Marta Chodyka[1]

Akademia Bialska im. Jana Pawła II, Biała Podlaska

Sławomir Żurawski[2]

Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie

Marcin Oskierko[3]

Państwowa Akademia Nauk Stosowanych w Chełmie

https://doi.org/10.29316/9788368103359_8

CYBERTERRORYZM JAKO ZAGROŻENIE BEZPIECZEŃSTWA PAŃSTWA W ŚRODOWISKU CYFROWYM

CYBERTERRORISM AS A THREAT TO NATIONAL SECURITY IN THE DIGITAL ENVIRONMENT

Streszczenie

Celem niniejszego rozdziału jest analiza cyberterroryzmu jako zagrożenia bezpieczeństwa państwa w środowisku cyfrowym oraz identyfikacja jego uwarunkowań, mechanizmów oddziaływania i sposobów przeciwdziałania. Problem badawczy

[1] https://orcid.org/0000-0002-8819-2451, e-mail: m.chodyka@dyd.akademiabialska.pl
[2] https://orcid.org/0000-0001-9527-3391, e-mail: slawomir.zurawski@onet.pl
[3] https://orcid.org/0000-0003-3450-6037, e-mail: moskierko@panschelm.edu.pl

sformułowano: w jakim stopniu cyberterroryzm wpływa na poziom bezpieczeństwa państwa oraz jakie działania podejmowane są w celu ograniczenia skutków tego zjawiska. Przyjęto hipotezę badawczą zakładającą, że cyberterroryzm stanowi jedno z najistotniejszych zagrożeń asymetrycznych współczesnych państw, a skuteczność przeciwdziałania temu zjawisku zależy od integracji działań instytucjonalnych, prawnych i technologicznych. W opracowaniu zastosowano metodę analizy literatury przedmiotu, analizę dokumentów strategicznych oraz metodę analizy systemowej, co pozwoliło na kompleksowe ujęcie problematyki cyberterroryzmu w kontekście bezpieczeństwa państwa. Przedstawione rozważania mają na celu ukazanie charakteru i skali współczesnych zagrożeń w cyberprzestrzeni oraz wskazanie kierunków rozwoju systemów ochrony państwa przed cyberterroryzmem.

Słowa kluczowe: bezpieczeństwo, cyberterroryzm, środowisko cyfrowe, zagrożenia

Abstract

The aim of this chapter is to analyze cyberterrorism as a threat to state security in the digital environment and to identify its conditions, mechanisms of impact and ways of counteracting. The research problem was formulated: to what extent does cyberterrorism affect the level of national security and what actions are taken to limit the effects of this phenomenon. A research hypothesis was adopted assuming that cyberterrorism is one of the most important asymmetric threats of modern states, and the effectiveness of counteracting this phenomenon depends on the integration of institutional, legal and technological activities. The study uses the method of literature analysis, analysis of strategic documents and the method of system analysis, which allowed for a comprehensive approach to the issue of cyberterrorism in the context of state security. The presented considerations are aimed at showing the nature and scale of contemporary threats in cyberspace and indicating the directions of development of state protection systems against cyberterrorism.

Keywords: security, cyberterrorism, digital environment, threats

Pojęcie cyberterroryzmu

Na przestrzeni ostatnich lat rozwinął się postęp technologiczny, postęp w procesach wytwarzania, przetwarzania i przekazywania informacji. Społeczeństwo uzależnia się od technologii informacyjnej, co sprawia, że staje ono w obliczu wzrastającego zagrożenia jakim jest cyberterroryzm.

Cyberterroryzm jest pojęciem wieloaspektowym. Stanowi jedno z trzech głównych wyzwań i zagrożeń dla bezpieczeństwa teleinformatycznego w wymiarze narodowym i międzynarodowym oraz jest zjawiskiem o dynamicznie narastającej charakterystyce. Cyberterroryzm powstał na podstawie terroryzmu z wykorzystaniem obszaru jakim jest cyberprzestrzeń, a także jest zjawiskiem z pogranicza innych obszarów, takich jak:

- bezpieczeństwo teleinformatyczne,
- technologie informatyczne i teleinformacyjne,
- bezpieczeństwo osobowe,
- bezpieczeństwo fizyczne,
- regulacje prawne narodowe i międzynarodowe,
- dane osobowe (Białoskórski, 2011).

Termin cyberterroryzm nie posiada jednoznacznej definicji zawierającej charakterystykę przedmiotu. W literaturze podjęto wiele prób definiowania cyberterroryzmu i do tej pory nie udało się jego zdefiniować. Terminu cyberterroryzm pojawił się po raz pierwszy w 1979 roku w Szwecji, w raporcie szwedzkiego ministerstwa obrony na temat zagrożeń komputerowych, w odniesieniu do destrukcyjnego wykorzystywania komputerów, który miał na celu niszczenia systemów teleinformatycznych, danych w nich przechowywanych, oprogramowania, a w konsekwencji w celu zastraszania rządów i społeczeństwa, wywierania presji psychologicznej, doprowadzenie do zagrożenia życia lub znacznych start materialnych. W tym samym czasie termin ten używany był przez amerykańskich specjalistów w dziedzinie wywiadu wojskowego.

Pierwszą próbę sformułowania pojęcia cyberterroryzmu podjął się Barry Collin w latach 80. XX wieku. Według niego to *„świadome wykorzystywanie systemu informacyjnego, sieci komputerowej lub jej części składowych w celu wsparcia lub ułatwienia terrorystycznej akcji”*. Cyberterroryzm przyjmuje formę ataków przeprowadzanych w cyberprzestrzeni przy pomocy komputerów na zasoby przeciwnika. Do najczęściej spotykanych definicji cyberterroryzmu należą:

- Dorothy Denning: „cyberterroryzm jest konwergencją cyberprzestrzeni i terroryzmu. Dotyczy nielegalnych ataków i gróźb ataków przeciwko komputerom, sieciom komputerowym i informacjom przechowywanych w nich, by zastraszyć lub wymusić na rządzie lub

społeczeństwie polityczne lub społeczne cele. By zakwalifikować atak jako cyberterroryzm powinien skutkować przemocą przeciwko ludziom lub mieniu lub przynajmniej wyrządzić wystarczająco szkody by stwarzać strach",

- James Lewis: „(...) wykorzystanie sieci komputerowych jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe, itp.) bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań",
- US National Infrastructure Protection Centre: „(...) akt kryminalny popełniony przy użyciu komputera i możliwości telekomunikacyjnych, powodujący użycie siły, zniszczenie i / lub przerwanie świadczenia usług dla wywołania strachu, poprzez wprowadzanie zamieszania lub niepewności w danej populacji, w celu wpływania na rządy, ludność tak, aby wykorzystać ich reakcje dla osiągnięcia określonych celów politycznych, społecznych, ideologicznych lub głoszonego przez terrorystów programu",
- US Federal Bureau of Investigation: „(...) jest to obmyślony, politycznie umotywowany akt przemocy wymierzony przeciwko informacjom, programom, systemom komputerowym lub bazom danych, który mając charakter niemilitarny, przeprowadzony jest przez ponadnarodowe lub narodowe grupy terrorystyczne",
- M. Pollitt z George Washington University: „(...) jest skrytym, politycznie motywowanym atakiem przeciwko informacji, systemom lub programom komputerowym, bazom danych, których efektem jest przemoc przeciwko celom niewojskowym realizowanym przez grupy ponadnarodowe" (Szybrycht, 2005).

W powyższych definicjach można zauważyć pojawiające się w nich dwa zasadnicze wyróżniki, a mianowicie:

- uwzględniają istnienie możliwości wykorzystania systemów komputerowych lub telekomunikacyjnych do przeprowadzenia ataku cybernetycznego,
- komputery i systemy informacyjne są celem takiego ataku (Yannakogeorgos, 2014).

Rozważając znaczenie pojęcia cyberterroryzm należy zauważyć, że cyberterroryzm to coś więcej aniżeli przedrostek rodzajowy zestawiony ze standardową aktywnością o charakterze terrorystycznym (Yannakogeorgos, 2014).

W dokumentach instytucji Unii Europejskiej pojęcie cyberterroryzmu nie zawsze funkcjonuje jako jedna, zamknięta definicja, jednak jest ono interpretowane poprzez regulacje dotyczące terroryzmu oraz cyberprzestępczości. Zgodnie z podejściem Unii Europejskiej cyberterroryzm można rozumieć jako działania terrorystyczne prowadzone z wykorzystaniem systemów teleinformatycznych lub skierowane przeciwko infrastrukturze cyfrowej w celu wywołania poważnych zakłóceń w funkcjonowaniu państwa, społeczeństwa lub gospodarki. Jednym z kluczowych aktów prawnych UE odnoszących się do tej problematyki jest Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 w sprawie zwalczania terroryzmu. Dokument ten wskazuje, że przestępstwa terrorystyczne obejmują działania polegające m.in. na: *„poważnym zakłóceniu lub zniszczeniu infrastruktury, w tym systemów informatycznych, które mogą narazić życie ludzkie lub spowodować poważne straty gospodarcze”* (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu, 2017).

Polskie prawo karne za działania o charakterze terrorystycznym przewiduje dla sprawcy karę pozbawienia wolności co najmniej 5 lat, jeśli dopuścił się on czynu mającego na celu:

- poważne zastraszenie wielu osób,
- zmuszenie organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,
- wywołanie poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej,
- innego państwa czy organizacji międzynarodowej (Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, 1997).

Analizując szereg różnorodnych definicji cyberterroryzmu można zaobserwować, że wszystkie definicje sprowadzają się do jednego wspólnego elementu, a mianowicie cyberterroryzm występuje wtedy, kiedy

mamy do czynienia z politycznie motywowanym atakiem z użyciem sieci teleinformatycznych.

Obszary oddziaływania cyberterroryzmu na bezpieczeństwo państwa

Obiektami i obszarami atakowanymi przez cyberterrorystów może być infrastruktura krytyczna państw, wspólnot i różnego rodzaju organizacje, czyli innymi słowy systemy, funkcjonalne obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Typologia zaproponowana przez Thomasa R. Mockaitisa wskazuje, że działania cyberterrorystyczne mogą być realizowane przez różnorodne podmioty, w tym państwa prowadzące operacje w cyberprzestrzeni, organizacje terrorystyczne, zorganizowane grupy przestępcze oraz tzw. samotnych sprawców, którzy wykorzystują technologie informacyjne do destabilizacji systemów bezpieczeństwa państwa (Mockaitis, 2008).

Cyberterroryzm może być postrzegany jako zagrożenie będące konsekwencją rozwoju technologii, zwłaszcza Internetu oraz globalizacji. Z uwagi na specyfikę tego zjawiska, cyberterroryzm powinien stanowić przedmiot szczególnej analizy ze strony współczesnych decydentów odpowiedzialnych za bezpieczeństwo państw i społeczności międzynarodowej. Poniżej przedstawiono kluczowe aspekty, które powodują, że cyberterroryzm stanowi poważne zagrożenie dla bezpieczeństwa międzynarodowego:

- niskie koszty materialne – organizacja cyberataku nie wymaga znacznych nakładów finansowych, lecz przede wszystkim specjalistycznej wiedzy; koszty tego typu operacji są znacząco niższe niż tradycyjnych działań terrorystycznych,
- dostosowanie środków do celów operacyjnych – społeczeństwa adaptują swoje działania w celu osiągnięcia jak najbardziej efektywnych rezultatów. Cyberterroryzm minimalizuje ryzyko utraty życia, gdyż nie wiąże się z tak ekstremalnymi działaniami, jak ataki samobójcze,

- relatywna anonimowość – identyfikacja sprawców cyberataków jest wyjątkowo trudna, podobnie jak wykrycie motywacji stojących za konkretnymi aktami cyberterroryzmu,
- specyfika środowiska operacyjnego – Internet umożliwia przygotowanie ataków z wielu lokalizacji, ułatwiając działanie sprawców,
- efekt psychologiczny – w dzisiejszych czasach Internet jest wykorzystywany przez osoby fizyczne i instytucje do obsługi infrastruktury krytycznej. Skutkiem cyberataków jest zastraszenie obywateli poprzez naruszenie poczucia bezpieczeństwa,
- współzależność podmiotów – ogólnodostępny charakter cyberprzestrzeni sprzyja podejmowaniu działań, które mogą mieć negatywne, destrukcyjne skutki,
- globalny zasięg ataku – Internet jako medium globalne umożliwia przeprowadzenie ataków z dowolnego miejsca na świecie, co pozwala na skuteczne oddziaływanie na różnorodne cele.

Przyjmując atak cybernetyczny jako proces, można go przedstawić jako sekwencję następujących po sobie etapów obejmujących rozpoznanie celu, uzyskanie nieautoryzowanego dostępu do systemu oraz realizację działań destrukcyjnych lub destabilizujących. Poniżej na Rysunku 1 przedstawiono procesowy model realizacji ataku cybernetycznego.



Rysunek 1. Procesowy model realizacji ataku cybernetycznego

Źródło: opracowanie własne.

Rysunek 1 przedstawia procesowy model realizacji ataku cybernetycznego obejmujący trzy zasadnicze fazy. Pierwsza faza polega na identyfikacji i analizie celu ataku poprzez zbieranie informacji o systemie teleinformatycznym. Druga faza obejmuje działania prowadzące do uzyskania nieautoryzowanego dostępu do systemu poprzez wykorzystanie jego podatności.

Trzecia faza obejmuje realizację działań operacyjnych, takich jak modyfikacja, kradzież lub niszczenie danych oraz zakłócanie funkcjonowania systemów informatycznych.

W literaturze wyróżnia się dwa rodzaje akcji cyberterrorystycznych:

- ataki fizyczne na systemy informacyjne,
- ataki mające miejsce w cyberprzestrzeni (Białoskórski, 2011).

Atak fizyczny na systemy informacyjne to prowadzenie walki starymi metodami. W poprzednich latach terroryści uważali, że niszcząc systemy i instalacje komputerowe, atakują samo serce państwa. Natomiast specjaliści twierdzą, że nie trzeba się znać na informatyce by zniszczyć sieć informatyczną i tym samym sparaliżować życie w krajach wysoko rozwiniętych.

Atak w cyberprzestrzeni polega na uderzeniu w oprogramowanie przeciwnika (ang. Software). W tym przypadku jest wiele sposobów do przeprowadzenia takiego typu akcji w cyberprzestrzeni. Poniżej przedstawiono niektóre metody:

- stealing passwords – polega na uzyskaniu haseł dostępu do sieci,
- social engineering – wykorzystanie niekompetencji osób, które mają dostęp do systemu,
- bugs and backdoors – korzystanie z systemu bez zezwoleń lub używanie oprogramowania z nielegalnych źródeł,
- authentication failures – zniszczenie mechanizmu używanego do autoryzacji,
- protocol failures – wykorzystanie luk w zbiorze reguł sterujących wymianą informacji pomiędzy dwoma lub więcej niezależnymi urządzeniami lub procesami,
- information leakage – atakujący uzyskuje informacje dostępne tylko dla administratora, niezbędne dla prawidłowego funkcjonowania sieci,
- denial of service – uniemożliwienie użytkownikom korzystania z ich systemu (Szybrycht, 2005).

Cyberataki to działania mające na celu zakłócenie funkcjonowania systemów informatycznych lub uzyskanie nieautoryzowanego dostępu do danych poprzez różnorodne metody, takie jak kradzież haseł, wykorzystywanie luk w zabezpieczeniach czy instalowanie złośliwego oprogramowania. Współcześnie cyberprzestrzeń stała się jednym z głównych obszarów konfliktów, a cyberterroryzm jest uznawany za poważne zagrożenie

dla bezpieczeństwa państw i społeczeństw. W efekcie, zarówno instytucje publiczne, jak i prywatne firmy muszą nieustannie rozwijać środki ochrony przed tego typu zagrożeniami, aby zapewnić ciągłość działania i ochronę wrażliwych informacji.

System przeciwdziałania cyberterroryzmowi oraz kierunki jego rozwoju w środowisku bezpieczeństwa państwa

Rozwój cyberterroryzmu, rozumianego jako działania w cyberprzestrzeni ukierunkowane na zastraszenie społeczeństwa, wymuszenie decyzji politycznych lub destabilizację funkcjonowania państwa, wymaga budowy zintegrowanego systemu ochrony obejmującego rozwiązania prawne, organizacyjne, techniczne oraz kompetencyjne. W praktyce przeciwdziałanie cyberterroryzmowi opiera się na łączeniu narzędzi bezpieczeństwa informacji (zarządzanie ryzykiem, ciągłość działania, procedury reagowania na incydenty), cyberobrony i ochrony infrastruktury krytycznej, a także na mechanizmach współpracy międzysektorowej (administracja – operatorzy usług kluczowych – sektor prywatny) i międzynarodowej, ponieważ znaczna część incydentów ma charakter transgraniczny.

Postępujący rozwój technologii informacyjnych pozwala na stwierdzenie, iż ryzyko cyberataku terrorystycznego rzeczywiście wzrasta (Smarzewski, 2017).

Na poziomie międzynarodowym istotną rolę odgrywa NATO, które po doświadczeniach m.in. ataków na Estonię i rosnącej liczbie operacji w cyberprzestrzeni rozwija cyberobronę jako element zbiorowej obrony. Kluczowym krokiem było przyjęcie polityki cyberobrony na szczycie w Walii (2014), gdzie uznano cyberobronę za część fundamentalnych zadań NATO, a także wskazano, że poważny cyberatak może stanowić przesłankę do uruchomienia mechanizmu art. 5 Traktatu Północnoatlantyckiego (Cyber defence). Równolegle Sojusz rozwija zdolności operacyjne i planistyczne w cyberprzestrzeni oraz wzmacnia ochronę własnych systemów i świadomość sytuacyjną, co jest realizowane m.in. przez struktury NCIA i zdolności reagowania na incydenty (NCIRC) w ramach ochrony zasobów NATO (NCIA). Istotnym trendem pozostaje także pogłębianie współdziałania NATO – UE w zakresie wymiany informacji o incydentach (np. porozumienie techniczne

NCIRC – CERT-EU), co wzmacnia zdolności wykrywania i reagowania w obu organizacjach (EEAS).

Na poziomie Unii Europejskiej ciężar działań przesunął się w stronę spójnych wymagań prawnych i budowania odporności systemowej. Dyrektywa NIS2 ustanawia jednolite ramy cyberbezpieczeństwa dla kluczowych sektorów i wzmacnia obowiązki w zakresie zarządzania ryzykiem oraz zgłaszania incydentów, a także zakłada rozwój współpracy między państwami członkowskimi (European Commission). Równocześnie wzmocniono rolę ENISA, która działa na podstawie tzw. Cybersecurity Act (rozporządzenie 2019/881), otrzymując stały mandat oraz wspierając operacyjną koordynację i rozwój kultury cyberbezpieczeństwa w UE, w tym poprzez sieci współpracy CSIRT. W perspektywie rozwojowej oznacza to przejście od podejścia „reaktywnego" (po incydencie) do podejścia „odpornościowego" (resilience-by-design): audyty i minimalne standardy, wymogi zarządcze (odpowiedzialność kierownictwa), ćwiczenia, współdziałanie transgraniczne oraz tworzenie zdolności reagowania na kryzysy na poziomie UE.

W odniesieniu do ONZ/ITU należy podkreślić, że Global Cybersecurity Agenda (GCA) ma przede wszystkim charakter ramowy i historycznie ważny, natomiast współcześnie dyskusja międzynarodowa koncentruje się na harmonizacji podejść, budowaniu zdolności państw (capacity building) i wypracowywaniu zasad odpowiedzialnego zachowania w cyberprzestrzeni. Samo wskazywanie filarów ITU może pozostać w tekście jako tło, ale warto je osadzić w logice „rozwoju zdolności" i ograniczyć opisowość. Podobnie wątek IMPACT wymaga doprecyzowania: jest to inicjatywa współpracująca z ITU, opisywana jako platforma wsparcia i współpracy w obszarze cyberzagrożeń, jednak jej znaczenie w praktyce polityk cyberbezpieczeństwa państw UE jest zwykle drugorzędne względem mechanizmów NIS2/ENISA i struktur krajowych.

W Polsce zasadniczą ramą organizacyjną jest ustawa o krajowym systemie cyberbezpieczeństwa, która porządkuje role i obowiązki podmiotów oraz zakłada współpracę kluczowych zespołów reagowania na incydenty. Z perspektywy praktycznej i aktualnej terminologii należy wskazywać trzy CSIRT poziomu krajowego: CSIRT NASK, CSIRT GOV i CSIRT MON, które koordynują obsługę incydentów w swoich domenach oraz współdziałają, aby zapewnić spójny system reagowania na incydenty poważne i krytyczne. W tym ujęciu wcześniejsze określenie „CERT.GOV.PL" warto

zastąpić aktualnym „CSIRT GOV" (portal csirt.gov.pl), a opis zadań oprzeć na współczesnym katalogu: monitorowanie zagrożeń, szacowanie ryzyka, ostrzeganie, reagowanie i koordynacja obsługi incydentów istotnych dla ciągłości działania państwa i infrastruktury krytycznej. Dodatkowo komponent wojskowy cyberbezpieczeństwa i cyberobrony wzmacniany jest przez struktury odpowiedzialne za funkcjonowanie CSIRT MON, co wpisuje się w trend integracji bezpieczeństwa cywilnego i wojskowego w obszarze zagrożeń hybrydowych.

Kierunki zmian w systemie przeciwdziałania cyberterroryzmowi zarówno w Polsce, jak i w UE i NATO można ująć w kilku dominujących tendencjach:

- wzrost roli zarządzania ryzykiem i odporności (ciągłość działania, segmentacja, „security by design"),
- przyspieszenie wymiany informacji i wspólnego reagowania (CSIRT-y, koordynacja transgraniczna, ćwiczenia),
- wzmacnianie ochrony infrastruktury krytycznej i usług cyfrowych poprzez minimalne standardy oraz obowiązki raportowania,
- profesjonalizacja kadr i rozwój kompetencji w administracji, służbach i wymiarze sprawiedliwości,
- rosnące znaczenie współpracy publiczno-prywatnej, ponieważ znaczna część zasobów i usług krytycznych znajduje się w domenie operatorów i dostawców technologii.

Współczesne bezpieczeństwo cybernetyczne wymaga zintegrowanego podejścia na poziomie międzynarodowym, europejskim i krajowym. Organizacje międzynarodowe, takie jak NATO i Unia Europejska, rozwijają polityki i struktury, które mają na celu zwiększenie odporności na cyberzagrożenia, promowanie współpracy i wymiany informacji, a także koordynację działań w przypadku incydentów. Jednolitość przepisów prawnych, ustanawianie minimalnych standardów ochrony i wzmacnianie systemów raportowania są dziś kluczowymi narzędziami budowania odporności infrastruktury krytycznej. Równocześnie wzrasta rola specjalistycznych zespołów reagowania na incydenty, profesjonalizacji kadr oraz łączenia sił pomiędzy administracją publiczną i sektorem prywatnym. Coraz większe znaczenie mają także działania edukacyjne i rozwijanie kompetencji, by sprostać dynamicznie zmieniającym się wyzwaniom w cyberprzestrzeni. Współczesna

strategia opiera się na prewencji, szybkim reagowaniu i budowaniu kultury bezpieczeństwa, która obejmuje zarówno państwa, jak i obywateli.

Podsumowanie

Cyberterroryzm stanowi jedno z kluczowych zagrożeń bezpieczeństwa współczesnych państw, którego znaczenie systematycznie wzrasta wraz z rozwojem technologii informacyjno-komunikacyjnych oraz postępującą cyfryzacją życia społecznego, gospodarczego i administracyjnego. Analiza problematyki cyberterroryzmu pozwala stwierdzić, że jest to zjawisko wielowymiarowe, łączące elementy klasycznego terroryzmu z wykorzystaniem narzędzi cyberprzestrzeni, co powoduje, że jego skutki mogą obejmować zarówno sferę bezpieczeństwa narodowego, jak i stabilność ekonomiczną oraz funkcjonowanie społeczeństwa informacyjnego.

Przeprowadzone rozważania wskazują, że cyberterroryzm może oddziaływać na państwo poprzez ataki na infrastrukturę krytyczną, systemy administracji publicznej, sektor finansowy oraz systemy komunikacyjne. W ujęciu procesowym działania cyberterrorystyczne mają charakter wieloetapowy i obejmują rozpoznanie celu, uzyskanie nieautoryzowanego dostępu do systemów teleinformatycznych oraz realizację działań destrukcyjnych lub destabilizujących. Złożoność i transgraniczny charakter tych zagrożeń powodują trudności w identyfikacji sprawców oraz skutecznym przeciwdziałaniu incydentom cybernetycznym.

Istotnym elementem przeciwdziałania cyberterroryzmowi jest rozwój systemów bezpieczeństwa obejmujących współpracę międzynarodową, regulacje prawne oraz rozwiązania technologiczne. Na poziomie globalnym i regionalnym znaczącą rolę odgrywają organizacje międzynarodowe, takie jak NATO, Unia Europejska oraz struktury ONZ, które podejmują działania na rzecz zwiększenia odporności państw na cyberzagrożenia oraz rozwijania mechanizmów reagowania na incydenty cybernetyczne. Równie istotne znaczenie ma rozwój krajowych systemów cyberbezpieczeństwa, w tym instytucji odpowiedzialnych za monitorowanie zagrożeń oraz reagowanie na incydenty w cyberprzestrzeni.

Współczesne kierunki rozwoju systemów przeciwdziałania cyberterroryzmowi wskazują na konieczność przechodzenia od działań reaktywnych do strategii opartych na zarządzaniu ryzykiem, budowaniu odporności

infrastruktury krytycznej oraz wykorzystywaniu nowoczesnych technologii, w tym systemów analizy danych i sztucznej inteligencji. Istotnym wyzwaniem pozostaje także rozwój kompetencji specjalistów w zakresie cyberbezpieczeństwa oraz wzmacnianie współpracy między sektorem publicznym i prywatnym.

Cyberterroryzm stanowi dynamicznie rozwijające się zagrożenie dla bezpieczeństwa państwa w środowisku cyfrowym, wymagające systemowego i wielowymiarowego podejścia do jego zwalczania. Skuteczność przeciwdziałania temu zjawisku zależy przede wszystkim od integracji działań instytucjonalnych, prawnych i technologicznych, a także od zdolności państw do adaptacji do zmieniającego się środowiska zagrożeń w cyberprzestrzeni.

Literatura

1. Białoskórski, R. (2011). *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku, Zarys problematyki*. Warszawa: Wyższa Szkoła Cła i Logistyki.
2. Cyber defence. (2026). *NATO Topic*. Pobrano z: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence (dostęp: 20.03.2026).
3. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu.
4. EEAS. (2026). *EU and NATO increase information sharing on cyber incidents*. Pobrano z: https://www.eeas.europa.eu/node/5253_en (dostęp: 20.03.2026).
5. European Commission. (2026). *NIS2 Directive: securing network and information systems, Shaping Europe's digital future*. Pobrano z: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (dostęp: 20.03.2026).
6. Mockaitis, T. R. (2008). *The New Terrorism: Myths and Reality*. Stanford: Stanford University Press.
7. NCIA. (2026). *NATO Cyber Security Centre.* Pobrano z: https://www.ncia.nato.int/about-us/service-portfolio/nato-cyber-security-centre (dostęp: 20.03.2026).
8. Smarzewski, M. (2017). Cyberterroryzm a cyberprzestępstwa o charakterze terrorystycznym. *Ius Novum, 11*(1), 64-75.

9. Szybrycht, T. (2005). Cyberterroryzm jako nowa forma zagrożenia terrorystycznego. *Zeszyty Naukowe Akademii Marynarki Wojennej, 1*(160), 173-181.
10. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553).
11. Yannakogeorgos, P. A. (2014). *Rethinking the Threat of Cyberterrorism*. W: T. M. Chen, L. Jarvis, S. Macdonald (red.), *Cyberterrorism: Understanding, Assessment, and Response* (s. 43-62). New York: Springer.