprawy z tego, jak bardzo rozpowszechni i urzeczywistni się to zjawisko. Z punktu widzenia John P. Barlow cyberprzesteń jest to „każda przestrzeń, w której ludzie mogą gromadzić swoje umysły bez zabierania tam swoich ciał" (Dobrzeniecki, 2004, s. 18). Takie psychologiczne podejście wskazuje na fakt, że cyberprzestrzeń różni się od świata rzeczywistego tym, że jest bez granic. Zainteresowanie cyberprzestrzenią oraz gwałtowny rozwój teleinformatyczny nadał konieczność stworzenia legalnych definicji opisujących to zjawisko. Według ustawowej definicji zawartej w art. 3 ust. 1b Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, poprzez cyberprzestrzeń rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, zapewniające przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne. W literaturze przedmiotu przyjmuje się, że cyberprzestrzeń jest powiązaniem działalności ludzkiej z ogólnie rozumianą teleinformatyką (ICT- Information and Communication Technology) (Bógdoł-Brzezińska, Gwrycki, 2003, s. 37). Pojęcie cyberprzestrzeni wraz z rozwojem teleinformatycznym zaczęło zyskiwać na ważności, a termin ten zaczął pojawiać się w strategicznych dokumentach państwowych. Obecnie, państwa członkowskie Unii Europejskiej mają obowiązek tworzenia państwowych cyberstrategii.

Obowiązek ten został nałożony w lipcu 2016 roku poprzez Dyrektywę Parlamentu Europejskiego i Rady UE 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Warchol, 2019, s. 97). Państwa członkowskie w swoich strategiach w różnorodny sposób określają zjawisko cyberprzestrzeni. Warta uwagi jest definicja zawarta we francuskiej strategii, która określa te pojęcie, jako przestrzeń do komunikowania się, której infrastruktura jest położona na całym świecie. Światowy zasięg tego zjawiska spowodował, że zyskało nazwę „Nowej Wieży Babel". Cybernetyczna przestań jest miejscem, z którego korzystają różnorodne kultury i narody, a miejsce zbliża do siebie osoby, które mogą przebywać na zupełnie innej części świata. Przykładem tego są przedsiębiorstwa, które mogą sprzedawać swoje produkty na całym świecie (Warchol, 2019, s. 97).

Jak już zostało wspomniane, pojęcie cyberprzestrzeni jest różnorodnie definiowane. Nie ma jednego, stałego ujęcia definicyjnego tego zjawiska. Jednakże można wskazać na cechy, które określają cyberprzestrzeń. Tomasz R. Aleksandrowicz w swojej publikacji słusznie zwrócił na to uwagę. Zostały one przedstawione poniżej (Aleksandrowicz, 2016, s.12):



Schemat 1. Cechy charakteryzujące cyberprzestrzeń

Źródło: Opracowanie własne na podstawie: Aleksandrowicz T.R., 2016. Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego. Przegląd Bezpieczeństwa Wewnętrznego 15/16, s. 12

Formy naruszające cyberbezpieczeństwo państwa (cyberprzestępstwo i cyberterrozym) – ujęcie definicyjne

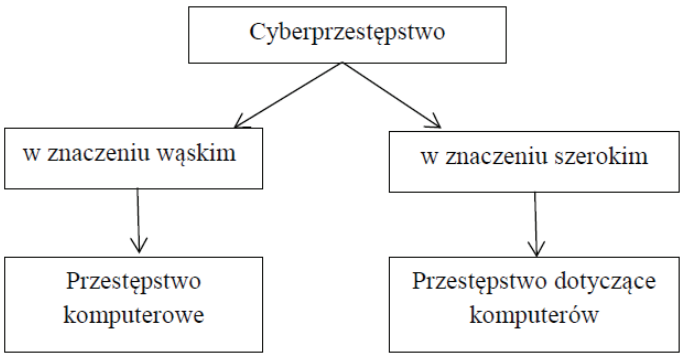
Cyberprzestrzeń to nie tylko rozwój technologii, ułatwienie życia codziennego, idealny świat bez granic, gdzie tylko ludzka wyobraźnia jest barierą. Cyberprzesteń to także miejsce coraz większej ilości zagrożeń spowodowanych między innymi

tym, że duża część osób czuje tam anonimowość. Wraz z tym przekonaniem rośnie przeświadczenie o bezkarności. Zaczęły pojawiać się zagrożenia i przestępstwa dokonywane w cyberprzestrzeni (Grzelak, Liedel, 2012, s. 126).

Tematykę zagrożeń cybernetycznych warto rozpocząć od samego pojęcia „cyberprzestępczość". Określenie „cyberprzestępczość" pochodzi z angielskiego słowa „cybercrime", które oznacza cybernetykę (cyber) i przestępstwo (crime) (Siwicki, 2015, s. 15). Autorem pierwszej definicji cyberprzestępczości był B. Parker, który określił te pojęcie jako czyn zabroniony, który został dokonany poprzez wyspecjalizowaną wiedzę informatyczną i komputerową (Hołyst, 2007, s. 326).

Polskie prawodawstwo nie posiada jednolitej definicji tego pojęcia, natomiast można wyróżnić definicje doraźne, które posiadają część wspólną, dotyczącą tego, że cyberprzestępstwo jest przestępstwem spowodowanym przy użyciu Internetu i komputera (Stefanowicz, 2017, s. 20). Niezwykle przydane do zdefiniowania tego pojęcia w literaturze przedmiotu są definicje legalne utworzone przez organizacje międzynarodowe tj. ONZ, czy też Radę Europy (Jaroszewska, 2017, s. 10).

Podczas X Kongresu ONZ w Sprawie Zapobiegania Przestępczości i Taktowania Przestępców, utworzono klasyfikację. Prezentuje się ona w następujący sposób:



Schemat 2. Znaczenie pojęcia „cyberprzestępstwo"
Źródło: na podstawie: M. Siwicki, Cyberprzestępczość, Wydawnictwo Beck, Warszawa 2015, s. 17

Cyberprzestępczość można definiować w znaczeniu wąskim i w znaczeniu szerokim. W znaczeniu wąskim jest to przestępstwo komputerowe, które polega na nielegalnej działalności, której celem jest stworzenie zagrożenia bezpieczeństwa systemów komputerowych oraz systemu danych. Zaś w znaczeniu szerokim, cyberprzestępczość charakteryzuje się tym, że dotyczy komputerów, przejawia się poprzez działania popełnione za pomocą, bądź też dotyczące systemów lub sieci komputerowych. Przykładem takich działań jest rozpowszechnianie i przechowywanie danych informacji za pomocą sieci komputerowych (Siwicki, 2015, s. 17).

Z kolei Rada Europy podczas Konwencji z dnia 23 listopada 2001 roku o cyberprzestępczości scharakteryzowała te pojęcie jako:

- zamierzony i pozaprawny dostęp do systemu teleinformatycznego;
- zamierzone i pozaprawne konfigurowanie, zmienianie, usuwanie danych, czy też spowodowanie zakłócenia teleinformatycznego;
- zamierzone i pozaprawne uzyskiwanie transmisji danych za pomocą prywatnych urządzeń technicznych (Stefanowicz, 2017, s. 20).

Jak słusznie zauważył A. Adamski (Adamski, 2001, s. 17), na Konwencji Rady Europy wyróżniono cztery rodzaje przestępstw. Do pierwszego rodzaju zalicza się przestępstwa, które ingerują w działanie systemów komputerowych i ich danych. Przykładem tego rodzaju przestępstw jest haktywizm. Drugi rodzaj dotyczy czynności spowodowanych za pomocą użycia komputera, do których zalicza się wszelakie oszustwa komputerowe, przykładem jest przekształcanie i podrabianie oficjalnych dokumentów wydawanych w formie elektronicznej. Do kolejnych rodzajów zalicza się przestępstwa popełnione ze względu na nielegalny, zabroniony charakter informacji stanowiącej jej przedmiot, a także wszelakie czyny przeciwko własności intelektualnej. Takie przestępstwa przejawiają się np. poprzez udostępnianie pornografii dziecięcej (Siemkowicz, Adamski, 2005, s. 52). Cyberprzestępstwa stanowią część cyberkonfliktów, które dzielą się na: aktywizm (obejmujący czynności, które za pomocą Internetu wspierają kampanie), cyberterroryzm i haktywizm (Liedel, Piasecka, 2011, s.17). Warto zwrócić uwagę na dwa ostatnie terminy.

Na początku warto wyjaśnić, czym jest cyberterroryzm. Ta forma terroryzmu jest niewątpliwie trudna do zdefiniowania, ponieważ obecnie nie ma ujednoliconej definicji znajdującej się w literaturze przedmiotu.

Termin „cyberterroryzm" został po raz pierwszy wprowadzony i użyty przez Barry'ego Colina w 1980 roku. Mężczyzna ten był pracownikiem naukowym w Instytucie Bezpieczeństwa i Wywiadu w Kalifornii (Górka, 2017, s. 300). Pojęcie to zostało stworzone w celu połączenia „cyberprzestrzeni" i „terroryzmu" (Denning, 2002, s. 79). B. Collin uważał, że cyberterroryzm jest przemyślanym, zaplanowanym użyciem systemu informacyjnego i sieci komputerowej w celu usprawnienia działań terrorystycznych (Smolski, 2015, s. 481). Natomiast w literaturze przedmiotu można natknąć się na definicję, która określa cyberterroryzm jako polityczny atak lub pogróżka ataku na systemy teleinformacyjne, sieci komputerowe, strony internetowe w celu destrukcji infrastruktury lub wzbudzenia poczucia strachu, co wiąże się ze zmuszaniem rządu i społeczności do wykonywania politycznych zamiarów. Jest to także rozpowszechnianie błędnych, fałszywych informacji i propagandy w celu osiągnięcia zamierzonych rezultatów przez grupy terrorystyczne (Smolski, 2015, s. 481).

Nieco inaczej cyberterroryzm definiuje Dorota Denning – ekspert ds. bezpieczeństwa. Według niej, podobnie jak stwierdził to Barry Colin, cyberterroryzm jest połączeniem terroryzmu i cyberprzestrzeni. Autorka tejże definicji dodaje, że jest to pełne motywacji działanie cyberprzestępcy, który dąży do wyrządzenia

niebagatelnych szkód tj. pozbawienie życia lub zniszczenie infrastruktury gospodarczej. Według niej jest to pozaprawny atak lub szantaż dotyczący ataku na sieci komputerowe oraz przechwycenie danych. D. Denning podkreśla, że kluczową cechą ataków cybernetycznych jest przemoc stosowana wobec ludzi, bądź też wyrządzenie zniszczeń w celu wywołania poczucia strachu. Przykładem takiego działania jest wywołanie wybuchu, bądź też zablokowanie e-bankowości (Górka, 2017, s. 301). Co więcej, autorka dodaje, że cel ataków ma charakter polityczny lub społeczny, wiąże się z manipulowaniem państwa i zmuszaniem do wykonania określonych czynności (Denning, 2000).

Inną definicję cyberterroryzmu określiło Narodowe Centrum Ochrony Infrastruktury Stanów Zjednoczonych, według którego jest to czyn kryminalny spowodowany za pomocą komputera oraz systemów teleinformatycznych, którego rezultatem jest uniemożliwienie korzystania z dotychczasowych usług w celu wzniecenia paniki i zaniepokojenia w danym społeczeństwie, chcąc mieć kontrolę nad nimi, móc wpłynąć na władze i ludność cywilną, aby osiągnąć zamierzony cel polityczny lub społeczny (Szubrycht, 2005, s. 175).

Natomiast M. Gawrycki uznał, że cyberterroryzm polega na spowodowaniu jak największych szkód przeciwnej stronie m.in. ofiar śmiertelnych np. w sytuacji, gdy przechwycone zostaną programy dotyczące lotów samolotowych, co w rezultacie może doprowadzić do katastrofy lotniczej (Jankowski, 2008, s.18).

Definicję omawianego pojęcia rozpowszechniło także Federalne Biuro Śledcze (FBI), które uznało, że cyberterroryzm jest świadomym, zaplanowanym, pozaprawnym działaniem, które posiada polityczne motywacje, którego skutkiem jest dostęp do sieci teleinformatycznych oraz wyłudzenie niepublicznych informacji i danych komputerowych. Takie ataki są przeprowadzane przez konspiratorskich agentów, bądź też zespoły narodowe (Górka, 2017, s. 301).

Podsumowując rozważania na temat pojęcia cyberterroryzmu, warto podkreślić, że cyberterroryzm ma na celu wywołanie paniki, strachu, paraliżu społecznego i niepokoju władz rządzących poprzez działania, które mają destruktywny charakter – wiąże się ze zniszczeniami infrastruktury, blokadą działania systemów zinformatyzowanych, a także powoduje skutki śmiertelne i katastrofy transportowe. Dokonywane są przy użyciu komputera i narzędzi teleinformatycznych. Celem ataków terrorystycznych jest posiadanie kontroli nad zastraszanym społeczeństwem i osiągnięcie konkretnych rezultatów (najczęściej politycznych).

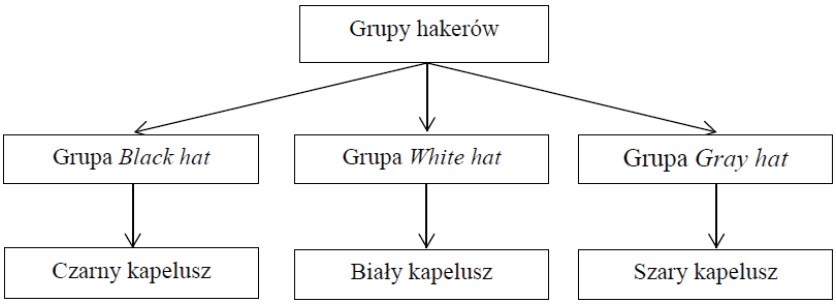
Haktywizm – definicja i geneza

Pojęcie haktywizmu jest dwuczłonowe – pochodzi od słów „hack" i „aktywizm". Termin ten, podobnie jak „cyberprzestrzeń" i „cyberterroryzm", wciąż ewoluuje, co stanowi problematykę do stworzenia jednej definicji tego zjawiska. K. Liedel

i P. Piasecka (Lidel, Piasecka, 2011, s. 18) w swojej publikacji określili haktywizm jako połączenie aktywizmu z użyciem technik hakerskich. Techniki te są stosowane w celu naruszenia prawidłowego funkcjonowania określonych systemów. Należy podkreślić, że ta aktywność nie przynosi tak poważnych szkód, jak w przypadku cyberterroryzmu. Działania te są powodowane po to, aby przykuć uwagę na wybrany problem polityczny, ekonomiczny lub społeczny.

Haktywizm jest sprzeciwieniem się, protestem i buntem obywatelskim poprzez zastosowanie włamań cybernetycznych. Powodem ich aktywności jest wzbudzenie uwagi na problemy, najczęściej podłoża politycznego (Rzeszutko, 2013, s. 31).

Wśród społeczności haktywizm bardzo często wywołuje negatywne emocje. Jest to spowodowane tym, że pojęcie te jest mylone i utożsamiane z krakerstwem. Należy zaznaczyć, że haktywizm wywodzi się z hakerstwa (Piotrowska, 2017, s. 27). Hakerów zaś można klasyfikować na kilka grup. M. Kowalska w swojej publikacji przedstawiła ich podział na trzy grupy. Został on zobrazowany na schemacie:



Schemat 3. Klasyfikacja Hakerów

Źródło: Opracowanie własne na podstawie: F. Kowalska, Hakerzy w służbie państwa – wirtualna strona patriotyzmu, DOI: 10.14746/r.2018.1.4, nr17, 2018, s. 41

1. Grupa „Czarny kapelusz" – ang. *Black hat*, hakerzy z tej grupy świadomie działają pozaprawnie poprzez wykorzystywanie luk cybernetycznych. Ich hasło brzmi: „Co nie jest zabronione jest dozwolone". Poprzez swoje działania dążą do zdobycia własnych, indywidualnych celów.

2. Grupa „Biały kapelusz" – ang. *White hat*, hakerzy z tej grupy starają się nie wyrządzać żadnych uszkodzeń. Takie osoby zazwyczaj pracują w legalny sposób i sprawują kontrolę nad lukami cybernetycznymi. Swoje zatrudnienie znajdują w różnorodnych firmach.

3. Grupa „Szary kapelusz" – ang. *Grey hat*, cechuje się tym, że działa pomiędzy dwiema powyższymi grupami. Z reguły działa na granicach prawa, bez powodowania szkód, jednakże czasami mają miejsce sytuację, gdzie prawo jest naruszane, a ich działania stają się pozaprawne (Kowalska, 2018, s. 41).

Początkowo powyższy podział nie miał zastosowania. Historia pierwszych hakerów wiąże się z latami 80. XX wieku. Wówczas haker był uznawany za osobę o ponadprzeciętnych zdolnościach informatycznych i posiadającą specjalistyczną wiedzę, za pomocą której był w stanie przechwycić dane z systemów komputerowych. Zamierzeniem hakera z lat 80. było jedynie oszacowanie swoich umiejętności. Wraz z upływem lat, hakerzy podzielili się na kilka grup. Jeden z odłamów hakingu tworzą krakerzy. Od hakerów różnią się zamierzonym celem – krakerzy pragną wyrządzenia szkód w systemach i bazach danych. Ich działalność jest bardziej szkodliwa niż przedsięwzięcia hakerów. Niektórzy publicyści są zdania, że powinno definiować się ich jako „pseudohakerów", ponieważ grupa ta składa się ze zróżnicowanych osób – w tym także początkowych amatorów, których celem bardzo często jest zdobycie indywidualnych korzyści np. majątkowych (Piotrowska, 2017, s. 27). Haktywista wyróżnia się tym, że jego działania mają na celu osiągnięcie zamierzonego celu nie tylko dla własnych korzyści, a między innymi dla dobra ogółu (Rzeszutko, 2013, s. 32).

Pierwsze działania haktywsitów polegały na blokowaniu witryn i portali internetowych za pomocą dużej ilości komunikatów. W rezultacie powstawał spam, a witryna nie była w stanie działać poprawnie. Dochodziło do zawieszeń i awarii stron internetowych. Innym sposobem było wirusowanie stron (Rzeszutko, 2013, s. 32-33). Jednakże metod działania haktywistów jest znacznie więcej.

Uznaje się, że haktywiści swoje działania rozpoczęli w 1989 roku, w tamtym czasie grupa haktywistów dokonała ataku cybernetycznego na Narodową Agencję Aeronautyki i Przestrzeni Kosmicznej (NASA) i Amerykański Departament Energii za pomocą wirusa pod nazwą „WANK - *Worms Against Nuclear Killer*". Celem ich działań nie było wywołanie szkód, a jedynie zwrócenie uwagi na problem związany z „nuklearnymi zabójcami". Wraz z upływem lat zainteresowanie działalnością haktywistów wzrastało. Zwiększyła się liczba osób działających w tej branży. Kluczową rolę w nasileniu się działań haktywistycznych odegrało stworzenie w 2003 roku portalu 4chang.org. Serwis ten umożliwiał maniakom informatycznym, interesującym się hakerstem, przedstawianie swoich umiejętności i dzielenia się nimi. Wszystkie publikowane treści były od anonimowych hakerów, którzy łączyli się w grupy osób o podobnych spostrzeżeniach politycznych i ponadprzeciętnych umiejętnościach. Serwis pierwotnie był miejscem rozrywki, hakerzy nie prowadzili poważnych działań. Ich czyny sprowadzały się do tworzenia żartów. Z biegiem czasu ich działalność przekształciła się w kierunku „cyberwojen". Co więcej, to właśnie na tym portalu została utworzona popularna obecnie grupa Anonymous (Piotrowska, 2017, s. 28-29).

Techniki i przykłady działań grup haktywistycznych

Pozaprawne działania cybernetyczne okazały się być trudne do ukarania. Działacze są anonimowi, a ich poczucie bezkarności przyczyniło się do coraz większej liczby cyberprzestępstw.

Wyróżnia się różne techniki działania haktywistów. Wśród nich znajduje się zamiana treści danej strony (ang. *defacing*). Działania te polegają na przechwyceniu danego serwisu i dodaniu swoich własnych treści. Takie ruchy haktywistyczne nie oddziaływają bezpośrednio na ludność cywilną, opierają się jedynie na zaburzeniu działania danej instytucji lub przedsiębiorstwa. Inną techniką stosowaną przez haktywistów jest atak DDoS, który polega na uderzeniu w jeden punkt z ogromnej ilości komputerów jednocześnie (ang. *Distribu-ted Denial of Service Attacks*). Taki rodzaj ataku jest najczęstszą techniką działania. Tego typu ataki często mają wpływ na funkcjonowanie danego społeczeństwa. Wówczas może to doprowadzić do zawieszenia funkcjonowania stron internetowych i pozbawienia ludności możliwości korzystania np. z e-bankowości. Równie popularnym działaniem jest blokada dostępu do danej strony lub serwisu (ang. *ping storm*). Inną metodą blokującą daną stronę lub e-skrzynkę jest dokonanie „*spamu*" wiadomościami na dany adres e-mail, bądź też profil internetowy (ang. *e-mail bombing*). Ogromna ilość wiadomości w skrzynce nadawczej powoduje, że poczta danej osoby jest blokowana. Wśród wymienionych metod należy również pamiętać o atakach złośliwego oprogramowania (ang. *malicious code attacks*). W tym celu używane są różnego rodzaju wirusy, trojany, robaki, czy też programy szpiegowskie. Ostatnią techniką wykorzystywaną przez haktywistów jest automatyczne przekierowywanie strony (ang. *redirects*). Technika ta polega na tym, że nieświadomi internauci po wpisaniu adresu URL danej strony internetowej, automatycznie przenoszeni są na zupełnie inną stronę, niż była docelowa. Taki typ działania może wiązać się ze szkodliwością wobec społeczeństwa np. gdy strona, na którą zostanie przekierowana dana osoba jest zawirusowana (Piotrowska, 2017, s. 29-32).

Powyższej wskazane techniki stosowane przez haktywistów i ich obfitość może świadczyć o tym, jak dużo różnorodnych działań jest przez nich podejmowanych. Haktywiści uaktywniają swoje działania w różnych celach. Pierwszy widoczny atak haktywistyczny w Polsce miał miejsce 20 czerwca 1997 roku podczas transmisji na żywo programu „TOK SZOK". Atak ten polegał na zwróceniu uwagi jak duże luki występują w polskich systemach teleinformatycznych. Aktywista pokazywał podczas transmisji ważne, tajne informacje. To przedsięwzięcie nie było szkodliwe dla społeczeństwa, jedynie wskazało na niedoskonałości systemu (Rzeszutko, 2013, s. 38).

Inne warte wskazania działanie haktywistów, zarówno w Polsce jak i w całej Europie, dotyczyło ACTA (ang. *Anti-Counterfeiting Trade Agreement*). 26 stycznia 2012 roku Unia Europejska wraz z państwami członkowskimi podpisała umowę ACTA, której celem było „ograniczenie naruszeń własności intelektualnej". Umowa ta nie wzbudziła aprobaty społeczeństw, a wręcz odwrotnie – wiązała się ze sprzeciwem obywateli państw Unii Europejskiej m.in. dlatego, że jednym z postulatów było umożliwienie kontroli wszystkich internautów korzystających z danych serwisów internetowych. Grupy aktywistyczne na początku ujawniły prywatne adresy e-mail i hasła polskiej elity rządzącej, kolejnym etapem był bezpośredni atak na

strony rządowe, a ich celem było wpłynięcie na zmianę decyzji i odrzucenia ACTA. Działania haktywistów spowodowały zablokowanie oficjalnych stron rządowych. W rezultacie umowa została odrzucona przez Parlament Europejski (Janik, s. 283). Zaangażowana w te działania była prężnie działająca grupa „Anonymous".

Grupa Anonymous słynie z wielu aktywności w sieci. Za pierwsze działanie Anonymous, dzięki któremu grupa zyskała rozgłos, uznaje się „Projekt Chanology" z 2008 roku. Projekt ten dotyczył sekty scjentologicznej, która zabraniała wolności słowa swoim członkom. Kościół sjentologiczny chciał ukarać osoby wypowiadające się niekorzystnie na temat scjentologistów przed sądem. Grupa Anonymous stanęła w obronie wolności i swoimi czynami zablokowała profile scjentologów na serwisach internetowych. Co więcej, to właśnie wtedy grupa Anonymous opublikowała nagranie, gdzie ujawnili swoje intencje działania – którymi są walka o sprawiedliwość i wolność w internecie. Grupa Anonymous wystąpiła w maskach, które obecnie są symbolem wizerunku haktywistów (Janik, s. 280-281).

Anonymous także prężnie uczestniczy w działaniach politycznych i „wojnach cybernetycznych". Można stwierdzić, że docierają tam w cyberprzestrzeni, gdzie w rzeczywistości mało kto ma odwagę i możliwość się pojawić. Przykładem jest działanie grupy Anonymous w 2015 roku, tuż po zamachach w Paryżu we Francji. Anonimowi przechwycili poufne dane dotyczące adresów osób współpracujących z ISIS. Przedsięwzięcie miało na celu likwidację kont dżihadystów z portalu Twitter, które pełniły u nich funkcję komunikatora (Piotrowska, 2017, s. 32).

Grupa Anonymous aktywnie angażuje się współcześnie podczas wojny na Ukrainie. Działacze dokonują włamań na rosyjskie serwery, witryny rządowe, czy też telewizję publiczną. Ich przedsięwzięcia nie mają na celu tworzenia ataków na ludność cywilną. Haktywiści pragnęli przekazać Rosjanom jak wygląda rzeczywistość wojny w Ukrainie m.in. zwracali uwagę na ataki na ludność cywilną i dzieci. Jednakże należy pamiętać, że ich działania niestety nie wywierają wpływu na rzeczywisty przebieg wojny, czy też zmniejszenie liczby rannych (Bochyńska, 2022).

Podsumowanie i wnioski

Cyberprzestrzeń wiąże się z rozwojem technologii, a także z nowymi zagrożeniami cybernetycznymi. Cyberbezpieczeństwo jest zagrożone poprzez ataki cybernetyczne. Haktywiści są prężnie działającą grupą w Internecie. Ich działania są pozaprawne, jednakże anonimowość i zaawansowane techniki haktywistyczne powodują, że przestępcy są trudni do zidentyfikowania i ukarania. Celem niniejszej publikacji było odpowiedzenie na pytanie: jakie narzędzia i techniki hakerskie stosowane są w cyberprzestrzeni? W niniejszej publikacji wyróżnia się kilka rodzajów cyberprzestępców oraz różnorodne techniki przez nich stosowane. Wśród nich można wyróżnić: wirusowanie stron, włamania cybernatyczne, blokowanie witryn,

defacing, ataki DDoS, czy też spam. Wybór techniki działania zależy od celu ich aktywności. Powszechnie znanym zagrożeniem hakerskim jest wirusowanie stron. Zazwyczaj technika ta ma na celu pozyskanie poufnych danych. Inną metodą stosowaną przy użyciu komputera jest włamanie cybernetyczne. Cel włamań może być różny. Włamywacze są w stanie przechwycić kontrolę nad daną witryną. Wśród włamywaczy wyróżnia się haktywistów, którzy co do zasady, nie chcą wpływać negatywnie na dane społeczeństwo, a jedynie na działania osób rządzących. Haktywiści bardzo często podczas włamań wykorzystują metodę zamiany treści danej strony - „defacing". Jednakże nie jest to najczęściej stosowaną metodą. Uznaje się, że najpopularniejszą techniką jest atak DDoS. Jest to uderzenie w jeden punkt z dużej ilości komputerów. Takie działanie powoduje blokowanie i uniemożliwia działanie danej witryny. Nie stanowi to bezpośredniego zagrożenia wobec danej społeczności, a jedynie uniemożliwia (zazwyczaj tymczasowe) korzystanie z danej strony internetowej. Podobnie działa „e-mail bombing". Technika ta powoduje blokowanie skrzynki odbiorczej danego użytkownika, na skutek dużego „spamu". Opiera się na wysyłaniu ogromnej ilości wiadomości na dany adres e-mail. Należy stwierdzić, że hakerzy stosują różne techniki w cyberprzestrzeni. Co więcej, warto mieć na uwadze, że technologie wciąż się rozwijają i nie wiadomo, jak mogą zmienić się na przestrzeni najbliższych lat.

BIBLIOGRAFIA

[1] Adamski, A., 2001. Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy, Toruń: Wydawnictwo TNOiK, 17.

[2] Aleksandrowicz, T.R., 2016. Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego. PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO 15/16, 12.

[3] Bochyńska, N., 2022. Cyberprzestępczość a haktywizm. Jak prawo podchodzi do hakerów w białych kołnierzykach? [online]. Defence 24. Dostępne pod adresem: https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-cyberprzestepczosc-a-haktywizm-jak-prawo-podchodzi-do-hakerow-w-bialych-kolnierzykach [dostęp: 08 czerwca 2022].

[4] Denning, D. E., 2000. Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Washington.

[5] Denning, D. E., 2002. Wojna informacyjna i bezpieczeństwo informacji. Warszawa: Wydawnictwa naukowo – techniczne, 79.

[6] Dobrzeniecki, K., 2014. Prawo a etos cyberprzestrzeni. Toruń: Wydawnictwo Adam Marszałek. Europejskiej. Studia de Securitate 9(4), 97.

[7] Górka, M., 2017. Wybrane aspekty definicyjne cyberterroryzmu i ich znaczenie w perspektywie polityki bezpieczeństwa. Cywilizacja i Polityka, 15(15), 300-301.

[8] Grzelak, M., Liedel K., 2012. Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu. Bezpieczeństwo Narodowe Warszawa: Biuro Bezpieczeństwa Narodowego 22 (2), 126.

[9] Hołyst, B., 2007. Kryminologia. Warszawa: Wyd. Prawnicze PWN, 326.

[10] Janik, J., Haktywizm i inne formy aktywizmu internetowego jako nowe mechanizmy demokracji bezpośredniej, 280-283.

[11] Jankowski, P., 2008. Cyberterroryzm jako współczesne zagrożenie dla administracji publicznej. Młody Jurysta2008/4 – numer specjalny –I Konferencja Młodych Naukowców Prawa Administracyjnego, 18.

[12] Jaroszewska, A., 2017. Wybrane aspekty przestępczości w cyberprzestrzeni. KPP Monografie, 10.

[13] Kowalska, F., 2018. Hakerzy w służbie państwa – wirtualna strona patriotyzmu, DOI: 10.14746/r.2018.1.4. Refleksje. Pismo naukowe studentów i doktorantów WNPiD UAM., 17, 41.

[14] Liedel, K., Piasecka P., 2011. Wojna Cybernetyczna – wyzwanie XXI wieku. Bezpieczeństwo Narodowe 1, 17-18.

[15] Piotrowska, M., 2017. Haktywizm – społeczna korzyść czy zagrożenie?. Studia Humanistyczna AGH 16/2, 27-32.

[16] Rzeszutko, M.,2013. Haktywizm – cyfrowe oblicze współczesnej solidarności, czyli zagrożenie bezpieczeństwa wewnętrznego państwa? Polityka i strategia bezpieczeństwa państwa, 31-33, 38.

[17] Siemkowicz, P, Adamski A., 2005. Cyberprzestępczość - aspekty prawne i kryminologiczne. Studia Prawnicze 4, 52.

[18] Siwicki, M., 2015. Cyberprzestępczość, Warszawa: Wydawnictwo Beck, 15.

[19] Smolski, W., 2015. Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa. Rodzinna Europa. Europejska myśl polityczno – prawna u progu XXI wieku, 481.

[20] Stefanowicz, M., 2017. Cyberprzestępczość – próba diagnozy zjawiska. Kwartalnik policyjny 4/2017, 20.

[21] Szubrych, T., 2005. Cyberterroryzm jako nowa forma zagrożenia terrorystycznego. Zeszyty naukowe Akademii Marynarki Wojennej 1 (160), 175.

[22] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2021.0.2070 t.j.) art.3 ust. 3.

[23] 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. z 2014 poz. 1815 t.j.) art. 2 ust. 1b.

[24] Warchoł, A., 2019. Pojęcie cyberprzestrzeni w strategiach bezpieczeństwa państw członkowskich Unii.

[25] Wasilewski, J., 2013. Zarys definicyjny cyberprzestrzeni. Przegląd Bezpieczeństwa Wewnętrznego 9 (5), 226.