Annales Universitatis Paedagogicae Cracoviensis 428

Studia de Securitate 15(2) ▪ 2025
ISSN 2657-8549
DOI 10.24917/26578549.15.2.11

Patryk Manowiecki
Uniwersytet Jana Kochanowskiego w Kielcach
ORCID 0009-0003-2257-0506

Zjawisko cyberterroryzmu a ochrona infrastruktury krytycznej

Wprowadzenie

Wraz z początkiem XXI wieku nastąpił intensywny postęp technologiczny w obszarze nowych technologii. Rozwój internetu oraz coraz większe możliwości cyberprzestrzeni sprawiły, iż wiele dziedzin życia społecznego przeniosło się do sfery wirtualnej. Cyberprzestrzeń stworzyła dla użytkownika wiele szans (dostęp do informacji, ułatwienia w kontaktach), jak również wykreowała wiele zagrożeń (np. oszustwa internetowe, kradzieże danych czy włamania na konta) oraz przestrzeń i ramy dla walki zbrojnej. Terroryści, „idąc z duchem czasu", przenieśli swoje działania ze świata realnego do wirtualnego, co doprowadziło do powstania nowego oblicza terroryzmu – cyberterroryzmu. To zjawisko możemy zaliczyć do jednych z najpoważniejszych zagrożeń XXI w.

Szczególnie wrażliwym obszarem państwa na ataki cyberterrorystyczne jest infrastruktura krytyczna (IK). W związku z powyższym jej ochrona jest jednym z najważniejszych zadań państwa – bardzo trudno wyobrazić sobie codzienne funkcjonowanie bez wody czy energii elektrycznej. Biorąc pod uwagę, iż obecnie społeczeństwo jest całkowicie uzależnione od systemów infrastruktury krytycznej, są one bardzo podatnym celem narażonym na wrogie ataki za pomocą cyberprzestrzeni. Hakerzy działający w sieci, za pomocą swoich działań, chcą wzbudzić strach w atakowanym społeczeństwie, nagłośnić atak czy np. zdobyć sławę.

Problematykę cyberterroryzmu poruszali w swoich publikacjach m.in. Jakub i Marian Kowalewscy, aczkolwiek analizowali ją w większym stopniu w kontekście bezpieczeństwa informacji. Wywody Joanny Bieniek czy Rafała Kołodziejczyka koncentrują się na zakresie ewolucji tego zjawiska i jego oddziaływania na bezpieczeństwo państwa (np. jako elementu wojny hybrydowej). Z kolei Mariusz Staszczak, pisząc o odporności infrastruktury krytycznej w kontekście współczesnych zagrożeń, skupił się bardziej na zagrożeniach w świecie rzeczywistym niż w cyberprzestrzeni.

Celem głównym niniejszego artykułu jest próba omówienia zjawiska cyberterroryzmu oraz ukazanie jego szkodliwego wpływu na funkcjonowanie infrastruktury krytycznej. Postawiono następujące pytanie główne: Jakie działania może podjąć państwo w celu ochrony infrastruktury krytycznej przed atakami cyberterrorystycznymi? Aby znaleźć odpowiedź na to pytanie, sformułowano pytania szczegółowe:

1. Czym jest cyberterroryzm oraz jakie są możliwe metody ataków stosowane przez hakerów?
2. Jakie wyznaczniki wpłynęły na przeniesienie działań terrorystów do przestrzeni wirtualnej?

Badania nad podjętą tematyką miały charakter teoretyczny, w związku z czym zastosowano takie metody jak: analiza krytyczna dostępnej literatury, dedukcja czy uogólnienie.

Cyberterroryzm

Pomimo że na przestrzeni ostatnich kilkunastu lat cyberterroryzm stał się przedmiotem debat publicznych i naukowych, wciąż nie ma wypracowanej jednej, w pełni przyjętej definicji tego terminu. Spowodowane jest to różnorodnością tego zjawiska oraz jego dynamicznym charakterem, co w połączeniu z jego różnymi formami stanowi trudność w dokładnym określeniu tego zagrożenia[1]. Jak pisze Rafał Kołodziejczyk, za twórcę terminu cyberterroryzm „uważa się pracownika Institute for Security and Intelligence w Kalifornii – Barry'ego Collina, który w latach 80. dwudziestego wieku użył go jako pierwszy (...)"[2].

[1] P. Jankowski (2018). *Cyberterroryzm jako współczesne zagrożenie dla administracji publicznej*. „Młody Jurysta Czasopismo Studentów i Doktorantów Wydziału Prawa i Administracji UKSW", 4, s. 16. https://czasopisma.uksw.edu.pl/index.php/mj/article/view/2988 [dostęp: 11.02.2025].

[2] R. Kołodziejczyk (2017). *Nowa odsłona terroryzmu – cyberterroryzm*. „Rocznik Bezpieczeństwa Międzynarodowego", 11(2) s. 148. Wydawnictwo Naukowe Dolnośląskiej Szkoły Wyższej.

Jednym z polskich naukowców, który podjął się próby zdefiniowania pojęcia *cyberterroryzm*, jest Miron Lakomy, pisząc, iż jest to „politycznie motywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów”[3]. Autor w przytoczonej definicji zawarł jeden z głównych motywów, który przyświeca hakerom w ich działaniach, tj. politykę.

Nieco inaczej cyberterroryzm zdefiniowali Sylwia Wojciechowska-Filipek oraz Zbigniew Ciekanowski, którzy w jednej z publikacji zawarli informację, że „cyberterroryzm może być rozumiany jako działanie blokujące, zniekształcające lub niszczące informacje przechowywane i przekazywane w cyberprzestrzeni oraz obezwładniające systemy teleinformatyczne”[4]. Warto dodać, iż ideą cyberterroryzmu nie jest tylko niszczenie informacji czy wymuszanie określonych działań na konkretnych jednostkach czy grupach. Możemy tutaj również wskazać na sparaliżowanie lub częściowe osłabienie działania takich obszarów, jak np. energetyka czy transport[5]. Nawiązuje do tego Kołodziejczyk: „cyberterroryzm to jedna z najbardziej nieprzewidywalnych form oddziaływania zorganizowanych grup przestępczych na stabilność infrastruktury krytycznej państwa (np. telekomunikacja, systemy energetyczne i finansowe)”[6]. To właśnie ataki wymierzone w te sektory mogą powodować największy chaos społeczny oraz destabilizować funkcjonowanie państwa.

Analizując powyżej przytoczone definicje oraz literaturę przedmiotu, możemy dostrzec, iż cyberterroryzm może być postrzegany w dwóch ujęciach: wąskim i szerokim. W znaczeniu wąskim będzie to: cyberprzestępstwo o charakterze terrorystycznym. Natomiast w ujęciu szerokim:

- terroryzm realizowany w cyberprzestrzeni;
- działanie pojedynczych osób, organizacji czy państw poza granicami prawa o charakterze terrorystycznym;
- działanie przeciwko treściom i zasobom informatycznym w celu ich modyfikowania lub zniszczenia;
- stosowanie przemocy (fizycznej i psychicznej) w celu wymuszenia określonych postaw czy zachowań u ofiary;
- wywołanie nacisku i wpływu na władzę, ośrodki decyzyjne w celu osiągnięcia zamierzonych celów;

[3] M. Lakomy (2015). *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw.* Wydawnictwo Uniwersytetu Śląskiego. Katowice, s. 157.

[4] S. Wojciechowska-Filipek, Z. Ciekanowski (2022). *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki – organizacji – państwa.* CeDeWu. Warszawa, s. 206.

[5] Tamże, s. 205.

[6] R. Kołodziejczyk (2017). *Nowa odsłona…* Dz. cyt., s. 148.

– działania o podłożu politycznym, ideologicznym i fundamentalnym w celu osiągnięcia korzyści[7].

Konkludując, można stwierdzić, iż cyberterroryzm to atak terrorystyczny przeprowadzony za pomocą cyberprzestrzeni. Należy jednak zaznaczyć, iż jest to temat bardzo obszerny, wymagający zgłębienia oraz ciągłej analizy. Właściwości cyberprzestrzeni sprawiają, że cyberterroryści wykorzystują sieć do różnych celów, np. propagandowych, szerzenia nienawiści, prowadzenia wojny psychologicznej czy wzniecania konfliktów w poszczególnych państwach[8]. Również jednym z głównych celów ataku cyberterrorystycznego jest szerzenie dezinformacji wśród społeczeństwa.

Metody ataków cyberterrorystycznych

Metody ataków, jakimi dysponują terroryści działający w cyberprzestrzeni, są bardzo różne. Marcin Sienicki zalicza do nich:

– bomby logiczne;
– *chipping* (chipy z oprogramowaniem dającym dostęp do systemu umieszczone w komputerach);
– *hijacking* (metoda polegająca na przechwyceniu transmisji między dwoma systemami);
– *backdoor* (tworzenie przez programistów specjalnych „furtek" w aplikacjach);
– *spoofing* (metoda polegająca na podszyciu się pod użytkowników systemu w celu jego destabilizacji);
– *keylogger* (oprogramowanie przechwytujące dane wpisywane na klawiaturze);
– *sniffing* (podsłuchiwanie ruchu w sieci w celu pozyskania haseł);
– *exploit* (oprogramowanie, które pozwala na dostęp do komputera ofiary w sposób bezpośredni)[9].

Innymi przykładami metod ataków komputerowych stosowanymi przez cyberterrorystów są:

– trojan (program, który pozwala na wykonanie przez użytkownika niepożądanego działania);

[7] J. Kowalewski, M. Kowalewski (2017). *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm.* Oficyna Wydawnicza Politechniki Warszawskiej. Warszawa, s. 81–82.

[8] R. Kołodziejczyk, P. Manowiecki (2024). *Cyberterroryzm jako element wojny hybrydowej.* W: P. Soroka, P. Zamelek, K. Rawska, A. Zagórska (red.). *Aspekty technologiczne i informatyczne współczesnych zbrojeń.* Dom Wydawniczy ELIPSA. Warszawa, s. 123.

[9] M. Sienicki (2024). *Cyberterroryzm – charakterystyka zjawiska.* „Kwartalnik Bellona", tom 716, nr 1, s. 54. https://kwartalnikbellona.com/article/547315/pl [dostęp: 11.02.2025].

- *phishing* (metoda polegająca na podszyciu się pod instytucje w celu kradzieży danych użytkownika);
- *spoofing* (podszycie się pod urządzenie w celu dokonania nielegalnego wtargnięcia do danego systemu);
- *spyware* (program wykorzystywany do szpiegostwa)[10].

Do metod ataków cybernetycznych możemy zaliczyć również różnego rodzaju wirusy czy spam, czyli wysyłanie dużej liczby wiadomości na konto pocztowe użytkownika. Joanna Bieniek w swojej publikacji do powyższego katalogu dodaje jeszcze takie metody jak: *DoS* (odmowa usługi) czy *flooding* (wysyłanie do komputera nadmiernej liczby żądań)[11]. Metody ataków cyberterrorystycznych możemy spróbować usystematyzować i podzielić na główne grupy:

- ataki blokujące, np. atak typu *DoS* lub *DDoS*;
- ataki podszywania się i oszustwa, np. *spoofing* i *hijacking*;
- ataki z elementami inżynierii społecznej (*phishing, pharming*);
- ataki kryptograficzne (*brute force*, ataki pasywne);
- oprogramowanie wspierające i ułatwiające przeprowadzenie ataku, np. *spyware*, *rootkit*;
- inne formy (*sniffing*)[12].

Jak można wywnioskować, możliwości przeprowadzenia ataku terrorystycznego w cyberprzestrzeni jest wiele, a powyższy katalog nie jest zamknięty. Cyberterroryzm jest zagrożeniem szczególnym dla społeczeństwa, jak również bardzo mało przewidywalnym[13]. Postęp technologiczny, który cały czas ma miejsce, i rozwój nowych technologii czy sztucznej inteligencji najprawdopodobniej będą generować coraz to nowsze metody ataków cyberterrorystycznych.

Analizując zjawisko cyberterroryzmu i możliwe metody ataków, nie sposób nie odnieść się do powodów, które skłaniają terrorystów do działania w cyberprzestrzeni. Są to m.in.:

1. Niski koszt – w porównaniu z możliwością przeprowadzenia klasycznego ataku. Do przeprowadzenia ataku wystarczy jedynie komputer z połączeniem do internetu.
2. Anonimowość sprawców ataku – cyberprzestrzeń oferuje większe możliwości anonimowej działalności sprawców niż klasyczny terroryzm.

[10] R. Kołodziejczyk (2017). *Nowa odsłona terroryzmu...* Dz. cyt., s. 152–153.

[11] J. Bieniek (2021). *Cyberterroryzm zagrożeniem bezpieczeństwa państw współczesnego świata*. „Rocznik Bezpieczeństwa Morskiego", 5, Akademia Marynarki Wojennej im. Bohaterów Westerplatte, s. 157.

[12] J. Kowalewski, M. Kowalewski (2017). *Zagrożenia informacji...* Dz. cyt.

[13] K. Chałubińska-Jentkiewicz (2019). *Cyberbezpieczeństwo – zagadnienia definicyjne.* „Cybersecurity and Law", 2 (2). Akademia Sztuki Wojennej, s. 19.

3. Bardziej rozbudowane możliwości ataku – biorąc pod uwagę fakt, iż obecnie praktycznie każda instytucja, firma, większość urządzeń czy część społeczeństwa korzysta z sieci, liczba możliwych celów ataków dla terrorystów jest ogromna.
4. Łatwość działania – cyberprzestrzeń zaciera granice, w związku z czym stwarza możliwość ataku z drugiego krańca świata, zmniejszając przy tym ryzyko wykrycia sprawców ataku.
5. Większy efekt propagandowy ataku[14].

Przyczyny, które powodują działanie terrorystów w cyberprzestrzeni, sprawiają, iż walka z cyberterroryzmem jest rzeczą skomplikowaną. Szczególnie w czasach obecnych, kiedy mamy tak rozbudowaną sieć oraz gdy sztuczna inteligencja zaczyna odgrywać coraz większą rolę. Dlatego podejmowane kroki w tym zakresie wymagają szerokiej współpracy na szczeblu państwowym i międzynarodowym.

Infrastruktura krytyczna (IK)

W obecnych czasach to właśnie elementy infrastruktury krytycznej są jednymi z najbardziej narażonych na wrogie ataki hakerów w sieci. Zgodnie z ustawą, poprzez infrastrukturę krytyczną należy rozumieć „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalne obiekty, w tym 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”[15]. Możemy tutaj wymienić systemy takie jak np.: zaopatrzenie w energię, surowce energetyczne i paliwa, łączność, sieci teleinformatyczne, systemy finansowe, zaopatrzenie w żywność i wodę, ochrona zdrowia, transport, ratownictwo, systemy zapewniające ciągłość działania administracji publicznej, produkcja, składowanie, przechowywanie i stosowanie substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych[16].

Wszystkie te sektory są kluczowe dla prawidłowego funkcjonowania państwa oraz społeczeństwa. Obecnie bardzo trudno wyobrazić sobie sytuację, w której nie mamy dostępu do żywności, energii czy łączności. Również sektor ratowniczy czy bankowy opiera swoje działanie głównie na usługach elektronicznych. Dlatego też dłuższa przerwa w działaniu tych obszarów mogłaby

[14] T. Szubrycht (2005). *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*. „Zeszyty Naukowe Akademii Marynarki Wojennej”, 46(1), Akademia Marynarki Wojennej im. Bohaterów Westerplatte, s. 185.

[15] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2007 Nr 89 poz. 590), art. 3.

[16] Tamże.

spowodować bardzo duży paraliż państwa. Należy mieć na uwadze również aspekt, o którym wspomina Marek Górka: „Cyberterroryzm zagraża więcej niż tylko jednemu lub dwóm obszarom infrastruktury krytycznej; wpływa na wszystkie systemy komputerowe, które zarządzają krytyczną infrastrukturą począwszy od sieci elektroenergetycznej, wodnej, urządzeń do sektorów transportu i bezpieczeństwa publicznego po globalne giełdy finansowe”[17].

Biorąc pod uwagę fakt, że infrastruktura krytyczna jest najważniejszą i niezbędną dziedziną dla państwa i jego obywateli, jej ochrona musi stanowić jedno z priorytetowych zadań państwa[18]. Szczególnie gdy spojrzymy na statystyki ukazujące liczbę ataków hakerskich na cele infrastruktury krytycznej. Według *Raportu o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 r.* Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV) zarejestrował łącznie 322 656 zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego, z czego 43 785 zakwalifikowano jako faktyczne incydenty bezpieczeństwa (przytoczone dane zawierają zgłoszenia rejestrowane w systemie ARAKIS[19], jak również obsługiwane w ramach pracy bieżącej Zespołu CSIRT GOV). Dokładną liczbę zgłoszeń i incydentów przedstawia Tabela 1.

Tabela 1. Liczba zarejestrowanych zgłoszeń oraz incydentów w 2023 r.

	Liczba zgłoszeń	Liczba incydentów
ARAKIS GOV	302 768	39 109
CSIRT GOV	19 888	4 676

Źródło: Opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 r.* CSIRT GOV. https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/980,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2023-roku.html [dostęp: 18.03.2025].

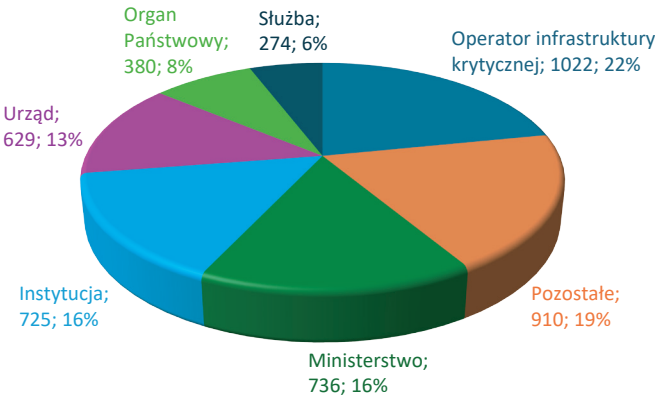
Jak zauważamy, w 2023 roku zespół CSIRT GOV przyjął blisko 20 000 zgłoszeń, na podstawie których zarejestrowano 4 676 incydentów

[17] M. Górka (2017). *Wybrane aspekty definicyjne cyberterroryzmu i ich znaczenie w perspektywie polityki bezpieczeństwa*. „Cywilizacja i Polityka”, (15), s. 303. https://czasopisma.marszalek.com.pl/images/pliki/cip/15/cip1518.pdf [dostęp: 12.02.2025].

[18] W. Leśnikowski (2011). *Cyberataki na infrastrukturę krytyczną jako tanie i skuteczne środki paraliżowania rozwiniętych państw.* Centrum Doktryn i Szkolenia Sił Zbrojnych. Bydgoszcz. https://archiwum-cdissz.wp.mil.pl/plik/file/Publikacje/cyberataki-na-infrastruktur-krytyczn.pdf [dostęp: 11.02.2025].

[19] ARAKIS GOV jest systemem wczesnego ostrzegania o zagrożeniach pojawiających się w internecie. Zob. *ARAKIS GOV*. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. https://csirt.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html [dostęp: 10.04.2025].

(w rozumieniu Ustawy o krajowym systemie cyberbezpieczeństwa z 2018 r.). Na wykresie poniżej przedstawiono, jak rozkładała się liczba zarejestrowanych incydentów w podziale na określone sektory (Wykres 1).



Wykres 1. Liczba incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa z podziałem na sektory

Źródło: Opracowanie własne na podstawie: ***Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 r.*** CSIRT GOV. https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/980,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2023-roku.html [dostęp 18.03.2025].

Z powyższego diagramu wynika, że infrastruktura krytyczna była najbardziej podatnym celem ataków z wszystkich wyszczególnionych dziedzin. To właśnie operatorów infrastruktury krytycznej dotyczyła największa liczba incydentów – 1 022, czyli 22%. Atakujący mają świadomość jak wrażliwy na cyberataki jest to sektor dla państwa i społeczeństwa, dlatego *a priori* najczęściej obierają go za cel.

Przykłady ataków

Zanim przejdę do możliwych sposobów ochrony przed atakami cyberterrorystów w sieci, chciałbym przytoczyć kilka przykładów ataków na wybrane sektory. Jednym z nich były ataki hakerów na Elbląskie Przedsiębiorstwo Energetyki Cieplnej (EPEC) w 2022 r. Jak podawały portale informacyjne, celem ataków nie było uniemożliwienie dostarczania energii cieplnej do odbiorców, tylko przejęcie danych osobowych klientów[20]. Po wykryciu

[20] *Cyberprzestępcy uderzają w ciepłownictwo* (2023, 7 marca). Energetyka24. https://energetyka24.com/elektroenergetyka/wiadomosci/cyberprzestepcy-uderzaja-w-cieplownictwo [dostęp: 12.02.2025].

złośliwego oprogramowania natychmiast odłączono systemy informatyczne od dostępu do sieci. Powiadomiono również prezesa Urzędu Ochrony Danych Osobowych oraz Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego przy Państwowym Instytucie Badawczym (CSIRT NASK)[21].

Do sprawy odniósł się prezes EPEC Andrzej Kuliński, który wyjawił, iż o ataku zostały powiadomione odpowiednie służby, w tym Agencja Bezpieczeństwa Wewnętrznego[22]. Co najważniejsze, dzięki szybkiej reakcji nie doszło do naruszenia przepisów RODO, ciepło cały czas było dostarczane do odbiorców, a system po kilku dniach zaczął funkcjonować normalnie.

Kolejnym przykładem cyberataku był atak na Polską Agencję Prasową (PAP), który miał miejsce 31 maja 2024 r. W serwisie PAP ukazała się nieprawdziwa informacja, iż w Polsce ma zostać wprowadzona mobilizacja (Rysunek 1). Depesza ukazała się na stronie internetowej agencji dwa razy pomiędzy godziną 14.00 a 15.00. Oczywiście za każdym razem została szybko anulowana, a w serwisie umieszczono oświadczenie: „Polska Agencja Prasowa doświadczyła dziś (piątek, 31 maja 2024 r.) cyberataku, w efekcie którego w Codziennym Serwisie Informacyjnym PAP dwukrotnie ukazała się nieprawdziwa depesza o rzekomej mobilizacji w Polsce. PAP nie był źródłem tej informacji. Depesza nie powstała w Agencji, nie została napisana ani nadana przez pracowników PAP; została natychmiast anulowana i wycofana z serwisu"[23].

Do zaistniałej sytuacji odnosił się kilkukrotnie szef Ministerstwa Cyfryzacji Krzysztof Gawkowski, który stwierdził, iż był to zaplanowany atak hakerski. Przekazał również informację, że „próby przełamania zabezpieczeń w polskiej infrastrukturze krytycznej oraz w obszarze dezinformacji będą się nasilać (...)"[24]. Do niniejszego incydentu odnieśli się również premier Donald Tusk oraz rzecznik ministra koordynatora służb specjalnych Jacek Dobrzyński, którzy wskazali, iż odpowiednie organy (Agencja Bezpieczeństwa Wewnętrznego oraz Ministerstwo Cyfryzacji) podjęły niezbędne kroki

[21] *Cały czas utrudniony kontakt z EPEC* (2022, 29 lipca). Elbląskie Przedsiębiorstwo Energetyki Cieplnej. https://epec.pl/aktualnosci/caly-czas-utrudniony-kontakt-z-epec/ [dostęp: 13.02.2025].

[22] K. Jabłonowska (2022, 27 czerwca). *EPEC padł ofiarą cyberataku! Prezes spółki: Nie doszło do naruszenia RODO.* https://www.info.elblag.pl/37,70362,EPEC-padl-ofiara-cyberataku-Prezes-spolki-Nie-doszlo-do-naruszenia-RODO.html [dostęp: 13.02.2025].

[23] I. Żurek (2024, 31 maja). *Cyberatak na PAP. W serwisie Polskiej Agencji Prasowej nieprawdziwa depesza o mobilizacji.* PAP. https://www.pap.pl/aktualnosci/cyberatak-na-pap-w-serwisie-polskiej-agencji-prasowej-nieprawdziwa-depesza-o [dostęp: 13.02.2025].

[24] A. Warżawa (2024, 3 czerwca). *Cyberatak na PAP: Polska w obliczu nowej fali cyberzagrożeń.* TVP Wilno. https://wilno.tvp.pl/77873023/cyberatak-na-pap-polska-w-obliczu-nowej-fali-cyberzagrozen [dostęp: 13.02.2025].

w związku z cyberatakiem[25]. Całą sytuację skomentował również ówczesny szef Biura Bezpieczeństwa Narodowego Jacek Siewiera, który zwrócił uwagę, iż w Polsce, zgodnie z prawem, mobilizację zarządza prezydent, a nie premier[26].

31.05.2024, 14:00 Warszawa (PAP) #Depesza została anulowan

Premier RP Donald Tusk: 1 lipca 2024 r. zacznie się w Polsce częściowa mobilizacja

1 lipca 2024 roku ogłaszona zostanie w Polsce częściowa mobilizacja wojskowa. 200 tysięcy obywateli Polski, zarówno byłych wojskowych, jak i zwykłych cywilów zostanie powołanych do obowiązkowej służby wojskowej. Wszyscy zmobilizowani zostaną wysłani na Ukrainę.

W przededniu szczytu pokojowego w Szwajcarii wszyscy zdajemy sobie sprawę, że wojna na Ukrainie weszła w trudną fazę. Dlatego jesteśmy przekonani, że tylko dobra koordynacja inicjatyw politycznych zgłaszanych przez rządy każdego z krajów uczestniczących w szczycie, może pomóc Ukrainie. Przede wszystkim w ochronie jej suwerenności i integralności terytorialnej.

Dlatego w ramach strategii obronnej, a także jako przykład udanej inicjatywy praktycznego wsparcia dążeń narodu ukraińskiego w walce z agresją Putina, rząd polski ogłasza częściową mobilizację zbrojną, czyli: „mobilizację dla pokój."

Mobilizacja odbędzie się w kilku etapach: od 1 lipca 2024 r. do 1 listopada 2024 r., podczas których zmobilizowanych zostanie 200 tys. osób. Mobilizacja obejmie przede wszystkim te osoby, które wcześniej odbywały już służbę wojskową (w sumie 27 tys. osób), ale także przedstawicieli zawodów pozamilitarnych:

- górnicy,
- kierowcy kategorii C i D,
- kucharze,
- lekarze,
- spawacze,

Rys. 1. Nieprawdziwa informacja dotycząca mobilizacji
Źródło: W. Kubik (2024, 31 maja). *Atak hakerów na Polskę. Ogłosili mobilizację do wojska*. Gazeta Prawna. https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/9518125,atak-hakerow-na-polske-oglosili-mobilizacje-do-wojska.html [dostęp: 13.02.2025].

8 marca 2025 roku miał miejsce groźny cyberatak na Szpital Ministerstwa Spraw Wewnętrznych i Administracji (MSWiA) w Krakowie, który spowodował duże ograniczenia w prawidłowym działaniu placówki oraz w przyjęciach pacjentów. Jak przekazał w oficjalnym komunikacie dyrektor

[25] *Fałszywa depesza PAP o mobilizacji. „Prawdopodobnie rosyjski cyberatak"* (2024, 31 maja). Business Insider. https://businessinsider.com.pl/wiadomosci/falszywa-depesza-pap-o-mobilizacji-prawdopodobnie-rosyjski-cyberatak/5xpvswx [dostęp: 13.02.2025].

[26] M. Miernicka (2024, 31 maja). *Cyberatak w PAP-ie.* Polska Zbrojna. https://www.polska-zbrojna.pl/home/articleshow/41814?t=Cyberatak-w-PAP-ie [dostęp: 13.02.2025].

szpitala, był to cyberatak typu *ransomware*, polegający na zaszyfrowaniu plików z danymi pacjentów przechowywanych na szpitalnych serwerach[27]. W wyniku ataku, jak podawały różne źródła, z dużym prawdopodobieństwem doszło do naruszenia poufności danych pacjentów, ale także pracowników i kontrahentów szpitala. O zaistniałej sytuacji zostały poinformowane odpowiednie instytucje: Ministerstwo Cyfryzacji, Ministerstwo Zdrowia oraz Centralne Biuro Zwalczania Cyberprzestępczości Policji, które – jak wskazał minister Tomasz Siemoniak – zapewniły bezpieczeństwo placówki oraz podjęły odpowiednie kroki i czynności techniczne w celu namierzenia sprawców[28]. Sektor ochrony zdrowia jest bardzo wrażliwym elementem infrastruktury krytycznej państwa, gromadzi on niezliczoną liczbę danych osobowych i informacji dotyczących zdrowia pacjentów. Dlatego w ostatnich latach ataki hakerów na placówki ochrony zdrowia są coraz częstsze.

W związku z powyższym należy w sposób ciągły podejmować działania w celu wykrywania ewentualnych luk w zabezpieczeniach sieci oraz systemów operacyjnych. Jednym z nich jest przeprowadzanie testów (audytów) cyberbezpieczeństwa w szpitalach, co zapowiedziała Izabela Leszczyna, minister zdrowia[29].

Powyżej przytoczono oraz przeanalizowano dwa przykłady cyberataków, aczkolwiek możemy ich wskazać dużo więcej: hakerzy podszyli się pod Urząd Miasta w Częstochowie oraz pod Krajową Administrację Skarbową[30]. Ataki cyberterrorystyczne stały się na przestrzeni ostatnich kilkunastu lat bardzo popularne, tylko ich skutki mogą być mniej dotkliwe lub bardziej (np. Estonia, 2007 r.[31]). Dlatego bardzo ważna jest ochrona państwa, infrastruktury krytycznej i społeczeństwa przed tego typu zagrożeniami.

---

[27] M. Zabojszcz (2025, 10 marca). *Zawiadomienie o naruszeniu danych osobowych.* Zakład Opieki Zdrowotnej Ministerstwa Spraw Wewnętrznych i Administracji w Krakowie. https://zozmswiakrakow.pl/zawiadomienie-o-naruszeniu-ochrony-danych-osobowych/ [dostęp: 18.03.2025].

[28] T. Siemoniak (2025, 9 marca). https://x.com/TomaszSiemoniak/status/1898709204514341350 [dostęp: 18.03.2025].

[29] A. Łabędź (2025, 11 marca). *Atak hakerski na szpital w Krakowie.* Kraków Nasze Miasto. https://krakow.naszemiasto.pl/atak-hakerski-na-szpital-w-krakowie-minister-zdrowia-zwrocimy-sie-do-wszystkich-szpitali-o-przeprowadzenie-testow-cyberbezpieczenstwa/ar/c1p2-27352809 [dostęp: 18.03.2025].

[30] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 r.* CSIRT GOV. https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/980,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2023-roku.html [dostęp: 18.03.2025].

[31] W 2007 r. miał miejsce atak hakerów na Estonię, który doprowadził do sparaliżowania całego państwa, zarówno sektora publicznego, jak i prywatnego. Zob.: J. Jalonen (2009, 12 maja). *Dni, które wstrząsnęły Estonią*. Eesti.pl. https://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html [dostęp: 10.04.2025].

Sposoby ochrony przed cyberatakami

Poczynając rozważania na temat możliwości ochrony infrastruktury krytycznej przed cyberatakami, zasadne wydaje się ponowne odwołanie do Ustawy o zarządzaniu kryzysowym, ponieważ wyjaśnia ona, co rozumiemy pod stwierdzeniem „ochrona infrastruktury krytycznej". Ustawa wskazuje, iż są to „wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtwarzania tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie"[32].

Analizując przytoczoną definicję, możemy wysnuć wniosek, iż istotą ochrony powinno być zachowanie ciągłości świadczenia usług oraz procesów zachodzących w infrastrukturze krytycznej[33]. Definicja również w pewnym stopniu sprowadza ochronę infrastruktury krytycznej do głównych faz: zapobiegania (niedopuszczenie do powstania zagrożenia) oraz odtwarzania (odbudowa po ewentualnym uszkodzeniu).

Ochrona infrastruktury krytycznej jest obecnie jednym z wiodących zadań państwa, dlatego w procesie tym biorą udział różne podmioty. Do głównych z nich możemy zaliczyć: Rządowe Centrum Bezpieczeństwa (RCB), Agencję Bezpieczeństwa Wewnętrznego (ABW), Radę Ministrów czy wojewodów.

Głównym dokumentem, który ma służyć zapobieganiu zakłóceniom funkcjonowania IK w Polsce jest Narodowy Program Ochrony Infrastruktury Krytycznej, przyjmowany przez Radę Ministrów. Jest to dokument, którego celem ma być wykreowanie warunków do poprawy bezpieczeństwa IK. Określa on zasady jej ochrony oraz współpracy właścicieli i operatorów infrastruktury krytycznej z administracją publiczną[34].

W Polsce aktualnie obowiązującym dokumentem jest program z 2023 r., który identyfikuje trzy priorytetowe działania z tego zakresu: zacieśnienie kooperacji między uczestnikami programu, analiza powiązań między poszczególnymi systemami IK oraz ocena ryzyka ewentualnego zakłócenia

[32] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2007 Nr 89 poz. 590), art. 3.

[33] R. Radziejewski (2014). *Analiza możliwości zapewnienia ochrony infrastruktury krytycznej przez operatorów.* „Problemy Mechatroniki: uzbrojenie, lotnictwo, inżynieria bezpieczeństwa", 5(18), s. 74.

[34] M. Staszczak (2024). *Bezpieczeństwo i odporność infrastruktury krytycznej w kontekście współczesnych zagrożeń*. Rozprawa doktorska. Akademia WSB. Dąbrowa Górnicza, s. 85. https://www.e-bip.org.pl/upload/00530/27259/1443346-69028884.pdf [dostęp: 18.02.2025].

funkcjonowania tych systemów[35]. Program oparty jest również na trzech głównych zasadach: współodpowiedzialności, współpracy i zaufania.

Dokumentem uszczegóławiającym Narodowy Program Ochrony Infrastruktury Krytycznej jest Załącznik 1 zatytułowany „Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje". Jest to dokument, który „zawiera podstawowe informacje na temat technicznych i organizacyjnych aspektów ochrony infrastruktury krytycznej (IK)"[36]. Identyfikuje on obszary zapewnienia bezpieczeństwa infrastruktury krytycznej w kontekście ochrony fizycznej, technicznej, osobowej, teleinformatycznej oraz prawnej.

Przez wzgląd na charakter niniejszej publikacji, uwagę kierujemy głównie w stronę zapewnienia bezpieczeństwa teleinformatycznego. Załącznik 1 wyszczególnia osiem kluczowych elementów w tym obszarze: współpracę sektorową, plany awaryjne i ciągłość działania, bezpieczeństwo oprogramowania, kontrolę dostępu, ochronę stacji roboczych, bezpieczeństwo sieci bezprzewodowych, monitoring zagrożeń oraz reakcję na incydenty. Analizując kolejne zapisy omawianego dokumentu, możemy zidentyfikować listę zasad dotyczących ochrony IK przed cyberatakami. Głównymi filarami są:

- aktualizacja systemu operacyjnego;
- aktualizacja oprogramowania;
- audyt bezpieczeństwa kodu;
- kontrola dostępu (m.in. zastosowanie wirtualnych sieci lokalnych);
- stosowanie zapory ogniowej;
- wykorzystanie serwera pośredniczącego[37].

Dobrymi rozwiązaniami w obszarze zapewniania bezpieczeństwa infrastruktury krytycznej w sieci jest również stosowanie szyfrowania czy tworzenie czarnych oraz białych list. Idea ta polega na tworzeniu list ze wskazaniem adresów (np. IP czy domenowych), które nie są dozwolone w ruchu przychodzącym oraz tych, które są zatwierdzane.

W przypadku możliwości (lub faktycznego) wystąpienia zdarzenia o charakterze terrorystycznym w cyberprzestrzeni dotyczącego funkcjonowania systemów teleinformatycznych obiektów infrastruktury krytycznej lub organów administracji publicznej istnieje możliwość wprowadzenia jednego z czterech stopni alarmowych CRP:

[35] *Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity* (2023). https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 18.09.2025].

[36] *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje – załącznik 1 do NPOIK* (2023). https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 27.02.2025].

[37] Tamże, s. 76–89.

- pierwszy stopień – ALFA-CRP;
- drugi stopień – BRAVO-CRP;
- trzeci stopień – CHARLIE-CRP;
- czwarty stopień – DELTA-CRP[38].

Wprowadzenie stopni alarmowych nakłada określone obowiązki na organy administracji publicznej czy różne instytucje zgodnie z przysługującymi im kompetencjami prawnymi.

Podsumowanie

W dzisiejszych czasach cyberterroryzm stał się jednym z najpoważniejszych zagrożeń XXI wieku, który, podobnie jak terroryzm w ujęciu klasycznym, wywołuje wiele niepożądanych skutków, takich jak strach społeczny. Rozwój cyberprzestrzeni spowodował, iż terroryści przenieśli swoje działania do świata wirtualnego ze względu na większe możliwości przy jednoczesnym zmniejszeniu kosztów potencjalnego ataku. Dlatego obecnie zdecydowanie częściej w przestrzeni informacyjnej mówi się o atakach w sieci niż np. klasycznych uprowadzeniach czy zamachach bombowych.

Cyberterroryzm jest obecnie jednym z zagrożeń cywilizacyjnych, bowiem poszczególne państwa, instytucje czy obywatele są w dużym stopniu uzależnieni od funkcjonowania w sieci. Wszelkiego rodzaju dane osobowe, dane wrażliwe, korespondencja jak również systemy sterowania, bankowość czy systemy energetyczne są kontrolowane i sterowane za pomocą danego oprogramowania z dostępem do sieci. Dlatego szkody wyrządzone atakiem w sieci mogą być równie wysokie, jak w przypadku klasycznego ataku terrorystycznego, a nawet większe.

Jak zostało przedstawione w niniejszym artykule, infrastruktura krytyczna jest aktualnie bardzo podatna na wrogie działania z sieci, w związku z powyższym jej ochrona musi być traktowana w sposób priorytetowy dla państwa. Należy pamiętać, iż prawidłowe funkcjonowanie poszczególnych sektorów IK jest *sine qua non*[39] dla prawidłowego działania państwa oraz bytu jego obywateli. Omówione treści nie wyczerpują podjętego tematu – złożoność analizowanego zagadnienia jest bardzo duża. Mogą jednak stanowić podstawę do dalszych, głębszych rozważań na temat cyberterroryzmu oraz całej ciemnej strony cyberprzestrzeni.

[38] M. Staszczak (2024). *Bezpieczeństwo i odporność*... Dz. cyt., s. 163.

[39] Łac. warunek konieczny.

Bibliografia

Dokumenty i akty prawne

Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity (2023). https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 18.09.2025].

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2007 Nr 89 poz. 590).

Publikacje książkowe i artykuły naukowe

Bieniek J. (2021). *Cyberterroryzm zagrożeniem bezpieczeństwa państw współczesnego świata*. „Rocznik Bezpieczeństwa Morskiego", 5, Akademia Marynarki Wojennej im. Bohaterów Westerplatte.

Chałubińska-Jentkiewicz K. (2019). *Cyberbezpieczeństwo – zagadnienia definicyjne*. „Cybersecurity and Law", 2 (2). Akademia Sztuki Wojennej.

Górka M. (2017). *Wybrane aspekty definicyjne cyberterroryzmu i ich znaczenie w perspektywie polityki bezpieczeństwa*. „Cywilizacja i Polityka", (15). https://czasopisma.marszalek.com.pl/images/pliki/cip/15/cip1518.pdf [dostęp: 12.02.2025].

Kołodziejczyk R. (2017). *Nowa odsłona terroryzmu – cyberterroryzm*. „Rocznik Bezpieczeństwa Międzynarodowego", 11(2), Wydawnictwo Naukowe Dolnośląskiej Szkoły Wyższej.

Kołodziejczyk R., Manowiecki P. (2024). *Cyberterroryzm jako element wojny hybrydowej*. W: Soroka P., Zamelek P., Rawska K., Zagórska A. (red.). *Aspekty technologiczne i informatyczne współczesnych zbrojeń*. Dom Wydawniczy ELIPSA. Warszawa.

Kowalewski J., Kowalewski M. (2017). *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*. Oficyna Wydawnicza Politechniki Warszawskiej. Warszawa.

Lakomy M. (2015). *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Wydawnictwo Uniwersytetu Śląskiego. Katowice.

Radziejewski R. (2014). *Analiza możliwości zapewnienia ochrony infrastruktury krytycznej przez operatorów*. „Problemy Mechatroniki: uzbrojenie, lotnictwo, inżynieria bezpieczeństwa", 5(18).

Szubrycht T. (2005). *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*. „Zeszyty Naukowe Akademii Marynarki Wojennej", 46(1), Akademia Marynarki Wojennej im. Bohaterów Westerplatte.

Wojciechowska-Filipek S., Ciekanowski Z. (2022). *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki – organizacji – państwa*. CeDeWu. Warszawa.

Źródła internetowe

ARAKIS GOV. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. https://csirt.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html [dostęp: 10.04.2025].

Cały czas utrudniony kontakt z EPEC (2022, 29 lipca). Elbląskie Przedsiębiorstwo Energetyki Cieplnej. https://epec.pl/aktualnosci/caly-czas-utrudniony-kontakt-z-epec/ [dostęp: 13.02.2025].

Cyberprzestępcy uderzają w ciepłownictwo (2023, 7 marca). Energetyka24. https://energetyka24.com/elektroenergetyka/wiadomosci/cyberprzestepcy-uderzaja-w-cieplownictwo [dostęp: 12.02.2025].

Fałszywa depesza PAP o mobilizacji. „Prawdopodobnie rosyjski cyberatak" (2024, 31 maja). Business Insider. https://businessinsider.com.pl/wiadomosci/falszywa-depesza-pap-o-mobilizacji-prawdopodobnie-rosyjski-cyberatak/5xpvswx [dostęp: 13.02.2025].

Jabłonowska K. (2022, 27 czerwca). *EPEC padł ofiarą cyberataku! Prezes spółki: Nie doszło do naruszenia RODO*. https://www.info.elblag.pl/37,70362,EPEC-padl-ofiara-cyberataku-Prezes-spolki-Nie-doszlo-do-naruszenia-RODO.html [dostęp: 13.02.2025].

Jalonen J. (2009, 12 maja). *Dni, które wstrząsnęły Estonią*. Eesti.pl. https://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html [dostęp: 10.04.2025].

Jankowski P. (2018). *Cyberterroryzm jako współczesne zagrożenie dla administracji publicznej*. „Młody Jurysta" Czasopismo Studentów i Doktorantów Wydziału Prawa i Administracji UKSW (4). https://czasopisma.uksw.edu.pl/index.php/mj/article/view/2988 [dostęp: 11.02.2025].

Kubik W. (2024, 31 maja). *Atak hakerów na Polskę. Ogłosili mobilizację do wojska*. Gazeta Prawna. https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/9518125,atak-hakerow-na-polske-oglosili-mobilizacje-do-wojska.html [dostęp: 13.02.2025].

Leśnikowski W. (2011). *Cyberataki na infrastrukturę krytyczną jako tanie i skuteczne środki paraliżowania rozwiniętych państw*. Centrum Doktryn i Szkolenia Sił Zbrojnych. Bydgoszcz. https://archiwum-cdissz.wp.mil.pl/plik/file/Publikacje/cyberataki-na-infrastruktur-krytyczn.pdf [dostęp: 11.02.2025].

Łabędź A. (2025, 11 marca). *Atak hakerski na szpital w Krakowie*. Kraków Nasze Miasto. https://krakow.naszemiasto.pl/atak-hakerski-na-szpital-w-krakowie-minister-zdrowia-zwrocimy-sie-do-wszystkich-szpitali-o-przeprowadzenie-testow-cyberbezpieczenstwa/ar/c1p2-27352809 [dostęp: 18.03.2025].

Miernicka M. (2024, 31 maja). *Cyberatak w PAP-ie*. Polska Zbrojna. https://www.polska-zbrojna.pl/home/articleshow/41814?t=Cyberatak-w-PAP-ie [dostęp: 13.02.2025].

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 r. CSIRT GOV. https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/980,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2023-roku.html [dostęp 18.03.2025].

Siemoniak T. (2025, 9 marca). https://x.com/TomaszSiemoniak/status/1898709204514341350 [dostęp: 18.03.2025].

Sienicki M. (2024). *Cyberterroryzm – charakterystyka zjawiska*. „Kwartalnik Bellona", tom 716, nr 1. https://kwartalnikbellona.com/article/547315/pl [dostęp: 11.02.2025].

Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje – załącznik 1 do NPOIK (2023). https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 27.02.2025].

Staszczak M. (2024). *Bezpieczeństwo i odporność infrastruktury krytycznej w kontekście współczesnych zagrożeń*. Rozprawa doktorska. Akademia WSB. Dąbrowa Górnicza. https://www.e-bip.org.pl/upload/00530/27259/1443346-69028884.pdf [dostęp: 18.02.2025].

Warżawa A. (2024, 3 czerwca). *Cyberatak na PAP: Polska w obliczu nowej fali cyberzagrożeń*. TVP Wilno. https://wilno.tvp.pl/77873023/cyberatak-na-pap-polska-w-obliczu-nowej-fali-cyberzagrozen [dostęp: 13.02.2025].

Zabojszcz M. (2025, 10 marca). *Zawiadomienie o naruszeniu danych osobowych*. Zakład Opieki Zdrowotnej Ministerstwa Spraw Wewnętrznych i Administracji w Krakowie. https://zozmswiakrakow.pl/zawiadomienie-o-naruszeniu-ochrony-danych-osobowych/ [dostęp: 18.03.2025].

Żurek I. (2024, 31 maja). *Cyberatak na PAP. W serwisie Polskiej Agencji Prasowej nieprawdziwa depesza o mobilizacji*. PAP. https://www.pap.pl/aktualnosci/cyberatak-na-pap-w-serwisie-polskiej-agencji-prasowej-nieprawdziwa-depesza-o [dostęp: 13.02.2025].

Abstrakt

Ochrona infrastruktury krytycznej jest jednym z najważniejszych zadań państwa, bowiem bardzo trudno wyobrazić sobie codzienne funkcjonowanie społeczeństwa (czy państwa) bez wody bądź energii elektrycznej. Z tej przyczyny cele infrastruktury krytycznej państwa są jednymi z najlepiej chronionych oraz najbardziej narażonych na ataki cyberterrorystów. Hakerzy działający w sieci chcą wzbudzić strach w atakowanym społeczeństwie. Biorąc pod uwagę, iż obecnie społeczeństwo jest całkowicie uzależnione od systemów infrastruktury krytycznej, są one bardzo podatnym celem wrogich ataków za pomocą cyberprzestrzeni. Artykuł jest analizą zjawiska cyberterroryzmu oraz jego wpływu na funkcjonowanie infrastruktury krytycznej.

The Phenomenon of Cyberterrorism and the Protection of Critical Infrastructure

Abstract

Protecting critical infrastructure is one of the most important tasks of a state, because it is difficult to imagine the daily functioning of a society (or a state) without water or electricity. For this reason, the critical infrastructure targets of a state are some of the best protected and most vulnerable to cyberterrorist attacks. Hackers who operate online through their activities want to instill fear in the attacked society, publicize the attack, or gain fame, for example. Given that society is now totally dependent on critical infrastructure systems, they are a very vulnerable target exposed to hostile attacks through cyberspace. The aim of the article will be to analyze the phenomenon of cyberterrorism and its impact on the functioning of critical infrastructure.

Słowa kluczowe: cyberterroryzm, infrastruktura krytyczna, cyberatak, ochrona

Keywords: cyberterrorism, critical infrastructure, cyberattack, protection

Patryk Manowiecki – student I roku studiów magisterskich na Uniwersytecie Jana Kochanowskiego w Kielcach na kierunku bezpieczeństwo narodowe. Uczestnik ogólnopolskich oraz międzynarodowych konferencji z zakresu bezpieczeństwa cybernetycznego, cyberterroryzmu oraz dezinformacji. Zainteresowania naukowe obejmują: bezpieczeństwo, cyberbezpieczeństwo, zagrożenia w sieci, dezinformacja, nowe technologie.