dr Barbara Stefaniuk
Akademia Bialska im. Jana Pawła II
ORCID: 0000-0001-7430-075X
https://doi.org/10.29316/9788368103199_6

CYBERTERRORYZM JAKO ZAGROŻENIE BEZPIECZEŃSTWA GLOBALNEGO

CYBERTERRORISM AS A THREAT TO GLOBAL SECURITY

Streszczenie

Zagrożenie terroryzmem w ujęciu ogólnym postrzegane jest współcześnie jako jedno z największych wyzwań dla bezpieczeństwa globalnego. Nieprzypadkowo więc ta problematyka jest przedmiotem licznych analiz naukowych. Problemy globalne najczęściej postrzegane są w kontekście skali zagrożeń oraz wyzwań, jakie niosą dla ludzkości i świata. Celem niniejszego rozdziału będzie przybliżenie zagrożenia cyberterroryzmem jako zagrożenia bezpieczeństwa globalnego. Cyberterroryzm globalny, może przybierać różne formy oddziaływania na wybrane obszary funkcjonowania państwa i społeczeństwa., które ukierunkowane są na zaatakowanie i całkowite zniszczenie m.in. kluczowych obiektów infrastruktury krytycznej, jak i inżynierii społecznej.

Słowa kluczowe: bezpieczeństwo globalne, zagrożenie, terroryzm, cyberterroryzm, globalizacja

Summary

The threat of terrorism in general is currently perceived as one of the greatest challenges to global security in the modern era. It is no coincidence that this issue is the subject of numerous scientific analyses. Global problems are most often perceived in the context of the scale of threats and challenges they pose to humanity and the world. The aim of this chapter will be to present the threat of cyberterrorism as a threat to global security. Global cyberterrorism can take various forms of impact on selected areas of the functioning of the state and society, which are aimed at attacking and completely destroying, among others, key critical infrastructure facilities, as well as social engineering.

Keywords: global security, threat, terrorism, cyberterrorism, globalization

Wstęp

Współczesny świat podlega niezwykle dynamicznym i ciągłym zmianom, które uwarunkowane są różnymi zagrożeniami. Zagrożenia te mogą przybierać formę zagrożeń globalnych, które mogą mieć wpływ na bezpieczeństwo międzynarodowe i globalne. W związku z rozwojem technologii informacyjnej powstaje wiele form zagrożeń cybernetycznych. Terroryzm, który jest definiowany jako różnie umotywowana i realizowana z naruszeniem porządku prawnego forma przemocy polityczno – społecznej podjęta przez pojedyncze osoby lub grupy osób, skutkująca wywołaniem strat fizycznych, psychicznych lub materialnych[1]. Zagrożenie każdą formą terroryzmu jest obecnie zagrożeniem permanentnym i nie ma możliwości jego całkowitego wyeliminowania. W niniejszym rozdziale autorka skupiła swoją uwagę na zagrożeniu cyberterroryzmem jako jednym z rodzajów terroryzmu, który w pełni można uznać za globalny. Obecnie żyjemy w społeczeństwie sieciowym, które umożliwia korzystanie z dobrodziejstw Internetu w każdej sferze życia. Jednym z najbardziej znaczących zagrożeń dla współczesnej cywilizacji jest zagrożenie cyberterroryzmem. Cyberterroryzm jest to bezprawny atak lub groźba ataku na komputery, sieci lub systemy informacyjne, w celu zastraszenia lub wymuszenia na rządzie lub ludziach daleko idących politycznych i społecznych celów[2].

Gwałtowny postęp technologiczny w elektronice, technologii informacyjnej i telekomunikacji przyczynił się do rozwoju nowych zagrożeń o charakterze cyberterrorystycznym. Współcześnie zagrożenie cyberterroryzmem pozostaje jednym z najważniejszych globalnych wyzwań, z jakimi musi się zmierzyć także Polska oraz służby mundurowe, dbające o bezpieczeństwo państwa. Cyberterroryzm stanowi realne zagrożenie dla życia ludzi, stabilności instytucji państwowych, infrastruktury krytycznej państwa oraz ładu międzynarodowego, a także dla bezpieczeństwa globalnego. Rozwój cyberterroryzmu jest przejawem globalizacji i towarzyszących jej procesów. Globalizacja wpłynęła na cyberbezpieczeństwo, zwiększając złożoność i skalę potencjalnych zagrożeń oraz rozszerzając powierzchnię ataku[3]. Bezpieczeństwo globalne wchodzi w zakres pojęciowy bezpieczeństwa międzynarodowego, które

[1] S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny terroryzm*, Wydawnictwo Difin, Warszawa 2017, s. 26.

[2] W. Smolski, *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*. https://www.repozytorium.uni.wroc.pl/dlibra/publication/67850, [dostęp: 29.03.2025].

[3] A. Malewska i M. Filary-Szczepanik*, Globalizacja i współzależność*, Wydawnictwo Naukowe Akademii Ignatianum w Krakowie, Kraków 2022, s. 316.

obejmuje bezpieczeństwo całej zbiorowości państw oraz system międzynarodowy, w jakim państwa te występują. W świetle literatury przedmiotu bezpieczeństwo globalne obejmuje środki wojskowe i dyplomatyczne, które państwa i organizacje międzynarodowe, takie jak Organizacja Narodów Zjednoczonych i NATO, podejmują w celu zapewnienia wzajemnego bezpieczeństwa[4]. Ze względu na skalę zagrożeń i potencjalne skutki dla funkcjonowania państw i społeczeństw, problematyka zagrożeń cyberterroryzmem szybko nabierają znaczenia globalnego i stają się nieodłączną częścią relacji międzynarodowych. W niniejszym rozdziale wykorzystano następujące metody badawcze: analizę porównawczą, analizę i krytykę piśmiennictwa, analizę i krytykę źródeł oraz studium przypadku.

Zagrożenia bezpieczeństwa globalnego

Uwarunkowania zmian w globalnym środowisku bezpieczeństwa wskazują na coraz to bardziej zwiększoną liczbę zagrożeń w nim występujących. Współcześnie poziom bezpieczeństwa nie jest mierzony tylko prawdopodobieństwem wystąpienia zagrożenia militarnego. Cyfryzacja niemal wszystkich dziedzin życia ma niewątpliwie ogromny wpływ na bezpieczeństwo ludzi i państwa w wymiarze globalnym. Powszechne zastosowanie komputerów i technologii teleinformatycznych w sferze publicznej, jak i prywatnej wiąże się z ryzykiem powstania zagrożeń o charakterze cybernetycznym[5]. Zagrożenie jest to odziaływanie czynnika destrukcyjnego na podmiot. Etymologia pojęcia globalny oznacza odnoszący się do całego świata[6]. Zagrożenia globalne to takie, których nie można rozwiązać w skali tylko jednego państwa lub grupy państw. Dotyczą bowiem całej ludzkości, jej trwania i rozwoju. Wśród nich ważne miejsce zajmują zagrożenia dla środowiska naturalnego, dotyczące zmiany klimatu, przekształcanie się gleb w pustynie, brak dostępu do wody pitnej, zanieczyszczenie powietrza, wycinanie lasów tropikalnych lub nadmierna eksploatacja zasobów naturalnych. Równie istotne są problemy rozwoju na świecie – ubóstwo, niedożywienie, brak dostępu do leków i edukacji oraz problemy polityczne – rosnąca skala migracji, konflikty wewnętrzne

[4] R. Kuźniar, *Bezpieczeństwo międzynarodowe, Wydanie drugie rozszerzone*, Wydawnictwo naukowe Scholar, Warszawa 2022.

[5] T. Zieliński, P. Mróz, R. Bartnik, *Bezpieczeństwo i obrona Unii Europejskiej*, Akademia Sztuki Wojennej, Warszawa 2020, s. 43.

[6] *Globalny*, słownik PWN, https://sjp.pwn.pl/slowniki/globalny.html, [dostęp: 28.03.2025].

i międzynarodowe. Szczególną uwagę należy zwrócić na zagrożenie terroryzmem[7], który może przybrać postać cyberterroryzmu globalnego i rozwoju związanych z nim cyberzagrożeń.

Charakterystyka wybranych cyberzagrożeń

Wraz z rozwojem cyberzagrożeń podmioty, które próbują zagrozić bezpieczeństwu cybernetycznemu państwa lub organizacji, stają się coraz bardziej zróżnicowane. Cyberterroryści mogą pochodzić z kręgów zorganizowanych grup przestępczych, użytkowników wewnętrznych, operatów usług, haktywistów a nawet organów wywiadu wspieranych przez określone państwa[8]. Współczesne systemy i sieci informatyczne można atakować w różny sposób, którego efektem będzie osiągnięcie jednego z niszczycielskich celów, mianowicie: utrata danych, kradzież danych, ujawnienie danych, zdyskredytowanie danych, destabilizacja infrastruktury krytycznej, przejęcie kontroli nad systemem lub całym środowiskiem, szantaż lub awaria systemu[9]. Najgroźniejszą formą zagrożenia informatycznego jest cyberterroryzm, który definiowany jest jako politycznie umotywowany atak bądź groźba ataku na komputery, systemy lub sieci informacyjne. Jego celem jest doprowadzenie do zniszczenia infrastruktury oraz zastraszenie lub wymuszenie na rządach i ludziach określonych politycznych, bądź społecznych działań[10]. Wszelkie cyberzagrożenia mają swoje miejsce w cyberprzestrzeni. W świetle literatury przedmiotu cyberprzestrzeń jest pojmowana jako byt wirtualny, pozbawiony parametru geograficznego, jest niemierzalny i nieograniczony[11]. W. Krztoń określa cyberprzestrzeń jako globalną domenę środowiska informacyjnego, składającą się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe,

[7] *Globalizacja – szanse i zagrożenia*, https://globalna.ceo.org.pl/materialy/globalizacja-szanse-i-zagrozenia/, [dostęp: 24.03.2025].

[8] M., Rytko-Marczewska, *Haktywizm (Cyberterroryzm, Haking, Protest obywatelski, Cyberaktywizm, E- Mobilizacja)*, Wydawnictwo UMCS Lublin, Lublin 2014.

[9] T. Zieliński, P. Mróz, R. Bartnik, *Bezpieczeństwo i obrona Unii….,* op. cit., s. 45.

[10] Ibidem.

[11] A. Gałecki, *Bezpieczeństwo informacji w dobie cyberprzestrzennych zagrożeń*, Wydawnictwo Wyższa Szkoła Bezpieczeństwa, Poznań 2021, s. 51.

a także osadzone w nich procesory i kontrolery[12]. Cyberprzestrzeń to wirtualna przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery z całego świata[13]. Cyberataki mogą występować w postaci samodzielnego ataku np. na systemy odpowiedzialne za kontrolę ruchu lotniczego lub funkcjonowanie bankowości elektronicznej, co ma na celu spowodowanie jego dysfunkcyjności. Cyberataki mogą mieć również formę złożonych operacji i spowodować rolę wspierającą podczas zamachu fizycznego np. wyłączenie kontroli dostępu w obiekcie lub blokadę komunikacji pomiędzy służbami. Inną formą ataku terrorystycznego może być technika zamachu prowadzonego w cyberprzestrzeni za pomocą pozyskiwania informacji[14]. Działalność służb wywiadowczych jest bardzo ważna w procesie pozyskiwania informacji, ponieważ przyczynia się do zapobiegania i zwalczania czynów zagrażających ujawnieniem tajemnicy państwowej, przyczynia się do zapobiegania i zwalczania przestępczości związanej z funkcjonowaniem technologii informacyjnej i komunikacyjnej[15].

Zagrożenia cybernetyczne można podzielić na cztery główne kategorie, do której zalicza się cyberprzestępczość, cybernetyczne szpiegostwo, cyberterroryzm i cyberwojnę[16].

Cyberprzestępczość to wszelkie działania przeciwko poufności, integralności i dostępności danych, dotyczących nielegalnego dostępu do systemów to: hacking, podsłuch, podawanie fałszywej tożsamości, szpiegostwo komputerowe, sabotaże oraz wymuszenia komputerowe. Do cyberprzestępczości zaliczyć można wirtualne przestępstwa finansowe, bankowe, a więc newralgiczne systemy infrastruktury państwa.

Cyberprzestępstwa[17], to działania przeciwko poufności, integralności i dostępności danych, dotyczących nielegalnego dostępu do systemów obej-

[12] J. Lebiedź, W. Krztoń, B. Stefaniuk, *Współczesne wyzwania bezpieczeństwa narodowego. Zarządzanie kryzysowe. Wojna w cyberprzestrzeni. Rzeczywistość wirtualna*, Wydawnictwo Texter, Warszawa 2018, s. 100-101.

[13] Ibidem.

[14] J. Stelmach, *Zamachy terrorystyczne. Istota i koncepcja reagowania*, Wydawnictwo Difin, Warszawa 2023, s. 164.

[15] A. Olech*, Walka z terroryzmem polskie a francuskie doświadczenie*, Wydawnictwo Difin, Warszawa 2021.

[16] S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny terroryzm*, Wydawnictwo Difin, Warszawa 2017, s. 52.

[17] P. Różański, A. Warmiński., H. Chałupczak, *Zagrożenia bezpieczeństwa i porządku publicznego we współczesnej Polsce (wybrane aspekty),* Akademia Wychowania Fizycznego Józefa Piłsudskiego w Warszawie, Wydział Wychowania Fizycznego i zdrowia w Białej Podlaskiej, Biała Podlaska 2023.

mujące: hacking, podsłuchiwanie i podawanie fałszywej tożsamości, szpiegostwo komputerowe, sabotaże oraz wymuszenia komputerowe:

- manipulacje fakturami lub kontami firmowymi, nieprawdziwe aukcje czy nielegalne używanie kart kredytowych, komputerowe podróbki, molestowanie dzieci czy cyberstalking;
- ataki na życie ludzkie, manipulowanie systemami szpitalnymi lub kontrolą ruchu
- powietrznego, przestępstwa obejmujące dziecięcą pornografię, przekazywanie instrukcji zachowań przestępczych, oferty popełniania przestępstw, molestowanie i lobbing poprzez sieć, rozpowszechnianie fałszywych informacji oraz internetowy hazard;
- przestępstwa powiązane z naruszeniem prawa autorskiego i praw pokrewnych, do których należy np. nieautoryzowanie, kopiowanie i rozpowszechnianie programów komputerowych, cyberprzestępstwa są najczęściej formami przestępstw i działań zabronionych.

Do pierwszej grupy zalicza się oszustwa i fałszerstwa, do drugiej należą: pozyskiwanie, wytwarzanie, rozpowszechnianie oraz posiadanie treści nielegalnych. Trzecią grupą są ataki cybernetyczne na systemy informatyczne, zaś czwartą grupę stanowi kopiowanie i rozpowszechnianie w celach zarobkowych utworów chronionych prawem autorskim.

Cybernetyczne szpiegostwo to rodzaj cyberataku, w którym nieautoryzowany użytkownik próbuje uzyskać dostęp do poufnych lub tajnych danych albo własności intelektualnej (IP) w celu uzyskania korzyści ekonomicznych, przewagi konkurencyjnej lub z powodów politycznych. Szpiegostwo komputerowe to udzielenie obcemu wywiadowi wiadomości, ich gromadzenie lub przechowywanie, włącznie się do sieci komputerowej w celu ich uzyskania lub zgłaszanie gotowości działania na rzecz obcego państwa przeciwko Rzeczypospolitej Polskiej[18]. W sieci zdecydowana większość informacji jest jawna oraz możliwa do skopiowania i wykorzystania. Jednak niektóre nie są jawne, do których zalicza się: niejawne informacje wojskowe, tajemnice handlowe czy dane osobowe. To właśnie one stanowią obszar zainteresowań terrorystów[19]. W literaturze przedmiotu istnieje wiele pojęć cyberterroryzmu. Cyberterroryzm to wykorzystywanie cyberprzestrzeni w działaniach terrorystycznych. Narzędziem do wykonywania aktów terroru jest sieć komputerowa, a celem

[18] art. 130 Ustawy z dnia 6 czerwca 1997 r. *Kodeks Karny* (Dz. U. 1997 Nr 88, poz. 553).

[19] S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki- organizacji- państwa,* Wydawnictwo CedeWu, Warszawa 2016, s. 210.

zasoby infrastruktury krytycznej. Przejęcie kontroli nad tymi zasobami, które sterowane są za pomocą komputerów i Internetu, powoduje chaos i panikę oraz brak stabilizacji w funkcjonowaniu państwa[20].

Cyberwojna to jeden z elementów wojny informacyjnej. W cyberwojnie głównymi celami są szpiegostwo i sabotaż[21]. Wielu ekspertów ocenia, że w praktyce oznacza ona cyberterroryzm: ataki na infrastrukturę IT lub infrastrukturę sieciową na terenie wrogiego państwa. Na celownik brane są instytucje publiczne oraz firmy prywatne. Innym przejawem cyberwojny są akcje internetowych trolli, którzy tworzą, a następnie kolportują fake newsy np. w mediach społecznościowych. Dla agresora celem w cyberwojnie jest zmuszenie przeciwnika do posłuszeństwa. Wojna cybernetyczna jest narzędziem, żeby narzucić swoją wolę innemu państwu. Przykładem wojny cybernetycznej może być atak na systemy wyborcze lub blokowanie serwerów www. J. Kuck prezentuje następującą klasyfikację zagrożeń występujących w cyberprzestrzeni, dzieląc je na siedem kategorii[22]:

- stealingpasswords – uzyskiwanie haseł dostępu do sieci,
- social engineering – wykorzystanie niekompetencji osób posiadających dostęp do
- systemu,
- bugs and backdoors – nielegalne korzystanie z systemu lub używanie nielegalnego
- oprogramowania,
- authenticationfailures – zniszczenie mechanizmu autoryzacji,
- protocolfailures – wykorzystanie luk w oprogramowaniu i systemach,
- information leakage – przechwycenie informacji dostępnych dla administratora,
- denial of service – blokada kont użytkowników systemu.

Obszar działań cyberterrorystów jest bardzo obszerny, trudny do jednoznacznego zidentyfikowania i ciągle powiększający swój zasięg na nowe obszary. W związku z coraz częstszym użytkowaniem urządzeń mobilnych

[20] M. Górka, *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku,* Wydawnictwo Difin, Warszawa 2014, s. 265.

[21] M. Marszycki, *Cyberwojna między Rosją a Ukrainą wciąż trwa*, 3 marca 2023 r., https://itwiz.pl/cyberwojna-miedzy-rosja-a-ukraina-wciaz-trwa, [dostęp: 30.03.2025].

[22] J. Kuck, *Bezpieczeństwo informacyjne. Cyberterroryzm. Przestępczość komputerowa*, Wydawnictwo Państwowej Akademii Nauk Stosowanych w Jarosławiu, Jarosław 2023, s. 109-110.

wzrasta poziom ich zagrożeń, które można zaobserwować poprzez zwiększanie się ilości złośliwych programów wykrywanych na urządzeniach mobilnych. Do najczęściej stosowanych kategorii cyberzagrożeń przez cyberprzestępców w ostatnich latach należą m.in.[23]:

- ataki odmowy usługi, które są nakierowane na zaburzenie działania systemów i usług poprzez wyczerpanie ich zasobów, najczęściej spotykany przypadek Distributed Denial of Service (DDoS) osiąga ten cel poprzez przeciążenie wybranej usługi zapytaniami wysyłanymi z wielu kontrolowanych urządzeń naraz;
- ataki ransomware, w których cyberprzestępca szantażuje organizację po przejęciu kontroli nad jej zasobami, żąda okupu pod różnymi warunkami, na przykład przywrócenia dostępności danych i systemów lub obietnicy nieudostępniania przejętych wrażliwych informacji publicznie, odnotowano też przypadki żądania okupu za przerwanie ataku odmowy usługi, które nazywa się Ransom Denial of Service (RDoS)[24];
- ataki na dane, w ramach których dochodzi do nieuprawnionego dostępu do poufnych danych, może być to kradzież danych spowodowana celowo w ramach cyberataku lub nieumyślny wyciek w wyniku błędu.

Kolejnym rodzajem cyberzagrożenia jest socjotechnika mająca zastosowanie w inżynierii społecznej. To każda metoda, mająca na celu oszukanie człowieka do uzyskania dostępu do systemu lub danych. Warto podkreślić, że nie chodzi tu wyłącznie o maile phishingowe, ale złośliwe połączenia głosowe, smsy, kody QR, podstawienie strony bankowej[25]. Popularnym wektorem ataku jest obecnie Business Email Compromise (BEC), w którym atakujący podszywają się pod zaufaną osobę (np. prezesa, księgową) w celu wyłudzenia pieniędzy, na przykład wywierając presję do uregulowania płatności pod wskazanym adresem bankowym.

Złośliwe oprogramowanie jako ogólna kategoria, opisująca wszelkie ataki wykorzystujące złośliwy kod, programy i aplikacje do osiągnięcia swojego celu. Obecnie zauważyć można dużą popularność tzw. infostealerów, czyli oprogramowania do kradzieży danych z zainfekowanego urządzenia. Znalezienie poświadczeń pracownika organizacji w opublikowanych w Internecie

[23] M. Marczyk, M. Stolarz, B. Terebiński, *Bezpieczeństwo działań w cyberprzestrzeni. Wybrane aspekty. Tom II Działania w cyberprzestrzeni,* Akademia Sztuki Wojennej, Warszawa 2022, s. 184.

[24] Ibidem.

[25] J. Kuck, *Bezpieczeństwo informacyjne. Cyberterroryzm. Przestępczość*…, op. cit., s. 109.

logach takiego programu jest jedną z częstszych metod inicjalnego dostępu do organizacji[26].

Manipulacja informacją w sieci cyfrowej na celu wywołanie określonego wpływu na wydarzenie lub proces polityczny. Jest to szeroka kategoria działań, mieszcząca w sobie praktyki takie jak, dezinformacja i propaganda w sieciach i serwisach społecznościowych.

Istnieje kilka rodzajów ataków wykorzystujących inżynierię społeczną, takich jak wyłudzanie informacji, wyłudzanie informacji przez SMS, wyłudzanie informacji przez telefon i pretekst. Wyłudzanie informacji zwykle odbywa się za pośrednictwem poczty e-mail. Cyberprzestępca wysyła wiadomość e-mail wyłudzającą informacje z linkiem albo załącznikiem przeznaczonym do kliknięcia lub pobrania przez ofiarę. Kliknięcie lub pobranie podejrzanego linku albo załącznika może spowodować pobranie złośliwego oprogramowania na urządzenie ofiary i kradzież jej prywatnych danych przez cyberprzestępcę. Wyłudzanie informacji przez telefon i wyłudzanie informacji przez SMS są odmianami wyłudzania informacji różniącymi się wykorzystywaną metodą komunikacji.

Cyberterroryzm – jako forma terroryzmu globalnego

Od najdawniejszych lat rozwój technologiczny w znaczący sposób wpływał na życie człowieka. W ostatnich latach szczególnie intensywnie rozwija się obszar informatyki oraz szerokopasmowego Internetu, co przekłada się niewątpliwie na zwiększenie liczby jego użytkowników. Codzienne funkcjonowanie jest już nierozerwalnie związane z cyberprzestrzenią, czyli przestrzenią wirtualną, która stwarza warunki do rozwoju nowej platformy walki zbrojnej, nowej formy terroryzmu – cyberterroryzmu. Przestrzeń wirtualna może być określana jako globalna wioska, świat, w którym ludzie, dzięki środkom masowego przekazu, przeżywają jednocześnie te same wydarzenia i używają tych samych produktów masowej konsumpcji[27]. Zdefiniowanie cyberterroryzmu nie jest sprawą prostą, ponieważ obszar działań cyberterrorystów jest dość szeroki i trudny do jednoznacznego określenia. W literaturze przedmiotu istnieje wiele definicji cyberterroryzmu. Zjawisko cyberterroryzmu jest bardzo zróżnicowane, co przejawia się jego dynamiką. Cyberterroryzm jest

[26] Ibidem.

[27] *Globalny*, słownik PWN, https://sjp.pwn.pl/slowniki/globalny.html, [dostęp: 28.03.2025].

to jedna z form terroryzmu[28]. Ponadto, występuje pod wieloma postaciami, które zmieniają się pod wpływem rozwoju cywilizacyjnego i technologicznego. Cyberterroryzm w zakresie funkcjonowania infrastruktury krytycznej jest działaniem, które hamuje i całkowicie blokuje działanie systemów komputerowych, aby osiągnąć konkretne cele terrorystyczne[29].

Cyberterroryzm - pojęcie to odnosi się do bezprawnych ataków i zagrożeń wobec komputerów, sieci i informacji przechowywanych w nich, celem których jest zastraszenie lub zmuszenie rządu albo jego ludzi, po to, aby osiągnąć pewne korzyści polityczne lub społeczne[30].

Pojęcie cyberterroryzmu używane jest w kontekście politycznie umotywowanego ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów w szerokim rozumieniu tego słowa[31]. Cyberterroryzm może być wiązany z działaniami podejmowanymi przez rozmaite organizacje terrorystyczne z użyciem sieci internetowej, której celem jest zakłócenie pracy sieci komputerowych, wywołanie przez to chaosu i paniki wśród ludzi[32]. Cyberterroryzm ma miejsce wówczas, gdy[33]:

- jest przeprowadzony z wykorzystaniem systemów transmisji danych,
- skutkuje zniszczeniami i dalszymi działaniami przeciwko innym osobom,
- jest wymierzony przeciwko komputerom, sieciom oraz bazom danych, kontrolowanym przez instytucje rządowe,
- wywołuje chaos i panikę,
- doprowadza do zagrożenia życia i zdrowia ludzi,
- prowadzi do eksplozji
- skutkuje znacznymi stratami finansowymi,
- jest wymierzony w elementy infrastruktury krytycznej państwa.

---

[28] M. Górka, *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Wydawnictwo Difin, Warszawa 2014, s. 282.

[29] J. Stelmach, *Bezpieczeństwo terrorystyczne obiektów użyteczności publicznej,* Tom IV, Wydawnictwo Difin, Warszawa 2022, s. 95.

[30] *Infrastruktura krytyczna na celowniku hakerów – czy można ją skutecznie zabezpieczyć?* 12.02.2025, https://rocznikbezpieczenstwa.pl/ojs/index.php/rbm/article/view/449/404, [dostęp: 29.03.2025].

[31] M. Marczyk, M. Stolarz, B. Terebiński, *Bezpieczeństwo działań w cyberprzestrzeni. Wybrane aspekty. Tom I Działania w cyberprzestrzeni*, Akademia Sztuki Wojennej, Warszawa 2022.

[32] A. Gałecki*, Bezpieczeństwo informacji w dobie cyberprzestrzennych zagrożeń*, Wydawnictwo Wyższa Szkoła Bezpieczeństwa, Poznań 2021, s. 69.

[33] S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny*…, op. cit., s. 52.

Cyberterroryzm to terroryzm dokonywany, planowany i koordynowany w cyberprzestrzeni za pomocą komputerów podłączonych do sieci[34]. Cyberterroryzm to również forma współczesnej wojny, którą cechują przede wszystkim niskie koszty działalności. Do przeprowadzenia ataku nie jest wymagane posiadanie specjalistycznego sprzętu. Cyberterroryści dysponują jedynie komputerem oraz siecią internetową. Cyberterrorystów cechuje wysoki stopień anonimowości[35]. Wśród sprawców cyberataków wyróżnić można trzy główne grupy[36]:

- państwowi hakerzy, którzy działają na zlecenie rządów, którzy wykorzystują cyberataki do destabilizacji strategicznych obiektów lub prowadzenia działań szpiegowskich;
- zorganizowane grupy cyberprzestępcze zmotywowane korzyściami finansowymi, stosujące ataki w celu wymuszenia okupu lub kradzieży danych;
- cyberterroryści, których działania mają na celu wywołanie chaosu i zakłócenie funkcjonowania instytucji publicznych oraz przedsiębiorstw. Cyberterroryści wykorzystują platformy i technologie internetowe do rekrutacji, szkolenia, radykalizacji postaw, publicznej prowokacji, propagandy lub w celu planowania, przygotowywania i przeprowadzania ataków terrorystycznych. Zjawisko to wciąż ewoluuje wraz z pojawianiem się nowych platform i usług, umożliwiając terrorystom znajdowanie nowych i innowacyjnych sposobów wykorzystywania możliwości, jakie zapewniają te technologie.

Najczęstszą formą ataku cyberterrorystów na cele infrastruktury krytycznej jest wysłanie do systemów komputerowych wirusów, które uniemożliwiają ich prawidłowe działanie. Rezultatem takiego działania może być np.: utrata kontroli nad systemem, brak komunikacji, czy nawet konieczność wyłączenia systemów. Czynnikiem wzmacniającym działania terrorystów jest wprowadzany przez nich chaos informacyjny, podsycany publikowaniem fałszywych informacji na stronach internetowych. W dobie globalizacji i rozwoju technologicznego poszczególne obiekty infrastruktury krytycznej są

[34] J. Kuck, *Bezpieczeństwo informacyjne. Cyberterroryzm. Przestępczość komputerowa,* Wydawnictwo Państwowej Akademii Nauk Stosowanych w Jarosławiu, Jarosław 2023, s. 105.

[35] J. Stelmach, *Bezpieczeństwo terrorystyczne obiektów użyteczności*,…, op. cit., s. 95.

[36] *Infrastruktura krytyczna na celowniku hakerów – czy można ją skutecznie zabezpieczyć?* 12.02.2025, https://academy.asseco.pl/learning-center/infrastruktura-krytyczna-na-celowniku-hakerow-czy-mozna-ja-skutecznie-zabezpieczyc/, [dostęp: 28.03.2025].

coraz bardziej od siebie współzależne, nie tylko wymiarze funkcjonowania jednego państwa, ale w wymiarze globalnym. Połączenia sieci transkontynentalne powodują, że skutki ewentualnych zakłóceń mogą mieć swój wymiar globalny. Każdy obiekt infrastruktury może być obiektem ataku terrorystycznego. Jedną z najważniejszych cech współczesnego terroryzmu w każdej jego formie jest jego nieprzewidywalność, co do jego formy, czasu i miejsca, użytych środków i skutków[37]. Cyberatakami zagrożone są wszystkie elementy infrastruktury krytycznej, które funkcjonują dzięki technologii informacyjnej. Obszar zagrożeń cyberterrorystycznych obejmuje m.in.[38]:

Systemy wojskowe – które przechowują informacje o położeniu satelitów, rozmieszczeniu wojsk oraz broni, prowadzących badania nad nowymi rodzajami broni i systemami łączności.

Systemy przedsiębiorstw – które przechowują informacje ważne z punktu widzenia działalności firmy, np.: informacje o rezerwacjach, o klientach, o wykorzystywanych technologiach.

Systemy infrastruktury krytycznej tj.: bankowe, finansowe, energetyczne, telekomunikacyjne, dostarczania wody, transportu, służb do działań w sytuacjach wyjątkowych, które przechowują informacje ważne dla bezpieczeństwa państwa.

Systemy ratownicze – realizujące zadania w zakresie ochrony życia i zdrowia np. szpitale, jednostki organizacyjne systemu ochrony zdrowia, np. Państwowe Ratownictwo Medyczne, Lotnicze Pogotowie Ratunkowe.

Systemy transportowe – drogowe, kolejowe, morskie, lotnicze.

Systemy gazowe – rafinerie, koncerny energetyczne i ciepłownicze.

Zagrożenia w cyberprzestrzeni na infrastrukturę krytyczną mają na celu blokowanie dostępu do systemu informatycznego organizacji, włamanie do systemu lub jego całkowite zniszczenie.

Wybrane metody ataków cybernetycznych

Sieć internetowa i infrastruktura komputerowa wykorzystywane są w bezpośrednich cyberatakach oraz jako podstawowe narzędzia do jego przeprowadzenia. W wyniku rozwoju technologii informacyjnej stale wzrastają

[37] J. Stelmach, *Bezpieczeństwo terrorystyczne obiektów użyteczności publicznej,* Tom IV, Wydawnictwo Difin, Warszawa 2022, s. 93.

[38] A. Gałecki, *Bezpieczeństwo informacji w dobie cyberprzestrzennych zagrożeń*, Wydawnictwo Wyższa Szkoła Bezpieczeństwa, Poznań 2021, s. 73-74.

metody jego przeprowadzenia. Do najczęściej stosowanych metod cyberataków należą m.in.[39]:

- robak – to działanie polegające na zainstalowaniu złośliwego oprogramowania samoreplikującego niszczące dane,
- cookies – to technika polegająca na zbieraniu informacji o użytkownikach komputerów,
- phishing – to metoda oparta głównie na inżynierii społecznej, polegającej na podszywaniu się pod instytucje celem kradzieży danych,
- exploit – to użycie złośliwego oprogramowania, pozwalającego na bezpośredni dostęp do komputera ofiary,
- hijacking – obejmuje przechwycenie transmisji danych pomiędzy dwoma komputerami,
- inżynieria społeczna – to atak wykorzystujący niekompetencję i niewiedzę osób w zakresie działania systemów komputerowych,
- spam – polegający wysyłaniu na konto pocztowe atakowanego dużej ilości niechcianych wiadomości tekstowych,
- spoofing – to podszycie się pod urządzenie w sieci, w celu dokonania włamania do systemu,
- ransomware – to forma złośliwego oprogramowania, która blokuje użytkownika z jego plików lub urządzenia, a następnie żąda zapłaty za przywrócenie dostępu, atakujący ransomware uderzają w firmy, organizacje oraz indywidualnych użytkowników[40].

W ostatnim czasie obserwujemy tendencję do podejmowania w niej działań stricte operacyjnych atakowanie sieci teleinformatycznych i systemów technologicznych, mających strategiczne znaczenie dla bezpieczeństwa państwa. Warto podkreślić, że ataki cybernetyczne i operacje na szerszą skalę mogą podejmować zarówno grupy przestępcze, terrorystyczne, jak i państwa, w ramach szeroko rozumianej wojny informacyjnej. Z pewnością można stwierdzić, że wszystkie rodzaje niebezpieczeństw istniejących w tradycyjnej, fizycznej geoprzestrzeni będą mieć swoje odpowiedniki w cyberprzestrzeni.

[39] J. Kuck*, Bezpieczeństwo informacyjne. Cyberterroryzm. Przestępczość*…, op. cit., s. 75-77.

[40] M. Marczyk, M. Stolarz, B. Terebiński, *Bezpieczeństwo działań w cyberprzestrzeni. Wybrane aspekty. Tom II...,* op. cit., s. 82-84.

Charakterystyka wybranych ataków cybernetycznych na infrastrukturę krytyczną – studium przypadku

Do podmiotów dokonujących ataków cyberterrorystycznych należy zaliczyć zorganizowane grupy lub osoby działające indywidualnie. Wskazując na zagrożenia infrastruktury krytycznej można wyróżnić obiekty, instytucje oraz systemy wykorzystujące transmisję informacji w cyberprzestrzeni. Przykładem cyberterroryzmu na systemy infrastruktury krytycznej jest cyberatak na Lotnicze Pogotowie Ratunkowe w Polsce. W lutym 2022 r. celem cyberataku stało się Lotnicze Pogotowie Ratunkowe. Mimo informatycznego zamachu ani jeden dyżur nie został zawieszony, wszystkie wezwania do misji ratunkowych i transportów międzyszpitalnych były na bieżąco realizowane. Przez ponad tydzień po ataku cyberprzestępców jednostki Lotniczego Pogotowia Ratunkowego w całym kraju były pozbawione możliwości korzystania ze swoich systemów komputerowych. Niedostępne były systemy kluczowe dla działania pogotowia, jak system przesyłania informacji o prowadzonych interwencjach, strona www i poczta elektroniczna. Hakerzy zażądali okupu w wysokości 390 tysięcy dolarów, czyli około 1,5 mln złotych[41]. Najnowszym i najlepszym przykładem cyberterroryzmu jest eskalacja agresji Rosji na Ukrainę z lutego 2022 roku, która zapoczątkowała nowy etap rozwoju stosunków międzynarodowych i bezpieczeństwa globalnego[42]. Od początku wojny w Ukrainie w zasadzie możemy mówić o ciągłych, nieustających cyberoperacjach w postaci ataków na sieci i systemy informatyczne, cyberszpiegostwie oraz operacjach psychologicznych i informacyjnych radykalizujących społeczeństwo. Rosyjskim cybernetycznym "przygotowaniem ogniowym" w kierunku Ukrainy była m.in. masowa podmiana stron ukraińskich urzędów, wysyłanie fałszywych maili/sms-ów oraz ataki DDoS na witryny wojskowe, urzędowe oraz bankowe, portale informacyjne i dostawców usług internetowych. Rząd ukraiński zaapelował do podziemia hakerskiego o odpowiedź. Właściciel ukraińskiej firmy Cyber Unit Technologies wyznaczył nagrodę: 100 tys. dolarów za włamanie do rosyjskich systemów IT. Do ataku na rosyjskie

[41] M. Stańczyk, K. Lechowicz-Dyl, *Cyberatak na Lotnicze Pogotowie Ratunkowe. Hakerzy zażądali 390 tys. dolarów okupu*, PAP, 21 lutego 2022 r., https://www.pap.pl/aktualnosci/news%2C1086018%2Ccyberatak-na-lotnicze-pogotowie-ratunkowe-hakerzy-zazadali-390-tys-dolarow, [dostęp: 29.03.2025].

[42] R. Panas, *Wojna cybernetyczna i cyberterroryzm – czym są? Czy Polsce grozi cyberwojna?* 10 marca 2022 r., https://nano.komputronik.pl/n/cyberwojna-cyberterroryzm-wojna-cybernetyczna/, [dostęp: 29.03.2025].

serwery ruszyła też międzynarodowa grupa Anonymous. Większość rosyjskich cyberataków skierowana była na agencje wojskowe i rządowe oraz na infrastrukturę krytyczną, zwłaszcza na dostawców usług telekomunikacyjnych oraz firmy energetyczne. Najczęstszą techniką infiltracji stosowaną w cyberwojnie jest phishing, przy czym obie strony stosują ukierunkowane kampanie phishingowe, często z towarzyszącymi im exploitami plikowymi lub innymi szkodliwymi ładunkami, wskazują eksperci. Exploit[43] to kod programu służący do przeprowadzenia ataku wykorzystujący luki w zabezpieczeniach powszechnie wykorzystywanych aplikacji. Phishing jest popularny w cyberwojnie, ponieważ jest prosty, mało ryzykowny, skuteczny i wszechstronny.

Podsumowanie

Jednym z największych zagrożeń cywilizacyjnych XXI wieku jest terroryzm, który wywołuje psychozę strachu i zaniepokojenie mieszkańców całego globu. Obecnie, ochrona cyberprzestrzeni stała się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa i obronności państwa. Cyberprzestrzeń staje się nową przestrzenią funkcjonowania ludzi, państwa i świata, które przyjmuje postać społeczeństwa sieciowego. Społeczeństwo sieciowe porusza się w organizacji sieciowej, która złożona jest z setek tysięcy połączonych ze sobą sieci komputerów, routerów, przełączników i linii światłowodów, które pozwalają funkcjonować obiektom infrastruktury krytycznej. Cyberterroryzm staje się najbardziej nieprzewidywalnym sposobem oddziaływania zorganizowanych grup na funkcjonowanie i stabilność struktur państwowych. Pojawiła się kategoria infrastruktury krytycznej, której zniszczenie lub uszkodzenie może osłabić zdolność obronną oraz bezpieczeństwo państwa. Główne jej elementy to: telekomunikacja, system energetyczny, system bankowy, produkcja oraz sieć transportu gazu ziemnego i ropy naftowej, transport, system zaopatrzenia w wodę, służby ratownicze oraz ciągłość funkcjonowania administracji publicznej.

Działalność organizacji terrorystycznych w cyberprzestrzeni jest faktem. Organizacje dysponują zarówno potencjałem finansowym, jak i doskonale przygotowaną kadrą informatyków, którzy są gotowi wykorzystać swoje umiejętności realizując cele ideologiczne, ekonomiczne lub polityczne.

[43] J. Kuck, *Bezpieczeństwo informacyjne. Cyberterroryzm*…, op. cit., s.79.

Walka z cyberterroryzmem jest bardzo droga i trudna, ze względu na bezmiar cyberprzestrzeni i ogromne trudności związane ze zlokalizowaniem cyberterrorystów. Walką z cyberterroryzmem zajmują się agendy ONZ m.in. Komitet ds. Zwalczania Terroryzmu oraz NATO w zakresie wojny hybrydowej. Walkę z tego rodzaju zagrożeniami prowadzą również specjaliści z Europol i Interpol. Europol m.in. koordynuje transgraniczne policyjne akcje przeciwko cybergangom, a Interpol wspiera mundurowych walczących z cyberterroryzmem w skali globalnej.

Literatura

1. Cegiełka R., *Zagrożenie terroryzmem. Poczucie bezpieczeństwa na początku XXI wieku oraz wpływ terroryzmu na procesy gospodarcze w wymiarach mikro i makro,* Wydawnictwo Agencja Wydawnicza Synergy Elżbieta Meissner, Warszawa 2015.
2. Dróżdż D., *Terroryzm we współczesnym świecie w świetle prawa. Terror oraz terroryzm międzynarodowy i globalny z prawnego punktu widzenia*. Tom 2, Wydawnictwo My Book, Warszawa 2021.
3. Gałecki A., *Bezpieczeństwo informacji w dobie cyberprzestrzennych zagrożeń,* Wydawnictwo Wyższa Szkoła bezpieczeństwa, Poznań 2021.
4. Górka M., *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Wydawnictwo Difin, Warszawa 2014.
5. Kuck J., *Bezpieczeństwo informacyjne. Cyberterroryzm. Przestępczość komputerowa*, Wydawnictwo Państwowej Akademii Nauk Stosowanych w Jarosławiu, Jarosław 2023.
6. Kuźniar R., Bezpieczeństwo międzynarodowe, Wydanie drugie rozszerzone, Wydawnicto naukowe SCHOLAR, Warszawa 2022.
7. Lebiedź J., Krztoń W., Stefaniuk B., *Współczesne wyzwania bezpieczeństwa narodowego. Zarządzanie kryzysowe. Wojna w cyberprzestrzeni. Rzeczywistość wirtualna,* Wydawnictwo Texter, Warszawa 2018.
8. Olech A., *Walka z terroryzmem polskie a francuskie doświadczenie*, Wydawnictwo Difin, Warszawa 2021.
9. Malewska A. Filary-Szczepanik M., *Globalizacja i współzależność*, Wydawnictwo Naukowe Akademii Ignatianum w Krakowie, Kraków 2022.
10. Marczyk M., Stolarz M., Terebiński B., *Bezpieczeństwo działań w cyberprzestrzeni. Wybrane aspekty. Tom I Działania w cyberprzestrzeni*, Akademia Sztuki Wojennej, Warszawa 2022.
11. Marczyk M., Stolarz M., Terebiński B., *Bezpieczeństwo działań w cyberprzestrzeni. Wybrane aspekty. Tom II Działania w cyberprzestrzeni*, Akademia Sztuki Wojennej, Warszawa 2022.
12. Różański P., Warmiński A., Chałupczak H*., Zagrożenia bezpieczeństwa i porządku publicznego we współczesnej Polsce (wybrane aspekty),* Akademia Wychowania Fizycznego Józefa Piłsudskiego w Warszawie, Wydział Wychowania Fizycznego i zdrowia w Białej Podlaskiej, Biała Podlaska 2023.

13. Rytko-Marczewska M., *Haktywizm (Cyberterroryzm, Haking, Protest obywatelski, Cyberaktywizm, E- Moblilizacja)* , Wydawnictwo UMCS Lublin, Lublin 2014.
14. Stelmach J., *Bezpieczeństwo terrorystyczne obiektów użyteczności publicznej*, Tom III, Wydawnictwo Difin, Warszawa 2022.
15. Stelmach J., *Bezpieczeństwo terrorystyczne obiektów użyteczności publicznej*, Tom IV, Wydawnictwo Difin, Warszawa 2022.
16. Stelmach J., *Zamachy terrorystyczne. Istota i koncepcja reagowania*, Wydawnictwo Difin, Warszawa 2023.
17. Wojciechowska – Filipek S., Ciekanowski Z., Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki- organizacji- państwa, Wydawnictwo CedeWu, Warszawa 2016.
18. Wojciechowski S., Osiewicz P., *Zrozumieć współczesny terroryzm*, Wydawnictwo Difin, Warszawa 2017.
19. Zieliński T., Mróz P., Bartnik R., *Bezpieczeństwo i obrona Unii Europejskiej*, Akademia Sztuki Wojennej, Warszawa 2020.

Akt prawny

1. Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. 1997 Nr 88, poz. 553).

Netografia

1. *Globalizacja – szanse i zagrożenia*, https://globalna.ceo.org.pl/materialy/globalizacja-szanse-i-zagrozenia/.
2. *Globalny*, Słownik PWN, https://sjp.pwn.pl/slowniki/globalny.html.
3. *Infrastruktura krytyczna na celowniku hakerów – czy można ją skutecznie zabezpieczyć?* 12.02.2025, https://academy.asseco.pl/learning-center/infrastruktura-krytyczna-na-celowniku-hakerow-czy-mozna-ja-skutecznie-zabezpieczyc/.
4. Marszycki M., *Cyberwojna między Rosją a Ukrainą wciąż trwa*, 3 marca 2023 r., https://itwiz.pl/cyberwojna-miedzy-rosja-a-ukraina-wciaz-trwa/.
5. Oleksiewicz I., *Cyberterroryzm jako realne zagrożenie dla Polski*, https://rocznikbezpieczenstwa.pl/ojs/index.php/rbm/article/view/449/404.https://rocznikbezpieczenstwa.pl/ojs/index.php/rbm/article/view/449/404.
6. Panas R., *Wojna cybernetyczna i cyberterroryzm – czym są? Czy Polsce grozi cyberwojna?* 10 marca 2022 r., https://nano.komputronik.pl/n/cyberwojna-cyberterroryzm-wojna-cybernetyczna/.
7. Stańczyk M., Lechowicz-Dyl K., *Cyberatak na Lotnicze Pogotowie Ratunkowe. Hakerzy zażądali 390 tys. dolarów okupu*, PAP, 21 lutego 2022 r., https://www.pap.pl/aktualnosci/news%2C1086018%2Ccyberatak-na-lotnicze-pogotowie-ratunkowe-hakerzy-zazadali-390-tys-dolarow.
8. Smolski W., *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*. https://www.repozytorium.uni.wroc.pl/dlibra/publication/67850, [dostęp: 29.03.2025].