Patryk Ochyra[1]

Menadżerska Akademia Nauk Stosowanych w Warszawie

Mariusz Kubisz[2]

Wojskowa Akademia Techniczna w Warszawie

Bartosz Tarnowski[3]

Politechnika Gdańska

https://doi.org/10.29316/9788368103359_9

CYBERTERRORYZM JAKO WYZWANIE DLA BEZPIECZEŃSTWA PAŃSTWA – EWOLUCJA FORM, STRUKTUR ORGANIZACYJNYCH I IMPLIKACJE DLA POLSKI

CYBERTERRORISM AS A CHALLENGE TO NATIONAL SECURITY – THE EVOLUTION OF FORMS AND ORGANIZATIONAL STRUCTURES, AND IMPLICATIONS FOR POLAND

[1] https://orcid.org/0000-0001-8991-4068, e-mail: patryk.ochyra@op.pl

[2] https://orcid.org/0009-0003-7901-4690, e-mail: mariusz.kubisz@gmail.com

[3] https://orcid.org/0009-0000-0597-6684, e-mail: Bartosz.tarnowski@protonmail.ch

Streszczenie

Celem rozdziału jest analiza cyberterroryzmu jako współczesnego zagrożenia dla bezpieczeństwa państwa, ze szczególnym uwzględnieniem ewolucji form działalności terrorystycznej, zmian w strukturach organizacyjnych ugrupowań oraz implikacji tych procesów dla bezpieczeństwa Polski. Problem badawczy sformułowano: w jaki sposób rozwój cyberprzestrzeni wpływa na ewolucję terroryzmu oraz jakie zagrożenia cyberterroryzm stanowi dla bezpieczeństwa Polski? Przyjęto hipotezę, że cyberterroryzm stanowi realne i rosnące zagrożenie dla bezpieczeństwa państwa, ponieważ umożliwia destabilizację funkcjonowania kluczowych systemów, wywieranie presji politycznej oraz oddziaływanie psychologiczne na społeczeństwo przy relatywnie niskich kosztach i wysokiej anonimowości sprawców. W rozdziale zastosowano metody badawcze właściwe dla nauk o bezpieczeństwie, w szczególności analizę literatury przedmiotu, analizę danych empirycznych dotyczących incydentów cyberbezpieczeństwa oraz metodę analizy porównawczej i systemowej, pozwalające na identyfikację mechanizmów funkcjonowania współczesnych organizacji terrorystycznych oraz ocenę podatności państwa na zagrożenia w cyberprzestrzeni. Główny wniosek wskazuje, że cyberterroryzm stanowi jeden z istotnych elementów współczesnych zagrożeń hybrydowych, a skuteczne przeciwdziałanie temu zjawisku wymaga kompleksowego podejścia obejmującego rozwój zabezpieczeń technicznych, wzmacnianie odporności instytucjonalnej i informacyjnej oraz podnoszenie świadomości społecznej w zakresie bezpieczeństwa cyfrowego.

Słowa kluczowe: cyberterroryzm, bezpieczeństwo państwa, terroryzm, cyberbezpieczeństwo, zagrożenia hybrydowe

Abstract

The aim of the chapter is to analyze cyberterrorism as a contemporary threat to the security of the state, with particular emphasis on the evolution of forms of terrorist activity, changes in the organizational structures of groups and the implications of these processes for the security of Polish. The research problem was formulated: how does the development of cyberspace affect the evolution of terrorism and what threats does cyberterrorism pose to the security of Polish? It has been hypothesized that cyberterrorism poses a real and growing threat to the security of the state, as it allows for destabilization of the functioning of key systems, exerting political pressure and psychological impact on society at relatively low costs and high anonymity of perpetrators. The chapter uses research methods specific to security sciences, in particular the analysis of the literature on the subject, the analysis of empirical data

on cybersecurity incidents and the method of comparative and systemic analysis, allowing for the identification of the mechanisms of functioning of modern terrorist organizations and the assessment of the state's vulnerability to threats in cyberspace. The main conclusion points out that cyberterrorism is one of the important elements of today's hybrid threats, and effectively countering this phenomenon requires a comprehensive approach including the development of technical safeguards, strengthening institutional and information resilience and raising public awareness of digital security.

Keywords: cyberterrorism, state security, terrorism, cybersecurity, hybrid threats

Wstęp

Współczesne środowisko bezpieczeństwa państwa podlega dynamicznym i wielowymiarowym przemianom, wynikającym m.in. z postępu technologicznego, globalizacji oraz rozwoju cyberprzestrzeni. Jednym z kluczowych wyzwań XXI wieku pozostaje terroryzm, który ewoluuje zarówno pod względem form działania, jak i struktur organizacyjnych. Obok klasycznych metod przemocy coraz większe znaczenie zyskują działania prowadzone w cyberprzestrzeni, określane mianem cyberterroryzmu. Zjawisko to, choć rzadko prowadzi do bezpośrednich ofiar w ludziach, może powodować poważne zakłócenia funkcjonowania państwa, destabilizację społeczną oraz osłabienie zaufania obywateli do instytucji publicznych.

Celem niniejszego rozdziału jest analiza cyberterroryzmu jako współczesnego zagrożenia dla bezpieczeństwa państwa, ze szczególnym uwzględnieniem jego organizacyjnych uwarunkowań oraz implikacji dla Polski. Autor koncentruje się na ukazaniu ewolucji terroryzmu od form tradycyjnych do działań hybrydowych, łączących przemoc fizyczną z oddziaływaniem cyfrowym i informacyjnym. Praca podejmuje również próbę oceny skali i charakteru zagrożenia cyberterrorystycznego w polskiej cyberprzestrzeni, wskazując na kluczowe obszary podatności oraz wyzwania stojące przed systemem bezpieczeństwa państwa.

Istota i formy współczesnego terroryzmu

Współczesny terroryzm stanowi jedno z najpoważniejszych i najbardziej złożonych zagrożeń dla bezpieczeństwa państw oraz społeczności międzynarodowej. Jego istotą pozostaje stosowanie przemocy lub groźby jej użycia wobec ludności cywilnej, instytucji państwowych bądź infrastruktury krytycznej w celu osiągnięcia określonych celów politycznych, ideologicznych, religijnych lub ekonomicznych. Charakterystycznym elementem działań terrorystycznych jest instrumentalne traktowanie ofiar, które nie są celem samym w sobie, lecz środkiem do wywołania określonego efektu psychologicznego i społecznego (Hoffman, 2017).

Klasyczne formy terroryzmu obejmują zamachy bombowe, zabójstwa, porwania, wzięcia zakładników, podpalenia oraz ataki z użyciem broni chemicznej lub biologicznej. Działania te mają na celu wywołanie strachu, destabilizacji oraz poczucia bezradności wśród obywateli, co w konsekwencji prowadzi do osłabienia zaufania do instytucji państwowych (Piątkowski, 1996). Strach staje się w tym ujęciu podstawowym narzędziem walki, oddziałującym nie tylko na bezpośrednie ofiary, lecz również na szerokie grono odbiorców za pośrednictwem mediów tradycyjnych i cyfrowych.

Współczesne ugrupowania terrorystyczne dowodzą, że do osiągnięcia znaczących efektów destabilizacyjnych nie są konieczne zaawansowane technologicznie środki ani rozbudowane struktury organizacyjne. Niewielkie grupy, a nawet pojedynczy sprawcy działający w ramach tzw. terroryzmu indywidualnego, są w stanie wywołać poważne skutki polityczne i społeczne. Zjawisko to nabrało szczególnego znaczenia w dwudziestym pierwszym wieku wraz z rozwojem Internetu i mediów społecznościowych, które ułatwiają proces radykalizacji, rekrutacji oraz rozpowszechniania propagandy ekstremistycznej.

Podział rozległego zjawiska jakim jest terroryzm nie jest jednolity, a każdy podejmujący się tego zadania autor przyjmuje własną koncepcję (Europol, 2023). W literaturze przedmiotu najczęściej wyróżnia się trzy główne nurty terroryzmu: polityczny, religijny i kryminalny (Superczyńska, 2019).

Terroryzm polityczny stanowi formę walki prowadzonej przez podmioty słabsze wobec silniejszych struktur państwowych. Jego celem jest wywarcie presji na władze poprzez akty przemocy lub groźby ich użycia. Terroryści polityczni dążą do zwrócenia uwagi opinii publicznej na postulowane

przez siebie problemy, destabilizacji porządku konstytucyjnego państwa lub pogłębienia istniejących antagonizmów społecznych i narodowościowych. Akt przemocy ma często charakter symboliczny i służy zapoczątkowaniu procesu eskalacji konfliktu.

Szczególną odmianą terroryzmu jest terroryzm religijny, który w ostatnich dekadach zyskał na znaczeniu. Opiera się on na fundamentalistycznej interpretacji doktryn religijnych, w ramach której przemoc uznawana jest za moralnie usprawiedliwioną, a niekiedy wręcz nakazaną. Przekonanie o działaniu w imię sił nadprzyrodzonych prowadzi do zniesienia tradycyjnych ograniczeń etycznych i sprzyja eskalacji brutalności, w tym gotowości do poświęcenia własnego życia (Hoffman, 2017).

Terroryzm kryminalny stanowi zjawisko pograniczne, w którym metody charakterystyczne dla działań terrorystycznych wykorzystywane są w celu osiągnięcia korzyści materialnych. Zorganizowane grupy przestępcze sięgają po zamachy, porwania czy zastraszanie, co prowadzi do przenikania się motywacji kryminalnych i politycznych. Zjawisko to obserwowane jest szczególnie w regionach dotkniętych słabością instytucji państwowych oraz wysokim poziomem korupcji (Wałek, 2018).

Inny podział omawianego zjawiska wskazuje na terroryzm międzynarodowy i lokalny. Terroryzmem międzynarodowym określamy działania skierowane przeciwko różnym krajom i rządom na całym świecie. Ta forma dotyczy takich sytuacji, gdy terroryści stacjonują, planują i realizują zamach na obcym terytorium. Stanowi ona potencjalnie większe zagrożenie w stosunkach międzynarodowych, oddziałując na obywateli różnych państw (Wałek, 2018). Terroryzm lokalny koncentruje swoje działania na walce z miejscowym rządem i ograniczając się do działalności na terenie danego kraju nie przekracza jego granic. Taka działalność ma głównie na celu zastraszenie lub usunięcie osób, które są postrzegane jako wróg publiczny lub działają wbrew woli ludności. Często wrogami terrorystów są inni terroryści lub niewygodne grupy etniczne stwarzające zagrożenie na własnym terytorium. Ten rodzaj terroryzmu zmierza do zastraszenia społeczeństwa, poprzez realizowanie ataków na cele przypadkowe i newralgiczne. Celem takich działań nie jest w przeciwieństwie do terroryzmu międzynarodowego uzyskanie rozgłosu, a jeśli nawet to nie w celu nagłośnienia swojej sprawy. Skupia się on na wyrażeniu niezadowolenia w postępowaniu władz danego kraju (Wałek, 2018).

Współczesne analizy wskazują również na rosnące znaczenie nowych form zagrożeń, takich jak cyberterroryzm. Cyberterroryzm obejmuje działania wymierzone w systemy teleinformatyczne, infrastrukturę krytyczną oraz sferę informacyjną państwa. Choć ataki te rzadko powodują bezpośrednie ofiary w ludziach, mogą prowadzić do poważnych zakłóceń funkcjonowania administracji publicznej, gospodarki oraz systemów bezpieczeństwa (Europol, 2023).

Podsumowując, terroryzm pozostaje zjawiskiem dynamicznym, które nieustannie dostosowuje się do zmieniających się warunków politycznych, technologicznych i społecznych. Zrozumienie jego nurtów i form stanowi kluczowy element skutecznego przeciwdziałania temu zagrożeniu na poziomie krajowym i międzynarodowym.

Organizacja grup terrorystycznych w warunkach cyfrowych

Cyberterroryzm jest współcześnie definiowany jako forma działalności terrorystycznej wykorzystująca narzędzia teleinformatyczne do wywoływania strachu, destabilizacji oraz presji politycznej lub społecznej poprzez zakłócanie dostępności, integralności lub poufności informacji i systemów informatycznych. Obejmuje on zarówno działania techniczne, takie jak ataki typu DDoS, sabotaż systemów informacyjnych czy niszczenie danych, jak również operacje informacyjne, w tym dezinformację, propagandę ekstremistyczną oraz oddziaływanie psychologiczne prowadzone w cyberprzestrzeni. W przeciwieństwie do klasycznych form terroryzmu, celem cyberterroryzmu jest najczęściej nie fizyczna destrukcja infrastruktury, lecz wywołanie efektu społecznego i psychologicznego poprzez paraliż usług, manipulację informacją oraz podważenie zaufania do instytucji państwowych (Liszkowska, 2023).

W literaturze przedmiotu podkreśla się, że cyberterroryzm bywa niekiedy określany jako potencjalna forma „broni masowego rażenia", jednak współczesne analizy odchodzą od tego ujęcia na rzecz koncepcji „broni masowych zakłóceń" (*mass disruption*). Oznacza to, że skuteczność cyberterroryzmu nie polega na generowaniu bezpośrednich ofiar, lecz na zdolności do dezorganizacji funkcjonowania państwa i społeczeństwa, w szczególności poprzez uderzenie w systemy informacyjne, komunikacyjne oraz infrastrukturę krytyczną. Zjawisko to nabiera szczególnego znaczenia w warunkach

rosnącego uzależnienia państw i organizacji międzynarodowych, w tym struktur bezpieczeństwa zbiorowego, takich jak NATO, od niezawodnych i bezpiecznych systemów teleinformatycznych (ENISA, 2024).

Współczesne organizacje terrorystyczne funkcjonują w sposób coraz bardziej złożony, łącząc klasyczne, hierarchiczne modele organizacyjne z elastycznymi strukturami sieciowymi, charakterystycznymi dla środowiska cyfrowego. Tradycyjny model oparty na centralnym dowództwie, komórkach wywiadowczych, logistycznych i wykonawczych nadal występuje, jednak w ostatnich latach ulega on istotnej transformacji pod wpływem rozwoju cyberprzestrzeni oraz technologii informacyjnokomunikacyjnych (Hoffman, 2017).

Na najwyższym szczeblu struktury organizacyjnej znajduje się dowództwo, które odpowiada za wyznaczanie strategicznych celów, kierunków ideologicznych oraz alokację zasobów finansowych. Coraz częściej osoby pełniące funkcje decyzyjne pozostają całkowicie anonimowe, działając w przestrzeni cyfrowej z wykorzystaniem szyfrowanych kanałów komunikacji, sieci TOR oraz kryptowalut, co znacząco utrudnia ich identyfikację przez służby bezpieczeństwa (CyberDefence24, 2022).

Kluczową rolę w nowoczesnych organizacjach terrorystycznych odgrywają komórki wywiadowcze i analityczne, które obecnie funkcjonują w dużej mierze w cyberprzestrzeni. Ich zadania obejmują nie tylko klasyczne rozpoznanie potencjalnych celów, lecz także analizę danych dostępnych w otwartych źródłach, monitorowanie mediów społecznościowych oraz prowadzenie działań dezinformacyjnych. Proces werbunku coraz częściej odbywa się online, a radykalizacja potencjalnych członków następuje za pośrednictwem forów internetowych, komunikatorów i platform streamingowych (Schmid, 2021).

Grupa wsparcia logistycznego, obok tradycyjnych zadań związanych z zapewnieniem schronienia, dokumentów i środków finansowych, rozszerzyła swoje działania o obsługę zaplecza cyfrowego. Obejmuje to zarządzanie infrastrukturą informatyczną, zabezpieczanie komunikacji, obsługę portfeli kryptowalutowych oraz ukrywanie przepływów finansowych przy użyciu technologii blockchain. Cyberprzestrzeń stała się kluczowym obszarem umożliwiającym funkcjonowanie organizacji bez konieczności fizycznej obecności jej członków na danym terytorium.

Realizacja działań operacyjnych, w tym zamachów terrorystycznych, nadal pozostaje domeną grup taktycznych. Jednak także w tym obszarze widoczny jest wpływ cyberterroryzmu. Ataki fizyczne coraz częściej poprzedzane są działaniami cybernetycznymi, takimi jak zakłócanie systemów alarmowych, infrastruktury krytycznej czy systemów łączności. Cyberataki pełnią również funkcję wspomagającą, dezorganizując działania ratownicze i utrudniając reakcję służb bezpieczeństwa. Taktyka działania organizacji terrorystycznych obejmuje obecnie zarówno klasyczne metody konspiracji, jak i zaawansowane techniki cyfrowe. Minimalizacja kontaktów osobistych, wykorzystanie szyfrowanych komunikatorów, skrzynek kontaktowych w sieci, a także stosowanie dezinformacji i fałszywych tożsamości cyfrowych stanowią podstawowe elementy współczesnego modus operandi. Działania te pozwalają na prowadzenie operacji niskokosztowych, a jednocześnie o wysokim potencjale oddziaływania psychologicznego (Liszkowska, 2023).

Analiza celów ataków terrorystycznych wskazuje na cztery podstawowe grupy podmiotów narażonych na oddziaływanie terroru: instytucje rządowe, aparat bezpieczeństwa państwa, sektor gospodarczy oraz ludność cywilną. W kontekście cyberterroryzmu szczególnie istotne stają się ataki na infrastrukturę krytyczną, systemy energetyczne, telekomunikacyjne oraz finansowe, których paraliż może prowadzić do długotrwałych skutków społecznych i gospodarczych bez konieczności użycia przemocy fizycznej (Carbonelli i in., 2024).

Motywacje działalności terrorystycznej pozostają złożone i wielowymiarowe. Obejmują one czynniki ideologiczne, społecznoekonomiczne oraz psychologiczne, które wzajemnie się przenikają. W środowisku cyfrowym proces radykalizacji ulega przyspieszeniu, a izolacja społeczna, frustracja oraz narracje spiskowe sprzyjają podatności jednostek na propagandę ekstremistyczną. Cyberprzestrzeń stała się zatem nie tylko narzędziem działania, lecz także środowiskiem sprzyjającym powstawaniu nowych form terroryzmu.

Podsumowując, współczesne organizacje terrorystyczne funkcjonują jako hybrydowe struktury łączące tradycyjne formy przemocy z zaawansowanymi działaniami w cyberprzestrzeni. Rosnące znaczenie cyberterroryzmu wymusza konieczność redefinicji dotychczasowych strategii

przeciwdziałania oraz wzmocnienia zdolności państw w zakresie ochrony cyberbezpieczeństwa i przeciwdziałania radykalizacji online.

Cyberterroryzm jako zagrożenie dla Polski

Ocena zagrożenia cyberterroryzmem dla Polski powinna być osadzona w empirycznym obrazie „codziennych" incydentów cyberbezpieczeństwa. Aktualne dane z krajowego ekosystemu reagowania pokazują dynamiczny wzrost skali zdarzeń, które choć w większości mają charakter oszustw lub cyberprzestępczości tworzą środowisko sprzyjające aktorom politycznym i ekstremistycznym. W analizie bezpieczeństwa polskiego internetu za 2024 rok, przygotowanej na podstawie danych CERT Polska, wskazano m.in., że liczba zgłoszeń przekroczyła 600 tys. (wzrost o 62% rok do roku), a liczba zarejestrowanych incydentów wzrosła o 29%. Dominującą kategorią były oszustwa komputerowe 94,7% wszystkich incydentów, w tym phishing (40 120 incydentów) (Gov.pl, 2025).

Z punktu widzenia cyberterroryzmu szczególne znaczenie mają dwie kategorie: ataki na dostępność i ciągłość działania (np. DDoS, sabotaż usług) oraz zdarzenia destrukcyjne, takie jak ransomware. W 2024 r. odnotowano 147 incydentów ransomware (spadek o ok. 8% w porównaniu z 2023), przy czym ofiarami były zarówno firmy, jak i osoby prywatne oraz instytucje publiczne. Ransomware jest o tyle istotne, że może zostać wykorzystane nie tylko do wymuszeń finansowych, lecz także do celów politycznych (np. „kara" za decyzje władz), a publikowanie danych po ataku może wzmacniać efekt zastraszenia (Gov.pl, 2025).

Wzrost skali smishingu i phishingu jest ważny również dlatego, że te techniki stanowią „wejście" do bardziej zaawansowanych kampanii. Przykładowo masowe kampanie socjotechniczne mogą posłużyć do uzyskania dostępu do kont uprzywilejowanych, co w efekcie umożliwia sabotaż usług publicznych lub zakłócenie pracy instytucji. Nawet gdy motywacją większości sprawców jest zysk, infrastruktura ataku i podatności użytkowników tworzą warunki, które mogą zostać wykorzystane przez aktorów dążących do wywołania efektu „terroru" w cyberprzestrzeni (Linkedin, 2024).

Wrażliwość Polski na cyberterroryzm wynika z trzech nakładających się czynników: rosnącego uzależnienia usług publicznych i gospodarczych od systemów informatycznych, wysokiej „widoczności" Polski w środowisku

geopolitycznym i sojuszniczym, oraz zróżnicowanego poziomu dojrzałości cyberbezpieczeństwa w sektorze publicznym i prywatnym (ABW, 2024). Cyberterroryzm w wariancie „sabotagefirst" koncentruje się na zakłóceniu usług o dużej widoczności społecznej: energetyki, wodociągów, łączności, transportu i usług finansowych. Nawet krótkotrwałe przerwy w dostępności mogą generować intensywny efekt psychologiczny, szczególnie gdy towarzyszy im narracja o „bezsilności państwa". Analizy dotyczące hybrydowego wymiaru współczesnego terroryzmu wskazują, że infrastruktura krytyczna pozostaje atrakcyjnym celem dla aktorów pragnących osiągnąć efekt polityczny i społeczny .

Administracja publiczna i usługi cyfrowe. Wraz z rozwojem eusług oraz cyfrowych kanałów kontaktu obywateli z państwem rośnie znaczenie ochrony systemów tożsamości, rejestrów oraz kanałów komunikacji. Ataki na te obszary mogą prowadzić do chaosu administracyjnego lub szeroko odczuwalnych utrudnień, a równocześnie są atrakcyjne z punktu widzenia propagandy. Z perspektywy sprawcy efekt „wymuszający" może zostać osiągnięty poprzez eskalację zakłóceń i wzrost presji społecznej na władze. Sektor zdrowia i usługi wrażliwe społecznie. Ransomware oraz ataki na dostępność systemów ochrony zdrowia mogą mieć silny efekt społeczny, ponieważ dotyczą obszaru wysokiej wrażliwości, jakim jest życie i zdrowie. Łańcuch dostaw i dostawcy usług IT. Coraz większa część usług państwa i gospodarki opiera się na zewnętrznych dostawcach oprogramowania, chmury oraz usług utrzymaniowych. Atak na dostawcę może skutkować efektem domina u wielu odbiorców. Europol zwraca uwagę na rosnącą złożoność ekosystemu cyberzagrożeń w UE, w tym na rozwój zorganizowanych modeli usług przestępczych oraz nadużyć technologicznych. W kontekście cyberterroryzmu oznacza to możliwość pośredniego oddziaływania poprzez mniej chronione ogniwa łańcucha dostaw (Europol, 2025).

W polskich realiach zagrożenie cyberterroryzmem należy postrzegać nie tylko przez pryzmat ataków technicznych na systemy informatyczne, lecz również jako ryzyko działań informacyjnych i procesów radykalizacyjnych zachodzących w cyberprzestrzeni. Środowisko cyfrowe sprzyja szybkiemu tworzeniu wspólnot ideologicznych, intensywnemu rozpowszechnianiu treści oraz funkcjonowaniu alternatywnych obiegów informacyjnych, w których narracje ekstremistyczne mogą się wzajemnie wzmacniać i normalizować. Skala oraz tempo cyrkulacji informacji powodują, że oddziaływanie

takich treści nie jest ograniczone do wąskich grup odbiorców, lecz może obejmować szerokie segmenty społeczeństwa (Liszkowska, 2023).

Szczególne znaczenie w tym kontekście mają mechanizmy charakterystyczne dla współczesnych platform cyfrowych. Przekaz może być łatwo skalowany i docierać do tysięcy odbiorców w krótkim czasie, a jednocześnie podlegać daleko idącej personalizacji dzięki algorytmom rekomendacji. Dodatkowym czynnikiem sprzyjającym jest możliwość anonimizacji działań oraz szybka migracja pomiędzy różnymi kanałami komunikacji w przypadku prób moderacji lub ograniczania treści. W rezultacie oddziaływanie informacyjne o charakterze cyberterrorystycznym nie musi opierać się na zaawansowanych kompetencjach technicznych; kluczowe staje się umiejętne wykorzystanie kanałów dystrybucji informacji oraz podatności poznawczych odbiorców. W tym sensie cyberterroryzm wpisuje się w szerszy katalog zagrożeń hybrydowych, w których presja na państwo i społeczeństwo budowana jest równolegle poprzez środki techniczne i oddziaływanie psychologiczne (Liszkowska, 2023).

Istotnym czynnikiem sprzyjającym tego rodzaju zagrożeniom jest także rosnąca skala masowych oszustw i kampanii socjotechnicznych w polskiej cyberprzestrzeni. Zjawiska te przyczyniają się do utrwalania „chaosu komunikacyjnego", upowszechnienia podszywania się pod instytucje publiczne oraz stopniowego osłabienia zaufania do cyfrowych kanałów kontaktu z państwem. W takim środowisku znacznie łatwiej o działania manipulacyjne i zastraszające, które w zależności od motywacji sprawcy i celu oddziaływania mogą przyjmować cechy cyberterroryzmu, zwłaszcza gdy służą wymuszaniu decyzji politycznych lub destabilizacji porządku społecznego (Gerwatowski, 2021).

Zagrożenie cyberterroryzmem dla Polski należy zatem ujmować jako splot kilku wzajemnie powiązanych wymiarów. Obejmuje ono ryzyko techniczne, związane z zakłóceniami dostępności i integralności systemów informatycznych, ryzyko społeczne, wyrażające się w narastaniu strachu, dezorientacji i utracie zaufania do instytucji publicznych, a także ryzyko polityczne, polegające na wywieraniu presji na decydentów poprzez eskalację zakłóceń i napięć społecznych. Skala i charakter incydentów obserwowanych w polskiej cyberprzestrzeni wskazują, że dominacja phishingu i technik socjotechnicznych tworzy sprzyjające warunki dla bardziej

ukierunkowanych i destrukcyjnych kampanii, których cele mogą wykraczać poza zwykły zysk finansowy (Rzeczpospolita, 2025).

W praktyce oznacza to, że przeciwdziałanie cyberterroryzmowi nie może ograniczać się wyłącznie do wdrażania zabezpieczeń technicznych. Równie istotna jest odporność instytucjonalna, rozumiana jako zdolność administracji i podmiotów publicznych do utrzymania ciągłości działania w warunkach zakłóceń, odporność informacyjna, polegająca na ograniczaniu skuteczności propagandy i dezinformacji, oraz odporność społeczna, obejmująca cyberhigienę i zdolność obywateli do rozpoznawania manipulacji. Z punktu widzenia badań nad terroryzmem kluczowe pozostaje przy tym precyzyjne rozróżnianie motywacji sprawców i celów ataków, tak aby polityka bezpieczeństwa była w stanie adekwatnie reagować zarówno na masową cyberprzestępczość, jak i na rzadsze, lecz potencjalnie znacznie bardziej dotkliwe scenariusze o charakterze terrorystycznym (Jankowski, 2018).

Podsumowanie

Przeprowadzona analiza potwierdza, że terroryzm pozostaje zjawiskiem dynamicznym, które nieustannie adaptuje się do zmieniających się warunków technologicznych i społecznych. Rozwój cyberprzestrzeni stworzył nowe możliwości działania dla ugrupowań terrorystycznych, umożliwiając im prowadzenie operacji o charakterze hybrydowym, łączących elementy przemocy fizycznej z cyberatakami i oddziaływaniem informacyjnym. Cyberterroryzm, rozumiany jako narzędzie „masowych zakłóceń", może prowadzić do poważnych konsekwencji społecznych, gospodarczych i politycznych, mimo braku bezpośrednich strat w ludziach.

W odniesieniu do Polski zagrożenie cyberterroryzmem należy postrzegać wielowymiarowo, uwzględniając zarówno aspekty techniczne, jak i społeczne oraz informacyjne. Rosnąca liczba incydentów cyberbezpieczeństwa, uzależnienie funkcjonowania państwa od systemów informatycznych oraz znaczenie Polski w kontekście geopolitycznym zwiększają jej podatność na tego rodzaju działania. Skuteczne przeciwdziałanie cyberterroryzmowi wymaga zatem podejścia kompleksowego, obejmującego nie tylko rozwój zabezpieczeń technicznych, lecz także wzmacnianie odporności instytucjonalnej, informacyjnej i społecznej. Tylko takie podejście pozwala na

ograniczenie skutków potencjalnych działań cyberterrorystycznych oraz zwiększenie bezpieczeństwa państwa w warunkach cyfrowej rzeczywistości.

Literatura

1. Agencja Bezpieczeństwa Wewnętrznego. (2024). *Raport o stanie bezpieczeństwa w cyberprzestrzeni RP*, Warszawa.
2. *Analiza bezpieczeństwa polskiego internetu w 2024 rok.* Pobrano z: https://www.gov.pl/web/baza-wiedzy/analiza-bezpieczenstwa-polskiego-internetu-w-2024-roku (dostęp: 20.03.2026).
3. Carbonelli, M., Quaranta, R., Malizia, A., Gaudio, P., Di Giovanni, D. (2024). An Analysis of Terrorist Attacks on Soft and Hard Targets in the Period 2000-2019, *International Journal of Safety and Security Engineering, 14*(3).
4. *Digital Scams Lead to Terror Financing.* Pobrano z: https://www.linkedin.com/pulse/digital-scams-lead-terror-financing-haunting-threat-qureshi-4ml0f (dostęp: 20.03.2026).
5. *EU struggles to protect itself from cyberattacks*. Pobrano z: https://euranetplus-inside.eu/eu-struggles-to-protect-itself-from-cyberattacks (dostęp: 20.03.2026).
6. Europol. (2023). *European Union Terrorism Situation and Trend Report*, Publications Office of the European Union, Luxembourg.
7. Gerwatowski, J. (2021). Cyberterroryzm jako efekt rozwoju nowych technologii informatycznych w pierwszej i drugiej dekadzie XXI wieku. *Przegląd Policyjny*, *141*(1).
8. Hoffman, B. (2017). *Inside terrorism*, Columbia University Press, Columbia.
9. Jankowski, P. (2018). Cyberterroryzm jako współczesne zagrożenie dla administracji publicznej. *Młody Jurysta*, (4), 13-27.
10. Kosta, R. A., *Terroryzm jako zagrożenie dla bezpieczeństwa cywilizacji zachodniej w XXI wieku*, Wydawnictwo Adam Marszałek, Toruń 2012.
11. *Kryptowaluty w finansowaniu terroryzmu.* Pobrano z: https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-kryptowaluty-w-finansowaniu-terroryzmu--realne-zagrozenie (dostęp: 20.03.2026).

12. Liszkowska, D. (2023). Cyberterrorism as a contemporary threat to the security of the state and socjet*y, De Securitate et Defensione. O Bezpieczeństwie i Obronności, 2*(9), 131-148.
13. Piątkowski, P. (1996). *Terroryzm. Nowe wyzwanie dla bezpieczeństwa*, Wydawnictwo Adam Marszałek, Warszawa.
14. Schmid, A. P., Forest, J. J. F., Lowe, T. (2021). Terrorism Studies: A Glimpse at the Current State of Research (2021). *Perspectives on Terrorism, 15*(3), 142-152.
15. *Socjotechnika lepsza niż hacking.* Pobrano z: https://www.rp.pl/przestepczosc/art42149701-socjotechnika-lepsza-niz-hacking-tak-oszusci-osaczaja-swoje-ofiary#:~:text=Cyberprzest%C4%99pcy%20odchodz%C4%85%20od%20zaawansowanych%20atak%C3%B3w%20hakerskich%20na%20rzecz%20socjotechniki%20%2D%20rp.pl (dostęp: 20.03.2026).
16. *Steal, Deal, Repeat: Cybercriminals cash in on your data*. Pobrano z: https://www.europol.europa.eu/media-press/newsroom/news/steal-deal-repeat-cybercriminals-cash-in-your-data (dostęp: 20.03.2026).
17. Superczyńska, K. (2019). *Terroryzm polityczny na pograniczu prawa i nauk politycznych, Gdańskie Studia Międzynarodowe 17*(1-2).
18. *Terroryści i darknet.* Pobrano z: https://cyberdefence24.pl/terrorysci-niechetnie--korzystaja-z-darknetu (dostęp: 20.03.2026).
19. The European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2024*. Pobrano z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (dostęp: 20.03.2026).
20. Wałek, T. (2018). Pojęcie, geneza i klasyfikacja zjawisk terrorystycznych., *Securitologia, 2*(28), 107-119.