Tomasz Grudniewski[1]

Akademia Bialska im. Jana Pawła II, Biała Podlaska

Karol Zygo[2]

Uniwersytet w Siedlcach

Sławomir Żurawski[3]

Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie

https://doi.org/10.29316/9788368103359_7

CYBERTERRORYZM W ERZE ZAGROŻEŃ HYBRYDOWYCH

CYBERTERRORISM IN THE AGE OF HYBRID THREATS

Streszczenie

Rozdział podejmuje problematykę cyberterroryzmu jako jednego z kluczowych wyzwań współczesnego środowiska bezpieczeństwa międzynarodowego. W części pierwszej przedstawiono ewolucję pojęcia cyberterroryzmu oraz dokonano analizy najważniejszych podejść definicyjnych obecnych w literaturze przedmiotu, ze

[1] https://orcid.org/0000-0003-3394-8992, e-mail: t.grudniewski@dyd.akademiabialska.pl
[2] https://orcid.org/0000-0002-8274-1958, e-mail: karolzygo@interia.pl
[3] https://orcid.org/0000-0001-9527-3391, e-mail: slawomir.zurawski@onet.pl

szczególnym uwzględnieniem trudności w rozróżnieniu cyberterroryzmu od cyberprzestępczości, hacktywizmu i cyberwojny. Część druga poświęcona została identyfikacji głównych aktorów cyberterroryzmu oraz omówieniu metod działań stosowanych we współczesnej cyberprzestrzeni, w tym ataków na infrastrukturę krytyczną, operacji informacyjnych oraz wykorzystania oprogramowania ransomware. W części trzeciej cyberterroryzm ukazano jako element zagrożeń hybrydowych oraz przeanalizowano jego znaczenie dla bezpieczeństwa międzynarodowego, ze szczególnym uwzględnieniem problemu atrybucji oraz podatności państw demokratycznych na tego rodzaju oddziaływania. Problem badawczy rozdziału sformułowano: czy cyberterroryzm we współczesnym środowisku bezpieczeństwa funkcjonuje jako autonomiczne zjawisko, czy też stanowi narzędzie wykorzystywane w ramach szerszego spektrum zagrożeń hybrydowych? Hipoteza badawcza zakłada, że cyberterroryzm nie występuje obecnie jako samodzielna forma zagrożenia, lecz pełni funkcję narzędzia strategicznego oddziaływania w działaniach hybrydowych, którego skuteczność opiera się przede wszystkim na generowaniu efektów psychologicznych, społecznych i politycznych, a nie na bezpośrednim niszczeniu infrastruktury teleinformatycznej. W badaniach zastosowano metodę analizy jakościowej, obejmującą krytyczną analizę literatury przedmiotu, dokumentów strategicznych organizacji międzynarodowych, aktów prawnych Unii Europejskiej oraz raportów instytucji zajmujących się bezpieczeństwem cybernetycznym. Przeprowadzona analiza potwierdza zasadność przyjętej hipotezy oraz wskazuje na potrzebę dalszych badań nad cyberterroryzmem w kontekście zagrożeń hybrydowych.

Słowa kluczowe: bezpieczeństwo, cyberterroryzm, hybrydowość, bezpieczeństwo międzynarodowe

Abstract

The chapter addresses the issue of cyberterrorism as one of the key challenges of the contemporary international security environment. The first part presents the evolution of the concept of cyberterrorism and analyses the most important definitional approaches present in the literature on the subject, with particular emphasis on the difficulties in distinguishing cyberterrorism from cybercrime, hacktivism and cyberwar. The second part was devoted to the identification of the main actors of cyberterrorism and the discussion of methods of action used in modern cyberspace, including attacks on critical infrastructure, information operations and the use of ransomware. The third part shows cyberterrorism as an element of hybrid threats and analyses its significance for international security, with particular emphasis on the problem of attribution and the vulnerability of democratic states to such influences.

The research problem of the chapter is formulated: does cyberterrorism in the modern security environment function as an autonomous phenomenon, or is it a tool used within a wider spectrum of hybrid threats? The research hypothesis assumes that cyberterrorism does not currently exist as an independent form of threat, but serves as a tool of strategic influence in hybrid operations, the effectiveness of which is based primarily on generating psychological, social and political effects, and not on the direct destruction of ICT infrastructure. The research used the method of qualitative analysis, including a critical analysis of the literature on the subject, strategic documents of international organizations, legal acts of the European Union and reports of institutions dealing with cyber security. The analysis confirms the legitimacy of the adopted hypothesis and indicates the need for further research on cyberterrorism in the context of hybrid threats.

Keywords: security, cyberterrorism, hybridity, international security

Wstęp

Dynamiczny rozwój technologii informacyjnych oraz powszechna cyfryzacja życia społecznego, gospodarczego i politycznego sprawiły, że cyberprzestrzeń stała się jednym z kluczowych obszarów funkcjonowania współczesnych państw. Systemy teleinformatyczne odpowiadają obecnie za prawidłowe działanie infrastruktury krytycznej, administracji publicznej, sektora finansowego, energetycznego oraz transportowego. Wraz ze wzrostem zależności od technologii cyfrowych pojawiły się nowe formy zagrożeń, których charakter wykracza poza tradycyjnie rozumiane konflikty zbrojne.

Jednym z najbardziej złożonych i trudnych do jednoznacznego zdefiniowania zagrożeń jest cyberterroryzm. Pojęcie to funkcjonuje w literaturze przedmiotu od kilku dekad, jednak do dziś nie wypracowano jednej, powszechnie akceptowanej definicji. Wczesne ujęcia cyberterroryzmu koncentrowały się głównie na technicznych aspektach ataków na systemy informatyczne oraz na potencjalnych skutkach materialnych takich działań. Współczesne środowisko bezpieczeństwa, zdominowane przez zagrożenia hybrydowe, wymusza jednak szersze i bardziej kompleksowe spojrzenie na to zjawisko.

Cyberterroryzm coraz częściej nie występuje jako autonomiczna forma przemocy, lecz jako element złożonych operacji obejmujących działania informacyjne, dezinformacyjne oraz presję psychologiczną. Granice pomiędzy cyberterroryzmem, cyberwojną, cyberprzestępczością czy hacktywizmem ulegają zatarciu, co znacząco utrudnia identyfikację sprawców oraz reakcję państw i organizacji międzynarodowych. Celem niniejszego rozdziału jest wykazanie, że cyberterroryzm należy postrzegać przede wszystkim jako narzędzie strategicznego oddziaływania, którego skuteczność opiera się na destabilizacji społecznej i politycznej, a nie wyłącznie na technicznym zniszczeniu systemów.

Cyberterroryzm – współczesne podejścia definicyjne

Pojęcie cyberterroryzmu pojawiło się w literaturze naukowej pod koniec XX wieku wraz z gwałtownym rozwojem technologii informacyjnych oraz upowszechnieniem Internetu. Wczesne próby jego definiowania były silnie inspirowane klasycznymi teoriami terroryzmu i koncentrowały się na przeniesieniu znanych mechanizmów przemocy politycznej do nowej domeny, jaką stała się cyberprzestrzeń. Jednym z pierwszych badaczy, którzy podjęli próbę konceptualizacji tego zjawiska, był Barry Collin, wskazujący na cyberterroryzm jako formę wykorzystania systemów komputerowych do realizacji celów terrorystycznych (Collin, 1997).

W klasycznych ujęciach cyberterroryzm definiowano przede wszystkim jako politycznie lub ideologicznie motywowane ataki na systemy informatyczne, których celem było zastraszenie społeczeństwa lub wymuszenie określonych decyzji na rządach. Takie podejście wskazuje, że aby dane działanie mogło zostać zakwalifikowane jako cyberterroryzm, musi ono prowadzić do realnego strachu, porównywalnego ze skutkami tradycyjnych aktów terrorystycznych. W tym ujęciu cyberterroryzm odróżniano zarówno od cyberprzestępczości, jak i od zwykłych incydentów bezpieczeństwa teleinformatycznego (Denning, 2000, s. 10).

Jednocześnie już na wczesnym etapie rozwoju badań nad cyberterroryzmem zaczęto wskazywać na trudności definicyjne wynikające z niematerialnego charakteru cyberprzestrzeni oraz problemu oceny skutków ataków. W przeciwieństwie do klasycznych aktów terrorystycznych, cyberataki rzadko prowadzą do bezpośrednich ofiar śmiertelnych, co rodzi pytania

o zasadność stosowania terminu „terroryzm" w odniesieniu do działań prowadzonych wyłącznie w cyberprzestrzeni (https://www.unodc.org).

Współczesne podejścia definicyjne coraz częściej odchodzą od wyłącznie technicznego rozumienia cyberterroryzmu. Badacze zwracają uwagę, że istotą tego zjawiska nie jest sam atak na system informatyczny, lecz intencja oraz efekt oddziaływania społecznego i politycznego. Wskazuje się, że wiele działań określanych mianem cyberterroryzmu nie spełnia klasycznych kryteriów terroryzmu, jednak ich znaczenie strategiczne polega na destabilizacji, podważaniu zaufania do instytucji państwowych oraz wzmacnianiu poczucia zagrożenia (Rid, 2013, s. 14). Na tym tle szczególnie istotne staje się rozróżnienie cyberterroryzmu od zjawisk pokrewnych, takich jak cyberprzestępczość, hacktywizm czy cyberwojna. Cyberprzestępczość, zgodnie z definicjami stosowanymi przez Europol i ONZ, ma charakter przede wszystkim ekonomiczny i nastawiona jest na osiąganie zysków finansowych[5]. Hacktywizm natomiast, choć często motywowany ideologicznie, ma zazwyczaj charakter symboliczny i rzadko prowadzi do trwałego zastraszenia społeczeństwa.

Najwięcej kontrowersji budzi relacja pomiędzy cyberterroryzmem a cyberwojną. Cyberwojna jest zazwyczaj wiązana z działaniami prowadzonymi przez państwa lub podmioty działające na ich rzecz w ramach konfliktów zbrojnych lub rywalizacji strategicznej (https://www.nato.int). W praktyce jednak wiele działań w cyberprzestrzeni realizowanych jest przez aktorów pośrednich (proxy actors), co prowadzi do zatarcia granic pomiędzy terroryzmem a działaniami państwowymi. Problem ten jest szeroko omawiany w dokumentach NATO oraz Unii Europejskiej dotyczących zagrożeń hybrydowych (https://www.consilium.europa.eu).

Współczesne instytucje międzynarodowe coraz częściej unikają jednoznacznego definiowania cyberterroryzmu, koncentrując się zamiast tego na funkcjonalnym opisie zagrożeń. Przykładem jest podejście Unii Europejskiej, która w dokumentach strategicznych dotyczących bezpieczeństwa cybernetycznego i zagrożeń hybrydowych wskazuje na potrzebę wzmacniania odporności systemów i społeczeństw, niezależnie od formalnej kwalifikacji danego incydentu. Podobne stanowisko prezentuje Organizacja Narodów Zjednoczonych, akcentując znaczenie współpracy międzynarodowej i budowania zdolności reagowania.

Podsumowując, ewolucja pojęcia cyberterroryzmu prowadzi od wąskiego, technicznego ujęcia ku rozumieniu tego zjawiska jako narzędzia strategicznego oddziaływania. Współczesny cyberterroryzm nie musi prowadzić do fizycznego zniszczenia infrastruktury, aby osiągnąć swoje cele. Jego skuteczność opiera się na destabilizacji, chaosie informacyjnym oraz presji psychologicznej, co czyni go szczególnie niebezpiecznym elementem współczesnych zagrożeń hybrydowych.

Aktorzy i metody cyberterroryzmu we współczesnym środowisku bezpieczeństwa

Współczesny cyberterroryzm charakteryzuje się znacznym zróżnicowaniem aktorów oraz metod działań, co odróżnia go od klasycznych form terroryzmu. Rozwój cyberprzestrzeni, niski próg wejścia technologicznego oraz globalny zasięg Internetu sprawiają, że działania o charakterze cyberterrorystycznym mogą być prowadzone zarówno przez zorganizowane struktury, jak i przez pojedyncze osoby. W literaturze przedmiotu coraz częściej podkreśla się, że cyberterroryzm nie jest już domeną wyłącznie klasycznych organizacji terrorystycznych, lecz elementem szerszego spektrum aktywności niepaństwowych w cyberprzestrzeni (Kowalewski, Kowalewski, 2014, s. 25).

Do pierwszej kategorii aktorów zalicza się organizacje terrorystyczne, które wykorzystują cyberprzestrzeń przede wszystkim jako narzędzie wsparcia swojej działalności. Jak wskazują raporty Europolu (Europol, 2025), Internet odgrywa kluczową rolę w propagandzie, rekrutacji, komunikacji wewnętrznej oraz pozyskiwaniu środków finansowych. Choć bezpośrednie cyberataki prowadzone przez tego typu organizacje są stosunkowo rzadkie, ich aktywność w sferze informacyjnej i psychologicznej może generować efekty porównywalne z klasycznymi aktami terroru.

Drugą, coraz istotniejszą grupą aktorów są podmioty niepaństwowe działające jako aktorzy pośredni (proxy actors). Są to grupy lub jednostki, które formalnie nie są powiązane z żadnym państwem, lecz w praktyce realizują działania zbieżne z interesami określonych aktorów państwowych. Zjawisko to jest szeroko analizowane w kontekście zagrożeń hybrydowych, gdzie cyberterroryzm może pełnić funkcję narzędzia destabilizacji bez jednoznacznego przypisania odpowiedzialności. Tego rodzaju działania

znacząco utrudniają reakcję prawną i polityczną na poziomie międzynarodowym (Jokinen, Normark, 2022, s. 5).

Szczególną kategorię stanowią samotni aktorzy (lone actors), którzy dzięki powszechnemu dostępowi do narzędzi informatycznych są w stanie prowadzić działania o charakterze destabilizującym bez zaplecza organizacyjnego. Jak wskazują analizy The European Union Agency for Cybersecurity (ENISA), niska bariera wejścia sprawia, że nawet osoby o ograniczonych kompetencjach technicznych mogą wykorzystywać gotowe narzędzia do przeprowadzania ataków lub kampanii dezinformacyjnych. W tym kontekście cyberterroryzm staje się zjawiskiem trudnym do przewidzenia i monitorowania (ENISA, 2023).

Jeśli chodzi o metody działań, współczesny cyberterroryzm obejmuje szerokie spektrum technik, które nie ograniczają się do klasycznych ataków na systemy informatyczne. Jednym z najczęściej wskazywanych obszarów są ataki na infrastrukturę krytyczną, w tym systemy energetyczne, transportowe, wodociągowe oraz telekomunikacyjne. Raporty instytucji międzynarodowych podkreślają, że nawet krótkotrwałe zakłócenia w funkcjonowaniu takich systemów mogą prowadzić do poważnych skutków społecznych i politycznych. Coraz większe znaczenie zyskują również operacje informacyjne i dezinformacyjne, które stanowią istotny element współczesnych działań cyberterrorystycznych. Ich celem nie jest fizyczne zniszczenie infrastruktury, lecz manipulowanie percepcją społeczną, pogłębianie podziałów oraz podważanie zaufania do instytucji publicznych. Działania informacyjne w cyberprzestrzeni są często integralną częścią szerszych operacji hybrydowych, w których cyberterroryzm pełni rolę katalizatora destabilizacji. Szczególnym narzędziem współczesnego cyberterroryzmu stało się oprogramowanie ransomware. Choć ransomware jest najczęściej klasyfikowane jako forma cyberprzestępczości, w określonych kontekstach może pełnić funkcję narzędzia terroru, zwłaszcza gdy jego celem jest sparaliżowanie funkcjonowania instytucji publicznych lub infrastruktury krytycznej. Ataki tego typu mogą prowadzić do efektu zastraszenia znacznie wykraczającego poza wymiar ekonomiczny (Stodolnik, 2025).

Warto również zwrócić uwagę na rosnącą rolę automatyzacji i sztucznej inteligencji w działaniach cyberterrorystycznych. Narzędzia oparte na algorytmach uczenia maszynowego mogą być wykorzystywane do automatyzacji ataków, generowania treści dezinformacyjnych czy analizy

podatności systemów. ENISA podkreśla, że rozwój tych technologii zwiększa skalę i tempo potencjalnych działań cyberterrorystycznych, jednocześnie utrudniając ich wykrywanie.

Podsumowując, współczesny cyberterroryzm charakteryzuje się dużą elastycznością oraz zdolnością adaptacji do zmieniającego się środowiska bezpieczeństwa. Zarówno zróżnicowanie aktorów, jak i ewolucja metod działań sprawiają, że cyberterroryzm stanowi istotne wyzwanie dla państw i organizacji międzynarodowych. Jego skuteczność opiera się nie na skali technicznego zniszczenia, lecz na zdolności do generowania długotrwałych skutków psychologicznych, społecznych i politycznych.

Cyberterroryzm jako element zagrożeń hybrydowych i wyzwanie dla bezpieczeństwa międzynarodowego

Współczesne środowisko bezpieczeństwa międzynarodowego charakteryzuje się rosnącą rolą zagrożeń hybrydowych, które łączą działania militarne i niemilitarne, jawne i skryte, państwowe i niepaństwowe. W tym kontekście cyberterroryzm należy postrzegać nie jako zjawisko izolowane, lecz jako jeden z instrumentów szerszego spektrum oddziaływań strategicznych. Jego znaczenie wynika przede wszystkim z możliwości prowadzenia działań destabilizujących bez formalnego wypowiadania wojny oraz przy zachowaniu wysokiego poziomu niejednoznaczności co do tożsamości sprawcy.

Zagrożenia hybrydowe definiowane są w dokumentach Unii Europejskiej oraz NATO jako działania wykorzystujące jednocześnie różne środki nacisku – polityczne, ekonomiczne, informacyjne, cybernetyczne i militarne – w celu osłabienia państwa przeciwnika. Cyberterroryzm doskonale wpisuje się w tę logikę, ponieważ umożliwia oddziaływanie na funkcjonowanie państwa i społeczeństwa bez konieczności użycia siły kinetycznej. Jego skuteczność opiera się na połączeniu cyberataków z operacjami informacyjnymi oraz dezinformacyjnymi, które wzmacniają efekt psychologiczny i społeczny.

Jednym z kluczowych problemów związanych z cyberterroryzmem w kontekście bezpieczeństwa międzynarodowego jest kwestia atrybucji, czyli jednoznacznego przypisania odpowiedzialności za dane działanie. W cyberprzestrzeni identyfikacja sprawcy jest szczególnie trudna ze względu na możliwość maskowania pochodzenia ataków, wykorzystywania

serwerów pośredniczących oraz działania aktorów proxy. Problem atrybucji stanowi jedno z głównych ograniczeń skutecznej reakcji państw na zagrożenia cybernetyczne. W przypadku cyberterroryzmu niejednoznaczność ta może być wykorzystywana celowo w celu eskalacji napięć lub destabilizacji relacji międzynarodowych (Derian-Toth, Walsh, Sergueeva, Kim, Coon, Hadan, Stancombe, 2021, s. 7).

Cyberterroryzm stanowi szczególne wyzwanie dla państw demokratycznych, które opierają swoje funkcjonowanie na otwartych systemach informacyjnych, wolności słowa oraz zaufaniu społecznym. Działania cyberterrorystyczne mogą prowadzić do erozji zaufania obywateli do instytucji publicznych, podważania legitymacji władzy oraz wzmacniania polaryzacji społecznej. Odporność społeczeństw demokratycznych staje się kluczowym elementem przeciwdziałania zagrożeniom hybrydowym, w tym cyberterroryzmowi.

W odpowiedzi na rosnące zagrożenia cybernetyczne organizacje międzynarodowe podejmują działania mające na celu wzmocnienie zdolności państw do zapobiegania i reagowania na cyberataki. Unia Europejska rozwija ramy prawne i instytucjonalne w zakresie cyberbezpieczeństwa, czego przykładem jest dyrektywa NIS2, nakładająca na państwa członkowskie obowiązek wzmacniania odporności infrastruktury krytycznej oraz systemów informacyjnych. Działania te mają pośrednio ograniczać skuteczność cyberterroryzmu poprzez podniesienie poziomu zabezpieczeń i zdolności reagowania (Dyrektywa NIS2).

Równie istotną rolę odgrywa Organizacja Narodów Zjednoczonych, która koncentruje się na budowaniu norm odpowiedzialnego zachowania państw w cyberprzestrzeni oraz na wspieraniu współpracy międzynarodowej. W dokumentach ONZ podkreśla się, że cyberzagrożenia, w tym cyberterroryzm, mogą stanowić zagrożenie dla pokoju i bezpieczeństwa międzynarodowego, nawet jeśli nie prowadzą bezpośrednio do konfliktu zbrojnego. W tym ujęciu cyberterroryzm traktowany jest jako element szerszego problemu bezpieczeństwa globalnego.

Istotnym aspektem cyberterroryzmu jako zagrożenia hybrydowego jest również jego niski koszt prowadzenia działań w porównaniu z klasycznymi formami konfliktu. Relatywnie niewielkie nakłady finansowe mogą prowadzić do nieproporcjonalnie dużych skutków politycznych i społecznych. Z tego względu cyberterroryzm stanowi atrakcyjne narzędzie dla

aktorów dysponujących ograniczonymi zasobami, a jednocześnie dążących do wywarcia presji na silniejsze państwa (Nye, 2017, s. 44-46).

Podsumowując, cyberterroryzm jako element zagrożeń hybrydowych stanowi poważne wyzwanie dla współczesnego bezpieczeństwa międzynarodowego. Jego specyfika polega na połączeniu działań cybernetycznych z oddziaływaniem informacyjnym i psychologicznym, co utrudnia zarówno identyfikację sprawców, jak i skuteczną reakcję. Przeciwdziałanie cyberterroryzmowi wymaga zatem nie tylko rozwoju zdolności technicznych, lecz także wzmocnienia odporności instytucjonalnej i społecznej oraz pogłębionej współpracy międzynarodowej.

Podsumowanie

Przeprowadzona w rozdziale analiza pozwala stwierdzić, że cyberterroryzm stanowi jedno z najbardziej złożonych i dynamicznie ewoluujących zagrożeń współczesnego środowiska bezpieczeństwa. Jego istota nie sprowadza się wyłącznie do technicznych ataków na systemy informatyczne, lecz obejmuje znacznie szerszy wymiar oddziaływania politycznego, psychologicznego i informacyjnego. W tym sensie cyberterroryzm należy postrzegać jako narzędzie strategicznego wpływu, którego skuteczność opiera się na destabilizacji funkcjonowania państw i społeczeństw, a niekoniecznie na fizycznym zniszczeniu infrastruktury.

Analiza ewolucji pojęcia cyberterroryzmu wskazuje, że klasyczne definicje, wypracowane na przełomie XX i XXI wieku, coraz częściej okazują się niewystarczające wobec współczesnych realiów. Wczesne ujęcia, koncentrujące się na analogii do tradycyjnych aktów terrorystycznych, nie uwzględniały w pełni specyfiki cyberprzestrzeni jako domeny niematerialnej, transgranicznej i trudnej do jednoznacznej kontroli. Współczesne podejścia definicyjne przesuwają akcent z samego aktu cyberataku na jego intencję oraz efekt oddziaływania społecznego, co pozwala lepiej uchwycić istotę cyberterroryzmu jako zjawiska politycznego i strategicznego.

Rozważania dotyczące aktorów i metod cyberterroryzmu potwierdzają, że zjawisko to nie jest ograniczone do działalności klasycznych organizacji terrorystycznych. Coraz większą rolę odgrywają aktorzy niepaństwowi działający pośrednio, a także samotni sprawcy, wykorzystujący powszechnie dostępne narzędzia cyfrowe. Zróżnicowanie podmiotów oraz

niski próg wejścia sprawiają, że cyberterroryzm staje się trudny do przewidzenia i skutecznego zwalczania. Jednocześnie ewolucja metod działań, obejmująca ataki na infrastrukturę krytyczną, operacje dezinformacyjne, ransomware oraz wykorzystanie automatyzacji i sztucznej inteligencji, wskazuje na rosnące znaczenie efektu psychologicznego i informacyjnego jako kluczowego elementu oddziaływania.

Umiejscowienie cyberterroryzmu w kontekście zagrożeń hybrydowych pozwala lepiej zrozumieć jego rolę w architekturze bezpieczeństwa międzynarodowego. Cyberterroryzm funkcjonuje jako narzędzie umożliwiające prowadzenie działań destabilizujących poniżej progu wojny, często bez jednoznacznego przypisania odpowiedzialności. Problem atrybucji, charakterystyczny dla cyberprzestrzeni, znacząco ogranicza możliwości reakcji państw i organizacji międzynarodowych, co czyni cyberterroryzm szczególnie atrakcyjnym środkiem oddziaływania asymetrycznego. Wyniki analizy wskazują również, że państwa demokratyczne są szczególnie podatne na skutki cyberterroryzmu. Otwartość systemów informacyjnych, znaczenie opinii publicznej oraz wysoki poziom cyfryzacji sprzyjają skuteczności działań wymierzonych w zaufanie społeczne i stabilność instytucjonalną. W tym kontekście cyberterroryzm stanowi wyzwanie nie tylko dla bezpieczeństwa technicznego, lecz także dla spójności społecznej i odporności politycznej państw. Podsumowując, cyberterroryzm należy postrzegać jako trwały element współczesnego środowiska bezpieczeństwa, którego znaczenie będzie rosło wraz z dalszym rozwojem technologii informacyjnych oraz pogłębianiem się procesów cyfryzacji. Skuteczne przeciwdziałanie temu zjawisku wymaga podejścia wielowymiarowego, łączącego środki techniczne, prawne, organizacyjne i edukacyjne, a także intensyfikacji współpracy międzynarodowej. Dalsze badania nad cyberterroryzmem powinny koncentrować się na doprecyzowaniu ram pojęciowych, analizie mechanizmów oddziaływania psychologicznego oraz wypracowaniu skutecznych modeli reagowania, adekwatnych do realiów zagrożeń hybrydowych XXI wieku.

Literatura

1. Collin B. (1997). *The Future of Cyberterrorism*. Hanover: Institute for Security Technology Studies, Dartmouth College.

2. Countering hybrid threats. Pobrano z: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats (dostęp: 20.03.2026).
3. Cyber defense. Pobrano z: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence
4. Cyberterrorism. Pobrano z: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html (dostęp: 20.03.2026).
5. Denning, D. E. (2000). *Cyberterrorism: Testimony before the U.S. House of Representatives*. Washington D.C: United States House of Representatives.
6. Derian-Toth, G., Walsh, R., Sergueeva, A., Kim, E., Coon, A., Hadan, H., Stancombe, J. (2021). *Opportunities for Public and Private Attribution of Cyber Operations*, TALLINN PAPERS YOUNG SCHOLAR EDITION, Nr 12, Tallin.
7. Developments in the field of information and telecommunications in the context of international security. Pobrano z: https://disarmament.unoda.org/en/our-work/emerging-challenges/developments-field-information-and-telecommunications-context (dostęp: 20.03.2026).
8. Dyrektywa NIS2. Pobrano z: https://eur-lex.europa.eu/eli/dir/2022/2555 (dostęp: 20.03.2026).
9. European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2023*, Luksemburg 2023.
10. Europol, *European Union Terrorism Situation and Trend Report 2025 (EU TE-SAT)* Publications Office of the European Union, Luksemburg 2025.
11. Hybrid threats. Pobrano z: https://www.consilium.europa.eu/en/policies/hybrid-threats/?utm_source (dostęp: 20.03.2026).
12. Jokinen, J., Normark, M. (2022). *Hybrid threats from non-state actors: A taxonomy***,** Helskinki: The European Centre of Excellence for Countering Hybrid Threats.
13. Kowalewski, J., Kowalewski, M. (2014). Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa. *Telekomunikacja i Techniki Informacyjne*, (1-2), 24-32.
14. Nye Jr, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security, 41*(3), 44-71.

15. Rid, T. (2013). *Cyber War Will Not Take Place*. Oxford-New York: Oxford University Press.
16. Stodolnik, M. (2025). Cyber threats as hybrid activity against the European Union in light of the current geopolitical situation. *Terroryzm – studia, analizy, prewencja*", Special Issue, 225-248.