Ewelina AMBROZIK
Uniwersytet w Siedlcach
Wydział Nauk Społecznych
ewelina.ambrozik01@gmail.com
https://orcid.org/0009-0008-5373-6712
Kacper JADCZAK
Uniwersytet w Siedlcach
Wydział Nauk Społecznych
kacper.jadczak21@onet.pl
https://orcid.org/0009-0003-0102-8427
https://doi.org/10.34739/dsd.2026.01.11

SAMOTNE WILKI W CYBERPRZESTRZENI – NOWE ZAGROŻENIE W DZIEDZINIE TERRORYZMU W CYBERPRZESTRZENI

ABSTRAKT: Artykuł podejmuje problematykę nowego, dynamicznie rozwijającego się zjawiska w obszarze terroryzmu internetowego, jakim są tzw. cyberwilki – sprawcy działający samodzielnie, łączący w sobie cechy klasycznych samotnych wilków oraz hakerów. Autorzy stawiają hipotezę, że cyberwilki stanowią autonomiczną kategorię podmiotów terroryzmu asymetrycznego, której nie można sprowadzić ani do postaci hakera działającego dla zysku, ani do terrorysty funkcjonującego w ramach zorganizowanej struktury. W artykule dokonano przeglądu literatury przedmiotu oraz raportów instytucji odpowiedzialnych za bezpieczeństwo, a także przeprowadzono analizę przypadku. Na tej podstawie wyodrębniono trzy główne kategorie cyberwilków: ideologicznych (hacktywiści), motywowanych osobistą zemstą oraz motywowanych psychopatologicznie. Przeprowadzona analiza wskazuje, że cyberwilki są zjawiskiem narastającym, a ich potencjał destrukcyjny często przewyższa możliwości zorganizowanych grup terrorystycznych ze względu na brak wewnętrznych mechanizmów kontroli, efekt zaskoczenia oraz trudności w przewidywaniu ich działań. Artykuł zamyka teza, że cyberwilki stanowią autonomiczną i dynamicznie rozwijającą się gałąź terroryzmu internetowego, wymagającą odrębnego ujęcia definicyjnego i analitycznego.

SŁOWA KLUCZOWE: cyberterroryzm, cyberwilk, samotny wilk, asymetryczne zagrożenie, infrastruktura krytyczna

LONE WOLVES IN CYBERSPACE – A NEW THREAT IN THE FIELD OF INTERNET TERRORISM

ABSTRACT: This article addresses a new, dynamically developing phenomenon in the field of online terrorism: so-called cyberwolves – perpetrators operating independently, combining the characteristics of classic lone wolves and hackers. The authors hypothesize that cyberwolves constitute an autonomous category of asymmetric terrorism actors, which cannot be reduced to either a hacker operating for profit or a terrorist operating within an organized structure. The article reviews the relevant literature and reports from security institutions, and analyzes case studies. Based on this, three main categories of cyberwolves were identified: ideological (hacktivists), those motivated by personal vengeance, and those motivated by psychopathology. The analysis indicates that cyberwolves are a growing phenomenon, and their destructive potential often exceeds the capabilities of organized terrorist groups due to the lack of internal control mechanisms, the surprise effect, and the difficulty in predicting their actions. The article concludes with the thesis that cyberwolves constitute an autonomous and dynamically developing branch of internet terrorism, requiring a separate definitional and analytical approach.

KEYWORDS: cyberterrorism, cyberwolf, lone wolf, asymmetric threat, critical infrastructure

WPROWADZENIE

Rozwój technologii informacyjno-komunikacyjnych w ostatnich latach przyniósł nie tylko korzyści społeczne i gospodarcze, ale także nowe obszary aktywności o charakterze destrukcyjnym. Wraz z upowszechnieniem się dostępu do narzędzi hakerskich, wiedzy specjalistycznej oraz możliwości zachowania anonimowości, pojawiła się tym samym nowa kategoria sprawców-cyberterrorystów – cyberwilki. To pojedyncze osoby, wykorzystujące cyberprzestrzeń do realizacji celów wykraczających poza klasyczną przestępczość komputerową[1]. Zjawisko to, określane w niniejszym artykule mianem cyberwilków, wykazuje istotne podobieństwa do koncepcji „samotnych wilków"[2] (lone wolves) w terroryzmie klasycznym – sprawców, nienależących do formalnych struktur organizacji terrorystycznych, lecz podejmujących działania motywowane własnymi przekonaniami. Równocześnie posługują się metodami właściwymi dla środowiska hakerskiego, co sprawia, że ich kwalifikacja definicyjna pozostaje niejednoznaczna[3].

W literaturze przedmiotu oraz w praktyce obserwuje się tendencję do klasyfikowania tego rodzaju sprawców albo jako cyberprzestępców (ze względu na narzędzia), albo jako terrorystów (ze względu na cele i skutki). Tymczasem, jak zostanie to wykazane w dalszej części artykułu, łączy on w sobie obie te cechy w sposób nierozerwalny: jest terrorystą posługującym się metodami hakerskimi, a jednocześnie hakerem działającym z motywacją terrorystyczną.

Dobrze znane już pojęcie terroryzmu pojawiło się stosunkowo niedawno i dotyczyło sytuacji, jaka miała miejsce w Stanach Zjednoczonych Ameryki i zamachu na WTC w 2001 r., wtedy to właśnie rozpoczęła się „oficjalna" wojna z terroryzmem, jaki znamy dziś. Zarówno ówcześnie, jak i obecnie działania asymetryczne stosowane przez terrorystów stanowiły zupełnie nieznaną i wcześniej niesklasyfikowaną dziedzinę, której zwalczanie i przeciwdziałanie stało się praktycznie niemożliwe. Największym problemem napotkanym przez systemy bezpieczeństwa wewnętrznego państw był problem ze zlokalizowaniem i określeniem potencjalnego terrorysty, a przede wszystkim jego przynależności państwowej, celu, środków i metod działań[4].

Początek XXI w. to okres destabilizowania państw nie potęgą militarną czy gospodarczą, skupiającą w sobie ogromny zakres sił i środków, lecz pojedynczych lub bardzo małych grup, działających na własną rękę, praktycznie niemożliwych do zlokalizowania i używających prymitywnych metod. Model ten w szerszej perspektywie nazywany jest samotnymi wilkami – pojedynczymi osobami działającymi na podstawie własnych pobudek, niezrzeszonych w żadnej organizacji albo współpracującej na zasadzie know-how[5]. To samo zjawisko pojawia się obecnie, tyle że przenosi się, jak większość obecnych działań, do świata cyberprzestrzeni.

[1] N. Czarnota, *Rola Agencji Bezpieczeństwa Wewnętrznego i Policji w zwalczaniu cyberterroryzmu,* „Studia Bezpieczeństwa Narodowego" 2020, 10(18), s. 112-113.
[2] *Lone Wolf Attacks Are Becoming More Common – And More Deadly*, „FRONTLINE", https://www.pbs.org/wgbh/frontline/article/lone-wolf-attacks-are-becoming-more-common-and-more-deadly/ (05.04.2026).
[3] D. Kucharek, *Model typowania sprawców zamachów z wykorzystaniem bojowych środków chemicznych,* „Przegląd Geopolityczny" 2023, t. 44, s. 107-108.
[4] J. Piątek, *Długa wojna z terroryzmem*, „Rocznik Bezpieczeństwa Międzynarodowego" 2019, 2, s. 51-62.
[5] Praktyczna, niejawna wiedza i doświadczenie, które pozwalają wykonywać zadania szybciej, lepiej lub taniej.

Literatura przedmiotu nie znalazła jeszcze osobnej definicji tej instytucji. Na potrzeby opracowania i na podstawie podobieństw można zdefiniować to jako cyberwilki[6].

Przyjęta wstępna analiza pozwoliła na sformułowanie głównego celu artykułu, jakim jest analiza rozwoju cyberterroryzmu – nowego zagrożenia dla bezpieczeństwa państw i użytkowników sieci, identyfikacja kluczowych wyzwań oraz przedstawienie rekomendacji dotyczących wzmocnienia zdolności systemów bezpieczeństwa państw w zakresie cyberbezpieczeństwa.

Przyjęcie celu artykułu umożliwiło sprecyzowanie problemu badawczego w formie pytania: Jakie miejsce cyberwilki zajmują w typologii współczesnego terroryzmu internetowego w porównaniu ze zorganizowanymi grupami terrorystycznymi i klasycznymi samotnymi wilkami? Naturalnym następstwem przyjętego problemu badawczego było sformułowanie następujących szczegółowych problemów badawczych, zawierających się w pytaniach:

1. Jakie kategorie cyberwilków można wyodrębnić ze względu na motywacje, metody działania oraz potencjał destrukcyjny?
2. Czy cyberwilki zasługują na miano autonomicznego podmiotu terroryzmu asymetrycznego, czy też powinni być traktowani jako subkategoria w ramach szerszego zjawiska terroryzmu internetowego?

Sformułowanie problemów szczegółowych umożliwiło postawienie głównego celu artykułu: analiza zjawiska cyberwilków jako autonomicznej kategorii podmiotów terroryzmu asymetrycznego, ze szczególnym uwzględnieniem relacji między tożsamością terrorysty a tożsamością hakera oraz określeniem miejsca tych sprawców w typologii współczesnego terroryzmu internetowego.

Przyjęcie głównego celu artykułu umożliwiło autorowi sprecyzowanie następującej hipotezy badawczej: cyberwilki stanowią autonomiczną kategorię podmiotów terroryzmu asymetrycznego, nie dającej się sprowadzić ani do klasycznego hakera działającego dla zysku, ani do terrorysty działającego w strukturze organizacyjnej. Ich samodzielność, połączona z dostępem do narzędzi hakerskich oraz motywacją o charakterze terrorystycznym, tworzy nową jakość sprawczą, wymagającą odrębnego ujęcia definicyjnego i analitycznego.

Analizując powyższe zjawisko jako podmiot terroryzmu asymetrycznego, zastosowano kilka metod badawczych. Przeprowadzono analizę treści dostępnych raportów instytucji bezpieczeństwa (Europol, ENISA, CISA) oraz artykułów eksperckich związanych z tematyką terroryzmu internetowego i cyberprzestępczości. Dokonano przeglądu i analizy literatury naukowej przedmiotu, co pozwoliło na zrozumienie szerszego kontekstu definicyjnego oraz ewolucji zjawiska samotnych wilków w cyberprzestrzeni. Dodatkowo zastosowano studium przypadku, koncentrując się na konkretnych atakach przeprowadzonych przez pojedynczych sprawców (m.in. atak na system uzdatniania wody w Oldsmar, serię ataków DDoS na europejskie szpitale, działania byłych pracowników wobec infrastruktury krytycznej) oraz ich skutkach dla bezpieczeństwa publicznego i funkcjonowania organów. Pozwoliło to na zastosowanie analizy porównawczej, uwzględniającej różnice i podobieństwa między poszczególnymi kategoriami

[6] G. Nowacki, *Zjawisko Terroryzmu W XXI Wieku*, „Studia Bezpieczeństwa Narodowego" 2014, 4(5), s. 403-404.

sprawców (ideologiczni, motywowani zemstą, motywowani psychopatologicznie). Analiza ta była wsparta badaniami jakościowymi, polegającymi na interpretacji motywacji sprawców, ich metod działania oraz kontekstu społeczno-politycznego poszczególnych zdarzeń, co umożliwiło pełniejsze zrozumienie dynamicznie zmieniającego się charakteru zagrożeń terrorystycznych w cyberprzestrzeni.

SAMOTNE WILKI W CYBERPRZESTRZENI – NOWE ZAGROŻENIE W DZIEDZINIE CYBERTERRORYZMU

Współczesne środowisko bezpieczeństwa wewnętrznego i zewnętrznego charakteryzuje się dynamicznym rozwojem zagrożeń asymetrycznych, wśród nich szczególne miejsce zajmuje terroryzm. Tradycyjne ujęcie tego zjawiska, to „różnie umotywowane ideologicznie, planowane i zorganizowane działania pojedynczych osób lub grup skutkujące naruszeniem istniejącego porządku prawnego, podjęte w celu wymuszenia od władz państwowych i społeczeństwa określonych zachowań i świadczeń, często naruszające dobra osób postronnych. Działania te realizowane są z całą bezwzględnością, za pomocą różnych środków (przemoc fizyczna, użycie broni i ładunków wybuchowych), w celu nadania im rozgłosu i celowego wytworzenia lęku w społeczeństwie”[7].

Zjawisko „samotnych wilków” (lone wolves) w terroryzmie klasycznym jest przedmiotem badań od ponad dwóch dekad. Jak wskazuje literatura, samotne wilki można podzielić na pięć głównych kategorii: motywowanych politycznie, religijnie, pojedynczymi zagadnieniami (single-issues), chęcią zysku oraz zaburzeniami osobowości lub problemami psychicznymi. Do najbardziej tragicznych w skutkach przykładów klasycznego samotnego wilka należą zamachy Timothy’ego McVeigha w Oklahoma City (1995)[8], który zabił 168 osób, oraz Andersa Breivika w Norwegii (2011)[9] – 77 ofiar śmiertelnych[10].

Jednakże wraz z rozwojem technologii informacyjno-komunikacyjnych oraz powszechnym dostępem do Internetu zjawisko samotnych wilków uległo znaczącej transformacji. Cyberprzestrzeń staje się dla nich nie tylko narzędziem radykalizacji i poszukiwania inspiracji, ale także, co istotne, bezpośrednim środowiskiem działania.

W kontekście tym pojawia się potrzeba zdefiniowania i scharakteryzowania nowego typu sprawcy, łączącego w sobie cechy terrorysty (motywacja polityczna, społeczna lub psychopatologiczna, cel w postaci zastraszenia i destabilizacji) oraz hakera (kompetencje techniczne, wykorzystanie narzędzi hakerskich, działanie w środowisku cyfrowym). Cyberterroryzm

[7] Definicje zaproponowane przez środowiska akademickie, https://www.unic.un.org.pl/terroryzm/d- efinicje.php, (05.04.2026).
[8] Federal Bureau of Investigation. (b.d.). „Timothy McVeigh”. FBI Vault, https://vault.fbi.gov/timothy-j.-mcveigh (01.07.2026)
[9] M. Czerniak, *Zamachy w Oslo i na wyspie Utøya w 2011 roku: analiza wydarzeń, reakcji służb i wniosków dla zarządzania kryzysowego,* „Studia de Securitate” 2024, 14(2), s. 250-263.
[10] O. Radkiewicz, *Terroryzm “samotnych wilków” na wybranych przykładach,* „SDirect24 Scientific Journal” 2021, 1, s. 66-67.

stanowi nową jakość w badaniach nad bezpieczeństwem, wymagającą interdyscyplinarnego podejścia łączącego wiedzę z zakresu nauk o bezpieczeństwie, socjologii oraz informatyki.

Terroryzm jako forma walki politycznej nie jest zjawiskiem nowym. Jego korzenie sięgają starożytności, jednakże w swojej nowoczesnej formie wykształcił się w okresie rewolucji francuskiej, termin ten po raz pierwszy wszedł do powszechnego użycia na określenie działań rządu rewolucyjnego wobec przeciwników politycznych. W XIX wieku terroryzm przybrał formę działań skrajnie lewicowych ugrupowań anarchistycznych, których ataki – często o charakterze indywidualnym – wstrząsały Europą i Stanami Zjednoczonymi[11].

W XX wieku terroryzm ewoluował w kierunku działań zorganizowanych grup o charakterze nacjonalistycznym, lewicowym, a następnie religijnym. Kluczowym momentem w rozwoju współczesnego terroryzmu był rok 1968, wyznaczył on początek „nowej fali" terroryzmu o charakterze międzynarodowym. W tym okresie dominowały ugrupowania takie jak Włoskie Czerwone Brygady (*Brigate Rosse*), niemiecka Frakcja Czerwonej Armii (*Rote Armee Fraktion* – RAF) czy Baskonia i Wolność (*Euskadi Ta Askatasuna* – ETA), działające w ramach rozbudowanych struktur organizacyjnych[12].

Definicja terroryzmu pozostaje jednym z najbardziej spornych zagadnień w naukach o bezpieczeństwie. Jak słusznie zauważa się w literaturze przedmiotu, problem definicyjny wynika z trzech głównych czynników: wartościującego charakteru pojęcia, różnic w podejściu prawnym poszczególnych państw oraz ewoluującego charakteru samego zjawiska[13].

Dla potrzeb analizy cyberwilków kluczowe znaczenie ma definicja terroryzmu akcentująca cel działania – zastraszenie i wymuszenie oraz charakter sprawcy. W polskim porządku prawnym terroryzm definiowany jest w art. 115 § 20 Kodeksu karnego jako czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu poważnego zastraszenia wielu osób, zmuszenia organu władzy państwowej lub samorządu terytorialnego do podjęcia lub zaniechania określonych działań lub wywołania zakłóceń w systemie konstytucyjnym Rzeczypospolitej Polskiej[14].

Cyberterroryzm jako kategoria analityczna wyłoniła się w latach 90. XX wieku wraz z upowszechnieniem dostępu do Internetu oraz cyfryzacją kluczowych sektorów gospodarki. Za prekursorkę definicji cyberterroryzmu uznaje się Dorothy Denning (2000), określiła go jako „nielegalne ataki lub groźby ataków na komputery, sieci oraz przechowywane w nich informacje, podejmowane w celu zastraszenia lub przymuszenia rządu lub społeczeństwa w realizacji celów politycznych lub społecznych"[15].

Definicja Denning wyznacza trzy kluczowe elementy konstytutywne cyberterroryzmu:

1. działanie o charakterze nielegalnym,
2. skierowane na systemy teleinformatyczne,

[11] *Ibidem*, s. 51-62.
[12] T. Aleksandrowicz, *Rok 1968 – początek terroryzmu?*, „Rocznik Polsko-Niemiecki" 2010, 10(23), s. 11-22.
[13] M. Gołda-Sobczak, W. Sobczak, *Problem definicji terroryzmu*, „THEMIS POLSKA NOVA" 2018, 2(14), s. 92-94.
[14] Ustawa z dnia 6 czerwca 1997 r., *Kodeks karny*, Dz. U. 1997 Nr 88 poz. 553, art. 115 § 20 .
[15] Oświadczenie Dorothy E. Denning, https://irp.fas.org/congress/2000_hr/00-05-23denning.htm (05.04.2026).

3. podejmowane w realizacji celów politycznych lub społecznych poprzez wywołanie strachu.

Kluczowe pytanie w badaniach nad cyberterroryzmem dotyczy jego relacji do terroryzmu klasycznego. Czy cyberterroryzm jest jedynie nowym narzędziem w rękach tradycyjnych organizacji terrorystycznych, czy też stanowi odrębne zjawisko o własnej dynamice?

W literaturze coraz częściej możemy spotkać się ze stwierdzeniem, że współczesny terroryzm wykorzystuje Internet nie tylko jako narzędzie komunikacji i radykalizacji czy pozyskiwania nowych członków, ale także jako bezpośrednie środowisko działania. W przypadku zamachów w Nicei (2016), Berlinie (2016), Londynie (2017), Manchesterze (2017) i Strasburgu (2018) Internet odgrywał kluczową rolę w procesie radykalizacji sprawców, umożliwiając łatwy dostęp do propagandy oraz komunikację z innymi radykałami.

Pojęcie „samotnego wilka" weszło do kanonu badań nad terroryzmem na początku XXI wieku, choć samo zjawisko jest znacznie starsze. Definicje samotnego wilka bardzo często podają „osobę działającą samodzielnie, bez bezpośredniego wsparcia organizacji terrorystycznej, podejmującej działania na własną rękę, często po procesie samoradykalizacji"[16].

Kluczowe cechy samotnego wilka w ujęciu obejmują:

- działanie samodzielne – brak przynależności do formalnej organizacji terrorystycznej;
- brak bezpośredniego wsparcia – sprawca nie otrzymuje bezpośrednich instrukcji, finansowania ani logistyki od zorganizowanej struktury;
- samoradykalizacja – proces przyjmowania ekstremistycznej ideologii przebiega niezależnie, często z wykorzystaniem dostępnych w Internecie treści;
- motywacja wewnętrzna – decyzja o podjęciu działań wynika z indywidualnych przekonań, a nie z polecenia przełożonych[17].

W literaturze przedmiotu wypracowano kilka typologii samotnych wilków. Kompleksowa klasyfikacja wyróżnia pięć kategorii sprawców:

1. Polityczni – działający z motywacji ideologicznych, dążący do zmiany systemu politycznego lub określonej polityki państwa. Przykładem jest Timothy McVeigh, który w 1995 roku dokonał zamachu w Oklahoma City w proteście przeciwko polityce rządu federalnego USA.
2. Religijni – kierujący się ekstremistyczną interpretacją doktryny religijnej, często inspirowani przez organizacje takie jak Al-Kaida czy Państwo Islamskie.
3. Pojedynczego zagadnienia – działający w imię ochrony zwierząt, środowiska naturalnego lub innych specyficznych spraw. Ich celem jest zwrócenie uwagi na określony problem poprzez akty przemocy.
4. Kierowani chęcią zysku – wykorzystujący przemoc dla osiągnięcia korzyści materialnych, choć w przypadku terroryzmu ta kategoria budzi kontrowersje definicyjne.

[16] *Ibidem*, s. 64-66.

[17] Osoby działające w pojedynkę jako wyzwanie w zakresie zapobiegania brutalnemu ekstremizmowi i zwalczania go, https://home-affairs.ec.europa.eu/document/download/83ad8ae0-d018-4fba-9df9-923aa55dcf9b_pl (05.04.2026)

5. zaburzeniami osobowości – działający pod wpływem problemów psychicznych, często z wyimaginowanym poczuciem misji. W tej kategorii trudno jednoznacznie odróżnić motywację terrorystyczną od działań wynikających z choroby psychicznej[18].

Klasyfikacja ta, choć opracowana na gruncie terroryzmu klasycznego, znajduje zastosowanie także w analizie przedmiotu z zastrzeżeniem, że w przypadku działań w cyberprzestrzeni kategorie te często się przenikają, a motywacje sprawców mogą być mieszane.

Przeniesienie koncepcji samotnego wilka na grunt cyberprzestrzeni prowadzi do wyodrębnienia nowej kategorii sprawcy – cyberwilka. Na podstawie analizy dostępnej literatury przedmiotu oraz studiów przypadków można zidentyfikować następujące cechy konstytutywne tego zjawiska.

Po pierwsze, działanie samodzielne. Cyberwilk, podobnie jak klasyczny samotny wilk, nie należy do formalnych struktur organizacji terrorystycznej ani zorganizowanej grupy przestępczej. Jego działania są wynikiem indywidualnej decyzji, a proces radykalizacji przebiega samodzielnie, często z wykorzystaniem dostępnych w Internecie treści.

Po drugie, wykorzystanie narzędzi hakerskich. W odróżnieniu od klasycznego samotnego wilka, posługującego się bronią fizyczną, cyberwilk działa w środowisku cyfrowym, wykorzystując narzędzia hakerskie od prostych ataków DDoS po zaawansowane złośliwe oprogramowanie. Samotne wilki w cyberprzestrzeni zyskują dostęp do zaawansowanych narzędzi w modelu „as-a-service”[19], co znacząco obniża próg wejścia i zwiększa ich potencjał destrukcyjny.

Po trzecie, cel o charakterze terrorystycznym. Działania ukierunkowane są na wywołanie strachu, destabilizację funkcjonowania instytucji lub wymuszanie określonych zachowań politycznych lub społecznych. W tym sensie cyberwilk jest terrorystą – różni się od klasycznego terrorysty jedynie narzędziami, którymi się posługuje.

Po czwarte, anonimowość i zasięg globalny. Działanie w cyberprzestrzeni umożliwia zachowanie anonimowości oraz przeprowadzenie ataku z dowolnego miejsca na świecie, niezależnie od lokalizacji celu[20].

Istotne znaczenie dla prawidłowego ujęcia zjawiska cyberterrorystów ma odróżnienie ich od klasycznych hakerów działających dla zysku. Jak słusznie zauważa się w literaturze przedmiotu, kluczowym kryterium różnicującym jest cel działania. Haker działający dla zysku (np. w ramach zorganizowanej grupy ransomware) jest przestępcą, ale nie terrorystą. Jego celem jest uzyskanie korzyści materialnej, a zakres działań jest ograniczony racjonalnością ekonomiczną. Cyberwilk natomiast kieruje się motywacją terrorystyczną, jego celem jest zastraszenie, destabilizacja, wywołanie chaosu. W konsekwencji jego działania mogą być bardziej destrukcyjne i mniej przewidywalne niż w przypadku sprawców kierujących się wyłącznie zyskiem.

[18] A. Kamińska M. Popiało J. Zaryczna (red.), *Strach – narzędzie przemocy w rękach terrorystów,* , Szczytno 2017, s. 43-77.
[19] Sposób dostarczania zasobów IT przez Internet w modelu subskrypcyjnym (pay-as-you-go), eliminujący potrzebę zakupu, instalacji i utrzymania własnej infrastruktury czy oprogramowania.
[20] Wyróżnione cechy cyberwilka wywodzą się na podstawie opracowań samotnych wilków, typologia działań wykorzystywanych przez oba zjawiska posiada wiele wspólnych cech, elementem wyróżniającym je pomiędzy sobą jest obszar działania, jedni działają w sferze fizycznej, drudzy w sferze cybernetycznej.

Równocześnie należy podkreślić, że cyberwilk nie jest „tylko hakerem" ani „tylko terrorystą". Jest podmiotem łączącym obie te tożsamości w sposób komplementarny. W tym miejscu można śmiało postawić tezę, że terrorysta wykorzystujący cyberprzestrzeń nie przestaje być terrorystą, podobnie jak haker działający z motywacji politycznej nie przestaje być hakerem.

Jednym z kluczowych aspektów zjawiska cyberterrorystów jest proces radykalizacji, który w ich przypadku przebiega w całości lub w przeważającej części w środowisku internetowym. Internet odgrywa kluczową rolę w przypadku samotnych wilków, umożliwiając łatwy dostęp do propagandy ekstremistycznej oraz komunikację z innymi radykałami bez konieczności fizycznego kontaktu.[21]

Wraz z rozwojem sztucznej inteligencji proces radykalizacji ulega dalszemu przyspieszeniu. Generatywne modele językowe mogą być wykorzystywane do tworzenia przekonującej propagandy, a zaawansowane algorytmy rekomendacyjne platform społecznościowych mogą prowadzić do tzw. „lejka radykalizacji"[22] (radicalization funnel), gdzie to użytkownicy stopniowo kierowani są ku coraz bardziej ekstremistycznym treściom.

Istotną rolę w procesie radykalizacji i przygotowania działań przez cyberwilki odgrywają ukryte zasoby Internetu – darknet oraz deep web. Nieindeksowane zasoby sieci stanowią istotne wyzwanie dla bezpieczeństwa cyfrowego, umożliwiając anonimową komunikację, dostęp do nielegalnych treści oraz handel narzędziami hakerskimi[23].

W szczególności darknet umożliwia cyberwilkom:

- anonimowe pozyskiwanie zaawansowanych narzędzi hakerskich (w tym złośliwego oprogramowania, exploitów, usług DDoS);
- komunikację bez ryzyka ujawnienia tożsamości;
- dostęp do forów, na których dzielono się wiedzą i doświadczeniami z zakresu cyberataków;
- pozyskiwanie materiałów instruktażowych dotyczących metod ataku na infrastrukturę krytyczną.

Jednym z najbardziej niebezpiecznych wymiarów działalności cyberterrorystów są ataki skierowane przeciwko infrastrukturze krytycznej. Jak wskazuje analiza przypadku ataku na system uzdatniania wody w Oldsmar na Florydzie (2021), pojedynczy sprawca dysponujący dostępem wewnętrznym był w stanie próbować doprowadzić do skażenia wody pitnej, co stanowiłoby zagrożenie dla tysięcy mieszkańców[24].

Cyberwilki coraz częściej sięgają także po ataki typu ransomware oraz DDoS. W odróżnieniu od zorganizowanych grup przestępczych, dla których ataki te stanowią źródło dochodu

[21] K. Karolczak, *Terroryzm XXI wieku – wybrane aspekty,* „Terroryzm - studia, analizy, prewencja" 2022, 1, s. 20-25.
[22] Model opisujący proces, w którym jednostka stopniowo przyjmuje coraz bardziej skrajne poglądy, często prowadzący do akceptacji przemocy lub zaangażowania w terroryzm. Jest to trajektoria, w której osoba przechodzi od poglądów umiarkowanych do ekstremistycznych, często pod wpływem ideologii, czynników społecznych lub psychologicznych.
[23] A.K. Olech, A. Lis, *Technologia i terroryzm: sztuczna inteligencja w dobie zagrożeń terrorystycznych,* Warszawa 2021, s. 76-78.
[24] *Precursor Analysis Report: Remote Access Attack On Oldsmar Water Treatment Facility 2021,* Idaho 2021.

wykorzystują je jako narzędzie realizacji celów terrorystycznych, maksymalizacji szkody, wywołania chaosu, zastraszenia społeczności[25].

Wartym poruszenia aspektem działań jest sabotaż informacyjny, działania ukierunkowane na manipulację informacją, wywołanie niepokoju społecznego oraz podważenie zaufania do instytucji publicznych. W tej kategorii mieszczą się m.in. wycieki danych (doxing), tworzenie i rozpowszechnianie deepfake'ów, a także kampanie dezinformacyjne prowadzone w mediach społecznościowych[26].

Przeprowadzona analiza literatury przedmiotu pokazuje, że cyberterroryści stanowią autonomiczną kategorię we współczesnej typologii terroryzmu. Nie są oni jedynie „hakerami o terrorystycznych poglądach" ani „terrorystami posługującymi się komputerami" – są nową jakością sprawczą, wymagającą odrębnego ujęcia definicyjnego i analitycznego.

W porównaniu z klasycznymi samotnymi wilkami, cyberwilki wyróżniają się:

- środowiskiem działania – cyberprzestrzeń, a nie przestrzeń fizyczna;
- narzędziami – kod, złośliwe oprogramowanie, inżynieria społeczna zamiast broni palnej czy materiałów wybuchowych;
- zasięgiem – globalnym, a nie lokalnym;
- poziomem anonimowości ;
- progiem psychologicznym – niższym ze względu na dystans wynikający
- z działania za pośrednictwem kodu.

W porównaniu z zorganizowanymi grupami terrorystycznymi cyberwilki charakteryzują się:

- brakiem struktury – działają samodzielnie, bez sieci wsparcia;
- nieprzewidywalnością – brak mechanizmów kontroli wewnętrznej, które ograniczają zakres działań w grupach;
- motywacją – często silnie zindywidualizowaną, o charakterze emocjonalnym lub psychopatologicznym;
- potencjałem destrukcyjnym – mogącym przewyższać możliwości grup ze względu na brak ograniczeń.

ROZWÓJ CYBERTERRORYZMU – IMPLIKACJE DLA BEZPIECZEŃSTWA PAŃSTW I SYSTEMÓW TELEINFORMATYCZNYCH

Przeprowadzona powyższa charakterystyka zjawiska jako autonomicznej kategorii sprawców terroryzmu asymetrycznego wymaga obecnie osadzenia w szerszym kontekście ewolucji samego cyberterroryzmu. Współczesne zagrożenia w cyberprzestrzeni charakteryzują się nie tylko rosnącą skalą, ale przede wszystkim jakościową zmianą natury ataków oraz podmiotów je przeprowadzających.

[25] M. Sienicki, *Cyberterroryzm – charakterystyka zjawiska*, „Kwartalnik Bellona" 2024, 716(1), s. 51-53.
[26] *Ibidem*, s. 53-54.

Przełom w postrzeganiu cyberterroryzmu nastąpił wraz z serią głośnych ataków na infrastrukturę krytyczną w drugiej dekadzie XXI wieku. Ataki na ukraińską sieć elektroenergetyczną (2015, 2016), wykorzystanie ransomware NotPetya[27] (2017), powodujące straty liczone w miliardach dolarów, czy wreszcie eskalacja cyberataków związana z agresją Rosji na Ukrainę – wszystkie te wydarzenia sprawiły, że cyberterroryzm przestał być abstrakcją, stając się codziennym wyzwaniem dla służb odpowiedzialnych za bezpieczeństwo państw[28].

Istotnym kontekstem dla zrozumienia rozwoju cyberterroryzmu są procesy określane mianem czwartej rewolucji przemysłowej (Industry 4.0). Upowszechnienie się technologii takich jak Internet Rzeczy (IoT), Sztuczna Inteligencja, chmura obliczeniowa czy systemy cyberfizyczne radykalnie podniosło skalę ataków dostępną dla potencjalnych sprawców. Każde nowe urządzenie podłączone do sieci, każdy czujnik w systemie infrastruktury krytycznej, każda chmura danych stanowi potencjalny cel lub wektor ataku[29].

Szczególnie istotne w kontekście omawianego zjawiska są tzw. systemy cyberfizyczne (CPS)[30], w których komponenty obliczeniowe integrują się z procesami fizycznymi. Atak na tego rodzaju systemy może mieć konsekwencje wykraczające daleko poza sferę wirtualną – może prowadzić do realnych uszkodzeń fizycznych, zagrożenia życia i zdrowia ludzi oraz paraliżu kluczowych sektorów gospodarczych. W przypadku cyberwilków, z definicji nie podlegających wewnętrznym mechanizmom ograniczającym, potencjał destrukcyjny ataków na systemy cyberfizyczne jest szczególnie wysoki.

Równocześnie jednak czwarta rewolucja przemysłowa dostarcza narzędzi do przeciwdziałania cyberterroryzmowi. Zaawansowane systemy detekcji oparte na uczeniu maszynowym, zdecentralizowane mechanizmy weryfikacji transakcji (blockchain) czy zaawansowane metody szyfrowania mogą stanowić skuteczną barierę przed atakami. Kluczowe wyzwanie polega na tym, że tempo rozwoju technologii obronnych często nie nadąża za tempem rozwoju technologii ofensywnych, a asymetria między potencjałem sprawcy a ofiary pozostaje znacząca[31].

Z kolei wojna w Ukrainie, jak wskazują uczestnicy konferencji poświęconej cyberodporności w epoce wojny hybrydowej, zorganizowanej w maju 2025 roku przez think tank Europa we współpracy z NATO unaoczniła, że cyberprzestrzeń stała się pełnoprawnym polem walki. W 2024 roku rosyjskie cyberataki na Ukrainę wzrosły o prawie 70%, przekraczając 4000 incydentów wymierzonych w infrastrukturę krytyczną od usług rządowych po sektor energetyczny

[27] Ransomware w nowej odsłonie, https://www.gov.pl/web/rcb/ransomware-w-nowej-odslonie (05.04.2026).
[28] *UKRAINA 2022: Na cyfrowym froncie*, Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, https://www.wojsko-polskie.pl/woc/u/4c/d1/4cd11eaf-3567-405d-994f-f88b6b45ad0b/ukraina_2022_na_cyfrowym_froncie.pdf, s. 5-19.
[29] Li Da Xu, Eric L. Xu, Ling Li, *Industry 4.0: state of the art and future trends*, „International Journal of Production Research" 2018, 56(8), s. 2943-2959.
[30] Zaawansowane sieci integrujące procesy fizyczne (maszyny, czujniki) z obliczeniami cyfrowymi (oprogramowanie, algorytmy) w czasie rzeczywistym.
[31] Li Da Xu, Eric L. Xu, Ling Li, *Industry 4.0…, op. cit.,* s. 32-40.

i obronny. Równocześnie obserwowano ataki na państwa sojusznicze, w tym trzykrotny wzrost liczby cyberataków w Wielkiej Brytanii oraz ataki na włoskie strony rządowe[32].

W kontekście omawianego tematu szczególnie istotne jest zjawisko, określane mianem „hacktywizmu inspirowanego konfliktem". Po inwazji na Ukrainę odnotowano znaczący wzrost aktywności pojedynczych sprawców, działających po stronie obu antagonistów, często bez formalnych powiązań z którąkolwiek ze stron podejmowali działania cybernetyczne o charakterze sabotażowym lub informacyjnym. Zjawisko to doskonale ilustruje tezę o komplementarności tożsamości terrorysty i hakera[33].

Zauważalnym zjawiskiem są popularne teraz kryptowaluty umożliwiające anonimowe transfery wartości, co ma kluczowe znaczenie zarówno dla grup terrorystycznych poszukujących źródeł finansowania, jak i dla cyberprzestępców żądających okupów w ramach ataków ransomware. Blockchain, choć z założenia przejrzysty, w praktyce przy użyciu technologii miksowania (tumblerów) pozwala na skuteczne zacieranie śladów transakcji[34].

Po drugie, darknet jest bezkresną przestrzenią, gdzie cyberprzestępcy i terroryści mogą dokonywać wymiany wiedzy, narzędzi i usług bez obawy przed ujawnieniem. Tego samego dotyczy obszar mediów społecznościowych i szyfrowanych komunikatorów, stały się one areną dla cyberprzestępców, terrorystów i hacktywistów prowadzących wymianę technik hakerskich, propagandy, rekrutacji oraz koordynacji działań.

Jednym z fundamentalnych wyzwań stojących przed państwami w zakresie przeciwdziałania cyberterroryzmowi jest problem definicyjny. Jak wynika z badań, pojęcia „cyberterroryzm" i „hacktywizm" są przedmiotem sporów w literaturze przedmiotu, a ich nieostrość prowadzi do trudności w klasyfikacji poszczególnych zdarzeń oraz w doborze odpowiednich środków reakcji. W szczególności w przypadku działających samodzielnie cyberwilków, często z mieszanymi motywacjami, kwalifikacja prawna ich działań jako aktów terrorystycznych bywa problematyczna, mimo że skutki społeczne tych działań mogą być tożsame z klasycznymi zamachami terrorystycznymi.

Najważniejszym problemem jest niedobór wykwalifikowanych specjalistów. Walka z cyberterroryzmem wymaga zaawansowanych kompetencji technicznych, natomiast są one deficytowe na rynku pracy. Państwa konkurują ze sobą oraz z sektorem prywatnym o specjalistów ds. cyberbezpieczeństwa, a luka kompetencyjna w tej dziedzinie stale się powiększa[35].

W tradycyjnych modelach bezpieczeństwa odpowiedzialność za przeciwdziałanie terroryzmowi spoczywa na państwie, podczas gdy ochrona przed cyberprzestępczością wymaga ścisłej współpracy

[32] Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni gospodarzem kluczowej konferencji NATO poświęconej cyberbezpieczeństwu, https://www.wojsko-polskie.pl/articles/tym-zyjemy-v/2025-05-23y-dowodztwo-komponentu-wojsk-obrony-cyberprzestrzeni-gospodarzem-kluczowej-konferencji-nato-poswieconej-cyberbezpieczenstwu/ (06.04.2026).

[33] P. Krapp, *Terror and Play, or What was Hacktivism?*, „Grey Room" 2015, 21, s. 72-79.

[34] *Miksery kryptowalut. Na czym polega miksowanie krypto?*, https://gieldomania.pl/miksery-kryptowalut/ (05.04.2026).

[35] *Brakuje pracowników w sektorze cyberbezpieczeństwa*, Cyberdefence24, https://cyberdefence24.pl/brakuje-pracownikow-w-sektorze-cyberbezpieczenstwa-2 (06.04.2026).

z sektorem prywatnym (dostawcami usług internetowych, operatorami infrastruktury krytycznej, firmami cyberbezpieczeństwa). W przypadku cyberterroryzmu granice między tymi obszarami odpowiedzialności ulegają zatarciu, co prowadzi do luk kompetencyjnych i odpowiedzialnościowych. Zarówno państwa, jak i podmioty prywatne są często niechętne do udostępniania informacji o incydentach cybernetycznych ze względu na obawy o poufność, bezpieczeństwo lub reputację, co znacząco podnosi problematyczność zagadnienia.

W kontekście cyberwilków szczególnie niepokojący jest fakt, że SI obniża próg wejścia do aktywności cyberterrorystycznej. Osoba z podstawowymi kompetencjami technicznymi, wspomaganymi przez generatywne modele językowe może dziś wygenerować kod złośliwego oprogramowania, napisać przekonujący phishingowy e-mail czy stworzyć wykorzystanego do dezinformacji deepfake'a. Równocześnie rozwój SI stwarza nowe możliwości dla systemów obronnych. Zaawansowane modele uczenia maszynowego mogą być wykorzystywane do przewidywania ataków, automatycznej detekcji anomalii czy wspomagania procesów asymilacji, kluczowe wyzwanie polega na tym, że tempo rozwoju technologii ofensywnych często przewyższa tempo rozwoju technologii defensywnych, a asymetria między potencjałem sprawcy i ofiary pozostaje znacząca.

W odpowiedzi na zidentyfikowane wyzwania w literaturze przedmiotu oraz w dokumentach strategicznych warto skupić się na istotnych celach możliwości przeciwdziałania bądź postawienia pewnego drogowskazu, skupiającego dotychczasowe i przyszłe formy walki z cyberterroryzmem. Można je podzielić na kilka kategorii, czyli:

- konieczność wypracowania jasnych ram odpowiedzialności, kluczowe jest tu określenie, kto odpowiada za zarządzanie zagrożeniami hybrydowymi – w tym cyberterroryzmem – oraz jakie są procedury koordynacji między różnymi podmiotami;
- potrzeba zwiększenia odporności infrastruktury krytycznej, opracowanie planów ciągłości działania, regularne ćwiczenia symulujące ataki oraz tworzenie rezerwowych systemów, które mogą przejąć funkcje systemów głównych w przypadku ich sparaliżowania;
- konieczność inwestycji w kapitał ludzki, programy edukacyjne i szkoleniowe w zakresie cyberbezpieczeństwa, zarówno na poziomie akademickim (kształcenie specjalistów), jak i na poziomie powszechnym (podnoszenie świadomości użytkowników). Niedobór wykwalifikowanych specjalistów jest jednym z kluczowych wąskich gardeł w systemie bezpieczeństwa;
- w aspekcie technicznym i operacyjnym wdrożenie zaawansowanych systemów detekcji i monitorowania opartych na uczeniu maszynowym oraz analizie behawioralnej. Tradycyjne systemy oparte na sygnaturach są niewystarczające wobec nowych, nieznanych wcześniej zagrożeń, a zwłaszcza wobec działań cyberwilków, często nie pozostawiają charakterystycznych artefaktów znanych z ataków zorganizowanych grup;
- w wymiarze międzynarodowym, wzmocnienie mechanizmów współpracy w ramach istniejących organizacji (ONZ, NATO, UE, BRICS) oraz wypracowanie nowych ram współpracy adekwatnych do wyzwań stawianych przez cyberterroryzm, państwa powinny wspierać ONZ w odgrywaniu centralnej roli w zarządzaniu cyberprzestrzenią oraz

promować wdrażanie Globalnej Strategii Antyterrorystycznej ONZ (przyjmując założenie ponadpaństwowe, podmioty na arenie międzynarodowej powinny skupiać się na zwiększeniu uczestników zwalczających cyberterroryzm ze względu na baraku szablonu działań, dotyczących całego świata, dlatego właśnie im więcej podmiotów skupionych jest w ramach organizacji międzynarodowej, tym większe jest prawdopodobieństwo zminimalizowania wystąpienia zagrożeń cyberterrorystów lub ich skutków).

PODSUMOWANIE

Przedmiotem niniejszego artykułu była analiza zjawiska cyberwilków jako autonomicznej kategorii podmiotów terroryzmu asymetrycznego. W odróżnieniu od zorganizowanych grup terrorystycznych oraz klasycznych hakerów działających dla zysku, cyberterroryści łączą w sobie cechy terrorysty, motywację polityczną, społeczną lub psychopatologiczną oraz cel w postaci zastraszenia i destabilizacji z cechami hakera, tj. wykorzystaniem narzędzi hakerskich i działaniem w środowisku cyfrowym. Przeprowadzona analiza potwierdza postawioną hipotezę, że obie te tożsamości pozostają względem siebie w relacji zbieżnej, a nie wykluczającej.

W ramach badań wyodrębniono trzy główne kategorie cyberwilków: ideologicznych (hacktywiści), motywowanych osobistą zemstą oraz motywowanych psychopatologicznie. Każda z tych kategorii charakteryzuje się odmiennymi motywacjami, metodami działania oraz potencjałem destrukcyjnym. Wspólnym mianownikiem jest działanie samodzielne, poza strukturami organizacyjnymi, co czyni ich szczególnie trudnymi do wykrycia i przewidzenia.

Systemy bezpieczeństwa państw mierzą się obecnie z szeregiem wyzwań w zakresie przeciwdziałania cyberterroryzmowi od problemów definicyjnych i prawnych, przez trudności natury technicznej (atrybucja, podatność infrastruktury krytycznej, niedobór specjalistów), po wyzwania instytucjonalne i związane z rozwojem Sztucznej Inteligencji. Skuteczna odpowiedź na te wyzwania wymaga kompleksowego podejścia łączącego działania strategiczne, techniczne oraz międzynarodowe, ze szczególnym uwzględnieniem wzmacniania odporności infrastruktury krytycznej, rozwoju zaawansowanych systemów detekcji oraz pogłębiania współpracy publiczno-prywatnej.

Cyberwilki stanowią nową i dynamicznie rozwijającą się gałąź terroryzmu internetowego. Ich znaczenie w środowisku bezpieczeństwa będzie prawdopodobnie rosło, co czyni koniecznym dalsze pogłębione badania nad tym zjawiskiem, w szczególności w zakresie empirycznej weryfikacji typologii sprawców oraz wpływu rozwoju Sztucznej Inteligencji na ewolucję ich metod działania.

BIBLIOGRAFIA

Aleksandrowicz Tomasz. 2010. „Rok 1968 – początek terroryzmu?". Rocznik Polsko-Niemiecki 10(23): 11-23.

Białoskórski Robert. 2011. Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki. Warszawa: Wydawnictwo WSCIL.

Cyberdefence24. 2016. Brakuje pracowników w sektorze cyberbezpieczeństwa. W https://cyberdefence24.pl/brakuje-pracownikow-w-sektorze-cyberbezpieczenstwa-2

Cybersecurity for the Operational Technology Environment (CyOTE). 2022. Precursor Analysis Report: Remote Access Attack On Oldsmar Water Treatment Facility 2021. W ttps://cyote.inl.gov/content/uploads/24/2025/12/CyOTE-Case-Study_Oldsmar.pdf

Czarnota Nikola. 2020. „Rola Agencji Bezpieczeństwa Wewnętrznego i Policji w zwalczaniu cyberterroryzmu". Studia Bezpieczeństwa Narodowego 10(18): 111-120.

Czerniak Martyna. 2024. „Zamachy w Oslo i na wyspie Utøya w 2011 roku: analiza wydarzeń, reakcji służb i wniosków dla zarządzania kryzysowego". Studia de Securitate 14(2): 250-263.

Da Xu Li. Xu Eric L. Xu. Li Ling. 2018. „Industry 4.0: state of the art and future trends". International Journal of Production Research 56(8): 2941-2962.

Definicje terroryzmu. b.d. W https://www.unic.un.org.pl/terroryzm/definicje.php.

Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni. 2022. UKRAINA 2022: Na cyfrowym froncie. W https://www.wojsko-polskie.pl/woc/u/4c/d1/4cd11eaf-3567-405d-994f-f88b6b45ad0b/ukraina_2022_na_cyfrowym_froncie.pdf.

Federal Bureau of Investigation. b.d. „Timothy McVeigh". FBI Vault. W https://vault.fbi.gov/timothy-j.-mcveigh.

Frąckowiak Kamil. 2022. „Asymetryczne zagrożenia w cyberprzestrzeni a ewolucja terroryzmu indywidualnego". Biuletyn Bezpieczeństwa Narodowego 4: 88-105.

Frontline. 2016. Lone Wolf Attacks Are Becoming More Common – And More Deadly. W https://www.pbs.org/wgbh/frontline/article/lone-wolf-attacks-are-becoming-more-common-and-more-deadly/

GiedłoMania. 2026. Miksery kryptowalut. Na czym polega miksowanie krypto? W https://gieldomania.pl/miksery-kryptowalut/.

Gołda-Sobczak Maria. Sobczak Witold. 2018. „Problem definicji terroryzmu". Themis Polska Nova 2(14): 92-119.

Hołyst Brunon. 2019. Terroryzm w świecie współczesnym. Warszawa: Wydawnictwo Naukowe PWN.

Jagusiak Bogusław. 2011. „Wpływ zagrożeń terrorystycznych na bezpieczeństwo międzynarodowe". Studia Bezpieczeństwa Narodowego 2(2): 265–293.

Kamińska Agnieszka. Popiało Małgorzata. Zaryczna Justyna (red.). 2017. Strach – narzędzie przemocy w rękach terrorystów. Szczytno: Wydawnictwo Wyższa Szkoła Policji w Szczytnie.

Karolczak Krzysztof. 2022. „Terroryzm XXI wieku – wybrane aspekty". Terroryzm – studia, analizy, prewencja 1: 9-28.

Kołodziejczyk Rafał. 2017. „Nowa odsłona terroryzmu". Rocznik Bezpieczeństwa Międzynarodowego 11(2): 147-155.

Krapp Peter. 2015. „Terror and Play, or What was Hacktivism?". Grey Room 21: 70–93.

Kucharek Daniel. 2023. „Model typowania sprawców zamachów z wykorzystaniem bojowych środków chemicznych". Przegląd Geopolityczny 44: 101-115.
Nowacki Gabriel. 2014. „Zjawisko terroryzmu w XXI wieku". Studia Bezpieczeństwa Narodowego 4(5): 403-441.
Olech Aleksander. Lis Alan. 2021. Technologia i terroryzm: sztuczna inteligencja w dobie zagrożeń terrorystycznych. W https://ine.org.pl/wp-content/uploads/2021/01/Technologia-i-terroryzm-sztuczna-inteligencja-w-dobie-zagrozen-terrorystycznych-1.pdf
Oleksiewicz Izabela. 2018. „Cyberterroryzm jako realne zagrożenie dla polski". Rocznik Bezpieczeństwa Międzynarodowego 12(1): 53-67.
Piątek Jarosław. 2019. "Długa wojna z terroryzmem". Rocznik Bezpieczeństwa Międzynarodowego 2: 51-63.
Radkiewicz Oliwia. 2021. „Terroryzm "samotnych wilków" na wybranych przykładach". SDirect24 Scientific Journal 1: 64-78.
Rządowe Centrum Bezpieczeństwa. b.d. Ransomware w nowej odsłonie. W https://www.gov.pl/web/rcb/ransomware-w-nowej-odslonie.
Sienicki Marcin. 2024. „Cyberterroryzm – charakterystyka zjawiska". Kwartalnik Bellona 716(1): 49-58.
Simon Jeffrey. 2013. What make lone-wolf terrorists so dangerous? W https://newsroom.ucla.edu/stories/what-makes-lonewolfe-terrorists-245316.
Smarzewski Marek. 2017. „Cyberterroryzm a cyberprzestępstwa o charakterze terrorystycznym". Ius Novum 11(1): 64-75.
Ustawa z dnia 6 czerwca 1997 r., Kodeks karny, Dz. U. 1997 Nr 88 poz. 553, art. 115 §20.
Wojsko-polskie.pl. 2025. Dowództwo Komponentyu Wojsk Obrony /cyberprzestrzeni gospodarzem kluczowej konferencji NATO poświęconej cyberbezpieczeńswu. W https://www.wojsko-polskie.pl/articles/tym-zyjemy-v/2025-05-23y-dowodztwo-komponentu-wojsk-obrony-cyberprzestrzeni-gospodarzem-kluczowej-konferencji-nato-poswieconej-cyberbezpieczenstwu/.
Zubrzycki Waldemar. Suchanek Paweł. 2014. „Bezpieczeństwo Rzeczypospolitej Polskiej w kontekście zagrożeń terrorystycznych". Studia Politologiczne 34: 153-165.