s. 97–113

PRAWO W DZIAŁANIU
SPRAWY KARNE
53/2023
DOI: 10.32041/pwd.5306

Dominika Skoczylas

Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe

Cyberthreats in cyberspace. Cybercrime, cyberterrorism and network incidents

Abstract

Nowadays, taking into account the number of Internet users, as well as the increasing use of ICT solutions in public administration, we are dealing with the intensification of cyberthreats, which take the form of cybercrimes, cyberterrorism or network incidents.
The aim of the article is to characterize the threats occurring in cyberspace. The subject of the study covers the classification of cybercriminal and cyberterrostic threats, including their criminalization. In addition, due to the variety of cyberthreats, aspects of the national cybersecurity system related to incident handling and the implementation of cybersecurity policy is presented.
The analysis of the issues will allow to answer the following questions: are we dealing with the intensification of cyberthreats today, and if so, are they homogeneous or diverse? Whether the only solution in the fight against cyberthreats is to penalise them? and what factors should be taken into account in order to minimise the negative effects of cyberthreats?
The study will discuss issues related to the systematics of network threats in the framework of cyberterrorism, cybercrime and network incidents. The adopted research methods include the analysis of basic legal acts and the literature on the subject.

Keywords: *cybersecurity, cybercrime, cyberterrorism, network incidents*

Dr Dominika Skoczylas jest adiunktem na Wydziale Prawa i Administracji Uniwersytetu Szczecińskiego, Polska, ORCID: 0000-0003-1231-8078, e-mail: dominika.skoczylas@usz.edu.pl
Data zgłoszenia tekstu przez autora: 23.02.2022 r.; data zaakceptowania do publikacji: 22.08.2022 r.

Streszczenie

Współcześnie, uwzględniając liczbę użytkowników internetu, a także coraz większe zastosowanie rozwiązań teleinformatycznych w administracji publicznej, mamy do czynienia z intensyfikacją cyberzagrożeń, które przybierają postać cyberprzestępstw, cyberterroryzmu czy incydentów sieciowych.

Celem artykułu jest ukazanie zagrożeń występujących w cyberprzestrzeni. Przedmiot badania obejmuje klasyfikację zagrożeń o cyberprzestępczym i cyberterrostycznym charakterze, w tym ich penalizację. Ponadto, ze względu na różnorodność cyberzagrożeń, przedstawione zostaną zadania krajowego systemu cyberbezpieczeństwa związane z obsługą incydentów oraz wdrożeniem polityki cyberbezpieczeństwa.

Analiza zagadnień pozwoli odpowiedzieć na następujące pytania: czy współcześnie mamy do czynienia z intensyfikacją cyberzagrożeń, a jeżeli tak, to czy są one jednorodne czy różnorodne? czy jedynym rozwiązaniem w walce z cyberzagrożeniami jest ich penalizacja? oraz jakie czynniki należy wziąć pod uwagę w celu zminimalizowania negatywnych skutków cyberzagrożeń?

W opracowaniu zostaną omówione zagadnienia odnoszące się do systematyki zagrożeń sieci w ramach cyberterroryzmu, cyberprzestępczości i incydentów sieciowych. Przyjęte metody badawcze obejmują analizę podstawowych aktów prawnych oraz literatury przedmiotu.

Słowa kluczowe: *cyberbezpieczeństwo, cyberprzestępczość, cyberterroryzm, incydenty sieciowe*

1. Wstęp

Nowoczesne technologie informacyjno-komunikacyjne umożliwiają stałą komunikację i wymianę danych bez jednoczesnej obecności stron (na odległość). Obecnie rynek teleinformatyczny bierze pod uwagę potrzeby tzw. społeczeństwa informacyjnego. W następstwie tego powszechne stało się korzystanie zarówno z e-usług, jak i e-informacji oraz gromadzenie, upowszechnianie, uzupełnianie, aktualizowanie czy przekazywanie danych. Informacja elektroniczna okazała się produktem, którego jednakże nie można traktować w oderwaniu od poszanowania i ochrony jawności, prywatności danych szczególnie chronionych[1]. Dynamizm procesów związanych z informatyzacją i cyfryzacją wynika przede wszystkim z globalizacji oraz e-rozwoju gospodarki i społeczeństwa. Aleksandra Monarcha-Matlak wskazuje, że „intensywne wdrażanie nowych technologii informatycznych jako narzędzi komunikacji elektronicznej będzie pociągało za sobą zmiany w strukturach państwa i sposobach jego funkcjonowania"[2]. W ślad za autorką należy dodać, że globalny rozwój nowych technologii wpłynął nie tylko na zmiany w administracji publicznej (e-administracja, digitalizacja dokumentacji), ale również na organizację przedsiębiorstw i zachowania użytkowników końcowych.

Współcześnie uwarunkowania rozwoju państwa i społeczeństwa to interoperacyjność, cyfrowość oraz transgraniczność. Wskazane czynniki bezpośrednio przekładają się na wzrost wirtualnej mobilności oraz uszczegółowienie technologiczne (polegające m.in. na rozwijaniu technologii cyfrowych nowej generacji, np. sztucznej inteligencji). Jednocześnie to właśnie cyberbezpieczeństwo stanowi globalne dobro publiczne. Kluczowe jest zatem zapewnienie ochrony przed cyberzagrożeniami. W tym celu potrzebna staje się zarówno penalizacja, jak i typizacja destrukcyjnych zachowań w cyberprzestrzeni, a także wdrożenie tzw. polityk cyberbezpieczeństwa[3].

2. Społeczeństwo informacyjne. Analiza danych statystycznych

Według raportu Głównego Urzędu Statystycznego (dalej GUS) z 2021 r.[4] społeczeństwo informacyjne w Polsce zyskuje na znaczeniu. Warto porównać dane z 2021 r. i 2018 r. Zgodnie z raportem GUS z 2021 r. odsetek osób korzystających z internetu wyniósł 88,9%, natomiast dostęp do internetu posiadało 92,4% gospodarstw

[1] M. Gołka, *Czym jest społeczeństwo informacyjne?*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2005/67(4), s. 254.

[2] A. Monarcha-Matlak, *Pojęcie komunikacji elektronicznej w doktrynie i aktach prawnych*, „Lingwistyka Stosowana. Applied Linguistics. Angewandte Linguistik" 2017/24, s. 143.

[3] D. Skoczylas, *Interoperacyjność, cyfrowość, transgraniczność technologii informacyjno-komunikacyjnych jako determinanty zrównoważonego rozwoju w XXI wieku*, [w:] *Zrównoważony rozwój i europejski zielony ład wektorami na drodze doskonalenia warsztatu naukowca*, red. M. Staniszewski, H.E. Kretek, Gliwice 2021, s. 238.

[4] *Wykorzystanie technologii informacyjno-komunikacyjnych w przedsiębiorstwach i gospodarstwach domowych: Badanie współfinansowane przez Unię Europejską*, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/wykorzystanie-technologii-informacyjno-komunikacyjnych-w-jednostkach-administracji-publicznej-przedsiebiorstwach-i-gospodarstwach-domowych-w-2021-roku,3,20.html# (dostęp: 20.02.2022 r.).

domowych. Dane z 2018 r.[5] wskazują, że odsetek osób korzystających z internetu znajdował się na poziomie 77,5%, zaś odsetek gospodarstw domowych z dostępem do internetu wynosił 84,2%.

Warto odnotować, że z biegiem czasu zmienił się cel zastosowania narzędzi teleinformatycznych. Polega on już nie tylko na komunikacji międzyludzkiej, lecz także na handlu elektronicznym i elektronicznej administracji publicznej. Szczególną rolę środków komunikacji elektronicznej można zauważyć zwłaszcza wtedy, gdy niemożliwe bądź utrudnione jest korzystanie z tradycyjnych form wymiany informacji czy świadczenia usług. Modelowy przykład stanowi okres pandemii COVID-19, kiedy to większość (o ile nie wszystkie) aktywności związane z życiem prywatnym i publicznym przeniosły się do cyberprzestrzeni. Z jednej strony pandemia była (jest) źródłem kryzysu funkcjonowania państwa i obywateli, z drugiej strony może stanowić (stanowi) impuls do wprowadzenia efektywnych rozwiązań w celu zminimalizowania negatywnych skutków kryzysu. Paulina Szyja zaznacza, że administracja publiczna jest wówczas zobligowana do podjęcia stosownych działań w oparciu m.in. o „implementację dobrych praktyk, w takich obszarach jak: zarządzanie zasobami ludzkimi, obsługa klienta, komunikacja na linii władze krajowe i obywatele”[6]. Nie dziwi zatem fakt, że w czasie pandemii COVID-19 środki komunikacji elektronicznej stanowiły często jedyną formę kontaktu ze światem zewnętrznym. Warto wspomnieć chociażby o *e-learningu*, e-administracji, pracy zdalnej czy telemedycynie.

Niestety nagła, nierzadko również nieprzemyślana, reakcja organów administracji publicznej w kontekście wykorzystania technologii informacyjno-komunikacyjnych w skali makro może mieć wpływ na intensyfikację cyberzagrożeń. Zasadniczo zagrożenia cyberbezpieczeństwa dzieli się na dwie grupy. Pierwsza dotyczy odporności systemów i narzędzi teleinformatycznych (odporności cybernetycznej), druga odnosi się do bezpieczeństwa użytkowników sieci[7]. Szczególnie niebezpieczne są cyberzagrożenia o cyberprzestępczym i cyberterrorystycznym charakterze. Co więcej, bardzo często użytkownik internetu nie zdaje sobie sprawy z tego, że wykonując określone ruchy w sieci, staje się ofiarą przestępstwa. Mając na uwadze powyższe, niezbędne jest stworzenie optymalnych, a jednocześnie skutecznych regulacji prawnych, uwzględniających aktualny rozwój technologiczny, potrzeby społeczeństwa informacyjnego i różnorodność ataków cybernetycznych.

Narzędzia teleinformatyczne wspomagają realizację zadań publicznych i świadczenie usług, umożliwiają odbiór komunikatu przez co do zasady nieograniczony krąg odbiorców w dowolnym miejscu i czasie. Jako atuty należy tu wskazać powszechny i względnie tani dostęp do internetu oraz szerokie możliwości jego zastosowania,

[5] *Raport Głównego Urzędu Statystycznego, Społeczeństwo informacyjne w Polsce w 2018 roku*, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2018-roku,2,8.html (dostęp: 20.02.2022 r.).

[6] P. Szyja, *Funkcjonowanie administracji publicznej w sytuacji kryzysu spowodowanego czynnikami zewnętrznymi – studium przypadku COVID-19*, „Rocznik Administracji Publicznej” 2020/6, https://doi.org/10.4467/24497800RAP.20.015.12909, s. 268.

[7] J. Groenendaal, I. Helsloot, *Cyber resilience during the COVID-19 pandemic crisis: A case study*, „Journal of Contingencies and Crisis Management” 2021/29(4), https://doi.org/10.1111/1468-5973.12360, s. 439–440.

zwłaszcza w takich sektorach jak: ochrona zdrowia, transport, handel, transakcje elektroniczne, administracja publiczna, gospodarka i finanse, bankowość[8]. Dodatkowe zalety to wielozadaniowość i współzależność środowiska wirtualnego oraz szczegółowość i aktualność danych przekazywanych przez środki komunikacji elektronicznej[9].

W raporcie GUS z 2019 r., obok informacji dotyczącej liczby osób korzystających z usług administracji publicznej za pomocą internetu (40,4%), można znaleźć interesujące dane związane z tzw. ryzykiem przetwarzania danych. Z raportu wynika, że wzrasta świadomość ryzyka przetwarzania danych w systemach teleinformatycznych oraz bezpieczeństwa infrastruktury teleinformatycznej. W tym celu w 2019 r. odnotowano wzrost użycia tzw. środków zabezpieczających sieć przed incydentami sieciowymi, zagrożeniami cyberterrorystycznymi i przestępstwami sieciowymi. Najczęściej stosowanymi środkami zabezpieczającymi w 2019 r. były bieżące aktualizacje oprogramowania i uwierzytelnianie silnym hasłem (80,8% i 76,4%)[10]. Obecnie, ze względu na stały wzrost liczby użytkowników internetu, równomiernie rośnie także liczba zagrożeń prawidłowego funkcjonowania cyberprzestrzeni. Uwzględniając skutki prawne cyberzagrożeń, wyróżnić należy cyberprzestępstwa, cyberterroryzm oraz incydenty sieciowe. Według badań przeprowadzonych w 2021 r. do najczęściej występujących zagrożeń użytkowników indywidualnych należą: nieuprawnione użycie karty kredytowej lub debetowej przez obcą osobę; utrata dokumentów, zdjęć lub innych danych z powodu wirusa lub innego złośliwego oprogramowania; niewłaściwe wykorzystanie informacji osobowych dostępnych w internecie; włamanie na konto e-mail lub konto w serwisie społecznościowym i udostępnienie jego zawartości bez wiedzy właściciela; kradzież tożsamości internetowej; fałszywe wiadomości e-mail mające na celu wyłudzanie danych; przekierowywanie na fałszywe strony internetowe wyłudzające dane osobowe; kontakt dzieci z nieodpowiednimi treściami w internecie[11].

Z kolei Interpol wskazuje, że cyberataki szczególnie nasiliły się w okresie pandemii COVID-19. Co więcej, cyberzagrożenia stale ewoluują, dostosowują się do aktualnych warunków społecznych, gospodarczych i politycznych. W trakcie pandemii pojawiły się m.in. opracowane ze złośliwym oprogramowaniem domeny zarejestrowane z kluczem słowa „COVID" czy „*corona*". Nastąpił również wzrost oszust internetowych i zjawiska *phishingu* (fałszywe strony internetowe związane

[8] M. Ganczar, *Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców*, Warszawa 2009, s. 21–22.

[9] E. Badzińska, *Technologie informacyjno-komunikacyjne w środowisku wirtualnym*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2014/809, „Ekonomiczne Problemy Usług" 113/2 („Ekonomiczno-społeczne i techniczne wartości w gospodarce opartej na wiedzy"), s. 167–168.

[10] *Raport Głównego Urzędu Statystycznego, Społeczeństwo informacyjne w Polsce w 2019 roku*, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2019-roku,2,9.html (dostęp: 20.02.2022 r.).

[11] *Wykorzystanie technologii informacyjno-komunikacyjnych w przedsiębiorstwach i gospodarstwach domowych: Badanie współfinansowane przez Unię Europejską*, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/wykorzystanie-technologii-informacyjno-komunikacyjnych-w-jednostkach-administracji-publicznej-przedsiebiorstwach-i-gospodarstwach-domowych-w-2021-roku,3,20.html# (dostęp: 20.02.2022 r.).

z COVID-19, wyposażone w linki *phishingowe*). Ponadto zauważono intensyfikację złośliwych oprogramowań gromadzących dane, takich jak trojan zdalnego dostępu czy *spyware*, oraz destrukcyjnych złośliwych oprogramowań (*ransomware* i DDoS). Te ostatnie były szczególnie niebezpieczne dla infrastruktury krytycznej i instytucji reagowania (np. szpitale i centra medyczne). Interpol wskazał też na luki w zabezpieczeniach systemów, sieci, cyberzagrożenia związane z użytkowaniem aplikacji przez organy administracji publicznej, instytucje publiczne i innych użytkowników sieci[12]. Powyższe potwierdza to, że wraz z rozwojem technologii informacyjno-komunikacyjnych wzrasta częstotliwość cyberataków o różnorodnym charakterze. Niepokojące jest zaś przede wszystkim to, że cyberataki powodują nie tylko przerwanie ciągłości świadczenia e-usług, ale są szczególnie niebezpieczne dla użytkowników sieci (zjawisko cyberprzestępczości i cyberterroryzmu).

3. Cyberzagrożenia, incydenty sieciowe, cyberbezpieczeństwo. Definicje, rodzaje cyberataków, penalizacja cyberprzestępstw

Definicję legalną cyberprzestrzeni określa m.in. ustawa o stanie wyjątkowym[13] i wskazuje wprost, że jest to „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami”[14]. Z treści definicji wynika, że cyberprzestrzeń tworzą dwa komponenty: informacja oraz systemy teleinformatyczne. Istnieje zatem potrzeba „ochrony treści informacji i metod jej przesyłu, rejestrowania, generowania i magazynowania”[15]. Należy jednocześnie odnotować, że ustawodawca nie zdecydował się na zdefiniowanie pojęcia cyberprzestrzeni w ustawie o krajowym systemie cyberbezpieczeństwa[16].

Bezpieczeństwo cyberprzestrzeni należy rozpatrywać przez pryzmat: strategicznych zasobów kraju; przetwarzania informacji w sposób aktualny, dokładny i wiarygodny, niezakłócony działaniem osób trzecich; funkcjonowania sieci teleinformatycznych i infrastruktury krytycznej; ochrony informacji niejawnych oraz ustawowo chronionych; prawa do prywatności. Ustalenie zagrożenia nie jest wcale łatwe, gdyż najczęściej ataki te są anonimowe, a wskazanie faktycznej lokalizacji miejsca i osoby, która go dokonała, wymaga przeprowadzenia dodatkowych czynności[17].

---

[12] *Global Landscape on Covid-19. Cyberthreat*, https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats (dostęp: 20.02.2022 r.).
[13] Ustawa z 21.06.2002 r. o stanie wyjątkowym (tekst jedn.: Dz.U. z 2017 r. poz. 1928).
[14] Artykuł 2 ust. 1a ustawy o stanie wyjątkowym.
[15] J. Taczkowska-Olszewska, K. Chałubińska-Jentkiewicz, M. Nowikowska, *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019, s. 4–5.
[16] Ustawa z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jedn.: Dz.U. z 2020 r. poz. 1369 ze zm.) – dalej u.k.s.c.
[17] T.R. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego” 2016/15(8), s. 12–13.

Ataki skierowane przeciwko systemom teleinformatycznym mają nie tylko wymiar *stricte* technologiczny, ale przede wszystkim naruszają sferę wolności korzystania z internetu czy dostępu do danych przetwarzanych w sieci.

Cyberbezpieczeństwo jest szczególnym typem bezpieczeństwa, pojmowanego przez pryzmat porządku i ładu struktur umieszczonych w cyberprzestrzeni. W zależności od przyjęcia określonego katalogu zadań i czynności realizowanych w cyberprzestrzeni można wyróżnić podstawowy zakres cyberbezpieczeństwa, czyli:

- bezpieczeństwo e-informacji, rozumiane również jako zachowanie integralności, dostępności i poufności danych zgromadzonych w systemach teleinformatycznych,
- ochronę danych osobowych i prywatności,
- ochronę infrastruktury krytycznej państwa, serwerów i systemów przed atakiem cyberterrorystycznym,
- utrzymanie zasobów informacyjnych i osiągnięcie odpowiednich celów informacyjnych, zachowanie ciągłości połączeń, nieprzerwanego świadczenia e-usług[18].

Z uwagi na powyższe, aby ustalić przeciwdziałanie zagrożeniom powstającym w cyberprzestrzeni, kluczowe będzie określenie, jakiego typu zjawiska o charakterze cyberterrorystycznym i cyberprzestępczym mogą mieć miejsce w internecie. W przypadku cyberataków o charakterze terrorystycznym istotne jest kryterium celu. Terror w cyberprzestrzeni wymaga zaangażowania systemów teleinformatycznych, za pomocą których następuje atak albo które stają się przedmiotem ataku (np. cyberatak na infrastrukturę krytyczną państwa)[19]. Ponadto, aby czyn został sklasyfikowany jako przestępstwo o charakterze terrorystycznym, muszą zostać spełnione przesłanki z art. 115 § 20 Kodeksu karnego[20]. Oprócz aktywizmu (niedestrukcyjnej działalności polegającej np. na wysyłaniu dużej ilości informacji na skrzynki elektroniczne użytkowników) czy haktywizmu (wykorzystywaniu metod hakerskich w celu zakłócenia funkcjonowania stron, bez poważnych konsekwencji, np. blokowanie witryn rządowych)[21] należy wymienić – najgroźniejszy – cyberterroryzm. Definicyjny zakres cyberterroryzmu obejmuje wszelkiego rodzaju politycznie umotywowane ataki z wykorzystywaniem sieci teleinformatycznych w celu zniszczenia bądź ograniczenia prawidłowego działania systemów i infrastruktury informacyjnej. Niestety, w związku z nieustającym rozwojem technologii informacyjno-komunikacyjnych, wzrasta również skala ataków, które często są trudne do wcześniejszego zidentyfikowania.

[18] T. Hoffmann, *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań 2018, s. 19–20.
[19] M. Skolimowski, *Polityka cyberbezpieczeństwa w świetle zagrożenia cyberterroryzmem*, [w:] *Internet. Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017, s. 107.
[20] Zgodnie z art. 115 § 20 ustawy z 6.06.1997 r. – Kodeks karny (tekst jedn.: Dz.U. z 2022 r. poz. 1138 ze zm.; dalej k.k.) przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu: poważnego zastraszenia wielu osób, zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu.
[21] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010, s. 64–66.

Ich skutki bywają natomiast wysoce szkodliwe dla całościowego działania sieci. Trudności wykrycia ataków terrorystycznych wynikają głównie z tego, że ich przeprowadzenie jest nieograniczone ze względu na czas i miejsce. Ponadto charakteryzuje się wysokim stopniem anonimowości, szerokim obszarem oddziaływania, potencjalną łatwością wykonania (wystarczy odpowiedni sprzęt i umiejętności) – przy założeniu minimalnych kosztów związanych z ich wykonaniem[22].

Obok działań typowo terrorystycznych (cyberterroryzmu) powszechna stała się cyberinwigilacja (kontrolowanie społeczeństwa przez sieci teleinformatyczne, głównie w państwach o systemie totalitarnym i autorytarnym), a także cyberprzestępczość (działania kryminalne mające miejsce w cyberprzestrzeni, np. działanie przestępczości zorganizowanej, grup mafijnych). Zauważa się również pojęcie cyberwojny (prowadzenie działań wojennych w internecie). Najczęściej na atak narażone są elementy infrastruktury krytycznej, np. sektor bankowy, finansowy, transportowy czy energetyczny. Cyberterroryści koncentrują się też na uzyskaniu dostępu do danych osobowych czy informacji publicznych, w szczególności niejawnych, posiadających klauzule: tajne lub ściśle tajne. Współczesne ataki cyberterrorystyczne nie ograniczają się jedynie do wykorzystywania złośliwych oprogramowań (wirusów, bakterii czy robaków) bądź koni trojańskich, ale dotyczą takich zdarzeń jak chociażby: *spoofing* (podszywanie się pod konkretnego użytkownika w celu zakłócenia systemu), *hijacking* (przejęcie transmisji połączeń międzystemowych), *sniffing* (lokalizowanie ruchu w sieci, poprzez przechwytywanie danych i ich późniejsze zapisywanie w celu ponownego przetworzenia i wykorzystania danych, haseł systemowych)[23].

Analiza ataków cybernetycznych nakazuje spojrzeć na owe zagadnienie pod kątem skali i rodzaju zagrożeń prawidłowego funkcjonowania sieci. W XXI w. miały miejsce liczne zdarzenia zmierzające bezpośrednio do ograniczenia bądź zaprzestania działania systemów, łamania zabezpieczeń lub kodów, szyfrowania, nielegalnego przejęcia w celu kopiowania, zmiany czy usuwania danych. Jako przykłady można podać ataki o znaczeniu historycznym, takie jak:

a) Estonia, 2007 r. – szereg cyberataków skierowanych na infrastrukturę informatyczną; zaatakowano głównie strony rządowe, m.in. parlamentu, ministerstw obrony i sprawiedliwości, policji, oraz sektor prywatny, m.in. bankowy, a także uniemożliwiono działanie portalu dziennika *Postimees*; inicjatorami ataku, stanowiącego odpowiedź na przeniesienie pomnika upamiętniającego sowieckich żołnierzy (Brązowego Żołnierza), byli prawdopodobnie rosyjscy hakerzy; cybernetyczna wojna estońsko-rosyjska trwała 3 tygodnie;
b) Gruzja, Rosja, 2008 r. – atak cybernetyczny na gruzińskie witryny najważniejszych organów władzy publicznej, w tym prezydenta Micheila Saakaszwiliego; blokada

[22] M. Łapczyński, *Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*, „Pulaski Policy Papers. Komentarz Międzynarodowy Pułaskiego" 2009/7, s. 2, https://pulaski.pl/wp-content/uploads/2015/02/Pulaski_Policy_Papers_No_7_09.pdf (dostęp: 21.02.2022 r.).
[23] K. Bielski, *Cyberterroryzm – nowe zagrożenie bezpieczeństwa państwa w XXI wieku*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego, Acta Politica" 2015/4(34), s. 98–99.

portali naukowych, informacyjnych i rządowych wymusiła wykorzystanie serwerów znajdujących się w Polsce, Estonii czy na Ukrainie[24];

c) Polska, 2012 r. – atak skierowany przeciwko systemom teleinformatycznym instytucji publicznych, m.in. Ministerstwa Obrony Narodowej czy Żandarmerii Wojskowej, spowodował zablokowanie świadczenia usług informacyjnych; odnotowano również znaczne przeciążenie serwerów instytucji państwowych (zablokowanie ciągłości usług w wyniku zmasowanego wysyłania pytań na skrzynki pocztowe organów)[25].

Obecnie zauważa się wzrost liczby cyberataków w sektorze administracji publicznej, bankowości i finansów, ochrony zdrowia, transportu publicznego, a także w sektorze usług prywatnych. Intensywnie atakowana jest cyberprzestrzeń krajów Europy (w tym krajów Europy Środkowo-Wschodniej) oraz Stanów Zjednoczonych Ameryki Północnej czy krajów azjatyckich. Jako przykłady można tu wymienić:

a) marzec 2020 r. – cyberatak na sieć hoteli *Marriott*; szacuje się, że zostały ujawnione dane 5,2 miliona gości hotelowych[26];
b) marzec 2021 r. – grupa o nazwie „*Ghostwriter*" przeprowadziła atak za pomocą tzw. *phishingu*; w ten sposób uzyskała dostęp do kont polityków Bundestagu[27];
c) maj 2021 r. – cyberatak z użyciem *ransomware* na największego operatora rurociągów z paliwami w USA (sektor naftowy – spółka *Colonial Pipeline*)[28];
d) 2022 r. – wzmożona liczba cyberataków na cyberprzestrzeń Ukrainy; ataki polegały na umieszczaniu na stronach (głównie rządowych) nieprawdziwych komunikatów w języku ukraińskim, rosyjskim i polskim (styczeń 2022 r.), a także na blokowaniu dostępu do ukraińskich witryn (atak typu DDoS – blokada serwera, polegająca na przeciążeniu sieci – luty 2022 r.)[29].

Bezpieczeństwo cyberprzestrzeni jest zagadnieniem niezwykle istotnym z punktu widzenia użytkowników oraz organów władzy publicznej. Prawidłowe funkcjonowanie infrastruktury telekomunikacyjnej, ciągłe świadczenie e-usług i wymiana e-informacji to kluczowe elementy, a zarazem podstawowe standardy bezpieczeństwa teleinformatycznego. Dlatego też nie dziwi to, że ustawodawca wprowadza szereg aktów prawnych, w których określa zasady komunikacji elektronicznej, obejmujące kwestie bezpieczeństwa i odpowiedzialności karnej. Należy zgodzić się ze stanowiskiem

---

[24] S. Wierzbicki, *Wojny cybernetyczne jako element niekonwencjonalnej konfrontacji międzypaństwowej. Pragmatyczna rzeczywistość, nieunikniona przyszłość*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2015/2(1), s. 141–143.

[25] A. Rolbiecka, *Cyberterrozyzm w Polsce*, s. 3, http://www.knbm.amw.gdynia.pl/wp-content/uploads/2014/12/Rolbiecka-Agnieszka-Cyberterroryzm-w-Polsce.pdf (dostęp: 21.02.2022 r.).

[26] Ł. Siwek, *Najgroźniejsze ataki hakerskie i największe wycieki danych w 2020 r.*, https://www.vida.pl/najgroszniejsze-ataki-hakerskie-i-najwieksze-wycieki-danych-w-2020-r/ (dostęp: 21.02.2022 r.).

[27] *Kolejny, przypuszczalnie rosyjski, cyberatak na posłów Bundestagu*, https://www.dw.com/pl/kolejny-przypuszczalnie-rosyjski-cyberatak-na-pos%C5%82%C3%B3w-bundestagu/a-57019102 (dostęp: 21.02.2022 r.).

[28] D. Sierakowska, *Cyberatak na kluczowy rurociąg z paliwem w USA*, https://www.pb.pl/cyberatak-na-kluczowy-rurociag-z-paliwem-w-usa-1116048 (dostęp: 21.02.2022 r.).

[29] *Cyberataki na Ukrainę. Ekspert: ich celem jest wywołanie paraliżu decyzyjnego*, https://www.polskieradio24.pl/5/1223/Artykul/2902870,Cyberataki-na-Ukraine-Ekspert-ich-celem-jest-wywolanie-paralizu-decyzyjnego (dostęp: 21.02.2022 r.).

wyrażonym przez Sąd Najwyższy, który wskazuje, że „Internet, choć jest przestrzenią wirtualną, to ma charakter miejsca publicznego", „nie ma wątpliwości, co do tego, że przy wykorzystaniu przestrzeni Internetu można popełnić zarówno przestępstwo, jak i wykroczenie, o czym świadczą zresztą różne postaci czynów (…)"[30].

Kodeks karny koncentruje się głównie na penalizacji cyberprzestępstw, takich jak: *hacking*, tj. nieuprawniony dostęp do informacji (art. 267 § 1 k.k.), *sniffing*, tj. nieuprawniony dostęp do całości lub części systemu informatycznego (art. 267 § 2 k.k.), niszczenie informacji (art. 268 § 2 k.k.), sabotaż komputerowy (art. 269 § 1 k.k.), zakłócenie pracy w sieci (art. 269a k.k.), oszustwo komputerowe (art. 287 k.k.). Można stwierdzić, że ustawodawca, penalizując wyżej opisane czyny, wprowadza pewnego rodzaju „politykę cyberbezpieczeństwa" o charakterze typowo sankcyjnym. Tak rozumiana polityka musi uwzględniać to, że „w systemie komputerowym mogą znajdować się dowody na działalność przestępczą"[31]. Tym samym nowe technologie mogą być zarówno narzędziem ataku, jak i jego przedmiotem. Na aprobatę zasługuje stosunkowo surowa penalizacja przestępstw komputerowych, np. przestępstwo polegające na oszustwie komputerowym podlega karze pozbawienia wolności od 3 miesięcy do lat 5 (art. 287 § 1 k.k.).

Cyberterroryści i cyberprzestępcy dokonują zorganizowanych i indywidualnych ataków przy wykorzystaniu sieci teleinformatycznych głównie po to, aby włamać się do komputerów czy systemów, wykorzystać programy w celu przechwytywania haseł dostępu, wykraść dane szczególnie chronione i informacje niejawne, uniemożliwić działanie infrastruktury krytycznej[32]. Pośrednio przepisy Kodeksu karnego odnoszą się do penalizacji czynów obejmujących ataki cyberterrorystów, np. art. 258 § 2 k.k. stanowi, że ten, kto bierze udział w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa o charakterze terrorystycznym (w tym w ramach cyberterroryzmu), podlega karze pozbawienia wolności od 6 miesięcy do lat 8. Efektem ataku cybernetycznego może być również wykorzystywanie sieci teleinformatycznych i bezpośrednie ingerowanie w prawidłowe działanie poszczególnych sektorów usług, w tym usług kluczowych, np. transportu. Czynności tego typu mogą spowodować zagrożenie bezpieczeństwa w sferze komunikacji, a nawet życia i zdrowia ludzi (np. art. 165 § 1 pkt 4 k.k.).

E-przestępczość przyjmuje najczęściej postać nieautoryzowanego dostępu do systemu komputerowego (*hacking*), naruszenia tajemnicy komunikacji (podsłuchy komputerowe), dostępu do informacji i integralności danych czy całego systemu teleinformatycznego (komputerowego). Jednakże obok przestępstw obejmujących *stricte* nadużycia komputerowe wyróżnia się takie, w których narzędzia teleinformatyczne są elementem umożliwiającym popełnienie przestępstwa innego typu. Wystarczy wspomnieć o nielegalnych transakcjach internetowych (których efektem

[30] Postanowienie Sądu Najwyższego z 17.04.2018 r., IV KK 296/17, OSP 2019/2, poz. 15.
[31] K. Witek, *Przestępczość komputerowa – aspekty prawne*, „Edukacja – Technika – Informatyka" 2018/2(24), https://doi.org/10.15584/eti.2018.2.4, s. 40.
[32] M. Czyżak, *Wybrane aspekty zjawiska cyberterroryzmu*, „Telekomunikacja i Techniki Informacyjne" 2010/1–2, s. 48.

może być chociażby wyłudzanie świadczeń płatniczych), oszustwach dotyczących fikcyjnych opłat elektronicznych, wyprowadzaniu środków finansowych czy nawet kradzieży tożsamości[33].

Wzmożona aktywność cyberprzestępców przejawia się również w *stalkingu*, czyli uporczywym nękaniu osoby, które narusza prywatność jednostki, wzbudzając w niej uzasadnione uczucie strachu. *Stalking* najczęściej ma na celu wykorzystywanie wizerunku lub innych danych osobowych w celu wyrządzenia szkody majątkowej lub osobistej. Konsekwencją takich nielegalnych zachowań cyberprzestępców może być nawet targnięcie się pokrzywdzonego na własne życie[34]. Idealne środowisko do popełnienia tego czynu stanowi cyberprzestrzeń. Przekonanie o anonimowości zachowań wzbudza po stronie sprawcy poczucie braku karalności za dokonanie przestępstwa *stalkingu*, który bardzo często przybiera formy brutalnego ataku słownego. Jak słusznie zauważa Marta Staręga, „ukształtowany współcześnie styl życia wyzwala w społeczeństwie ujemne wartości (...) zjawisko, jakim jest *stalking*, czyli uporczywe nękanie, jest w Polsce bardzo rozpowszechnione i wiąże się ściśle z gwałtownym rozwojem «nowoczesności»"[35].

Cyberprzestępczość ma wiele twarzy, albowiem oprócz przestępstw o charakterze finansowym, gospodarczym czy dotyczących dóbr osobistych każdego człowieka cyberatak może zostać skierowany również w dzieci. Internet stanowi doskonały obszar nadużyć seksualnych w ramach tzw. *groomingu*. Jest nim produkowanie lub utrwalanie treści pornograficznych za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej z zamiarem nawiązania kontaktu z małoletnim poniżej lat 15. Sprawca ma na celu spotkanie z nim lub złożenie mu propozycji obcowania płciowego, poddania się lub wykonania innej czynności seksualnej albo udziału w produkowaniu lub utrwalaniu treści pornograficznych i zmierza do realizacji tego celu[36]. Najczęściej tzw. przestępstwo uwodzenia dzieci poprzez kontakt internetowy stwarza pedofilom doskonałe warunki działania, gdyż zapewnia stosunkowo dużą anonimowość i potencjalne osiągnięcie zamierzonego celu (w szczególności w młodszej grupie wiekowej). Penalizacja tego typu czynów w Kodeksie karnym wzmacnia poczucie bezpieczeństwa najmłodszych użytkowników internetu, bo obejmuje ich szeroką ochroną prawną. Aspekt prawny wydaje się jednak niewystarczający, jeżeli opieka sprawowana przez rodziców czy opiekunów nie będzie na tyle odpowiednia, aby ustrzec dzieci przed niebezpiecznymi zachowaniami w sieci[37]. Wypada jednocześnie podkreślić, że „osoba, która, uznając, iż doszło do naruszenia jej praw poprzez rozpowszechnianie w Internecie dyskredytujących ją wypowiedzi, (…) może żądać przed sądami każdego państwa członkowskiego na terytorium, którego wypowiedzi

[33] D. Jagiełło, *Karnoprawne ramy odpowiedzialności za przestępstwa popełnianie w cyberprzestrzeni*, [w:] *Cyberbezpieczeństwo. Zarys wykładu,* red. C. Banasiński, Warszawa 2018, s. 459–461.
[34] Zob. art. 190a § 1–3 k.k.
[35] M. Staręga, *Stalking jako nowy czyn zabroniony w polskim kodeksie karnym. Aspekt prawny oraz znaczenie społeczne,* „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria: Administracja i Zarządzanie" 2012/94, s. 200.
[36] Zob. art 200a k.k.
[37] M. Szczepaniec, *Komputer jako narzędzie przestępstwa*, „Zeszyty Prawnicze" 2012/12(2), s. 172–173.

te są lub były dostępne, naprawienia szkody i krzywdy wyrządzonych na terytorium państwa członkowskiego siedziby sądu, do którego wniesiono powództwo, nawet jeśli sądy te nie są właściwe do rozpoznania żądania sprostowania i usunięcia"[38].

Oprócz prawnokarnej ochrony cyberbezpieczeństwa w zakresie przestępstw popełnianych w sieci bądź przy użyciu nowoczesnych technologii informacyjno-komunikacyjnych należy odwołać się do przepisów ustawy o krajowym systemie cyberbezpieczeństwa. Przedmiotowa ustawa *stricte* określa organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, w tym sposób sprawowania nadzoru i kontroli co do przestrzegania przepisów ustawy (art. 1 ust. 1 u.k.s.c.).

Krajowy system cyberbezpieczeństwa różnicuje zakres cyberbezpieczeństwa (czyli odporności systemów informacyjnych na działania uniemożliwiające zachowanie poufności, integralności, dostępności i autentyczności przetwarzanych danych i związanych z nimi usług[39]) od zdarzenia tzw. incydentu[40]. Incydenty mogą spowodować znaczną szkodę np. dla bezpieczeństwa lub porządku publicznego czy praw i wolności obywatelskich (incydent krytyczny – art. 2 pkt 6 u.k.s.c.), obniżyć jakość lub przerwać ciągłość świadczenia usługi kluczowej (incydent poważny – art. 2 pkt 7 u.k.s.c.), mieć istotny wpływ na świadczenie usługi cyfrowej (incydent istotny – art. 2 pkt 8 u.k.s.c.) czy spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego (incydent w podmiocie publicznym – art. 2 pkt 9 u.k.s.c.). Fundamentem zrównoważonego podejścia do ochrony cyberprzestrzeni jest zarówno obsługa incydentów, jak i wskazanie odpowiedniej polityki cyberbezpieczeństwa. W przypadku infrastruktury krytycznej, świadczenia usług kluczowych i usług cyfrowych niebezpieczeństwo, podobnie jak dla indywidualnych użytkowników, stanowią zagrożenia o cyberprzestępczym czy cyberterrorystycznym charakterze.

Krajowe polityki cyberbezpieczeństwa, co ciekawe, posiadają szczególny wydźwięk globalny, ponieważ zagrożenia cyberprzestrzeni mają również charakter transgraniczny. Dlatego też organy władzy publicznej, określając zasady cyberbezpieczeństwa, powinny uwzględniać konieczność inwestycji w systemy ochrony cyberprzestrzeni (również w ramach kompetencji cyfrowych), skoordynować działania w zakresie obsługi, zgłoszenia i zarządzania incydentem oraz dążyć do współpracy sektora prywatnego z sektorem państwowym w zakresie odporności cyfrowej[41].

Organizacja obsługi incydentu zapewnia szybką reakcję właściwych podmiotów, tj. Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego, w skład których wchodzą CSIRT GOV, CSIRT MON, CSIRT NASK, a także operatorzy usług kluczowych i usług cyfrowych[42]. W przypadku chociażby operatorów usług

[38] Wyrok Trybunału Sprawiedliwości z 21.12.2021 r., C-251/20 (Dz.Urz. UE C 84 z 2022 r., s. 13).
[39] Zob. art. 2 pkt 4 u.k.s.c.
[40] Nie ulega wątpliwości, że incydenty mogą mieć niekorzystny wpływ na cyberbezpieczeństwo (art. 2 pkt 5 u.k.s.c.).
[41] M. Czyżak, *Bezpieczeństwo w cyberprzestrzeni,* „Teka Komisji Prawniczej" 2018/11(2), https://doi.org/10.32084/tekapr.2018.11.2-7, s. 118.
[42] C. Banasiński, W. Nowak, *Europejski i krajowy system cyberbezpieczeństwa*, [w:] *Cyberbezpieczeństwo. Zarys wykładu,* red. C. Banasiński, Warszawa 2018, s. 160–162.

kluczowych (np. w sektorze energii czy transportu) powstaje obowiązek wdrożenia odpowiedniego systemu zarządzania bezpieczeństwem w systemie informacyjnym zapewniającego świadczenie usługi kluczowej poprzez m.in.: utrzymanie i bezpieczną eksploatację systemu informacyjnego; zapewnienie bezpieczeństwa i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej; zarządzanie incydentami; stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej[43].

Biorąc pod uwagę powyższe aspekty (z jednej strony prawnokarne, z drugiej – administracyjnoprawne), związane z zapewnieniem cyberbezpieczeństwa w skali makro, należy zdecydowanie pozytywnie ocenić zasady penalizacji cyberprzestępstw oraz konieczność wdrożenia polityk cyberbezpieczeństwa sieci i systemów. Osiągnięcie celów bezpieczeństwa cybernetycznego nie jest jednak możliwe bez aktualnej analizy i klasyfikacji cyberzagrożeń. W ślad za tym niezbędne jest opracowanie adekwatnych rozwiązań prawnych, uwzględniających prawo unijne, kwestie technologiczne i społeczno-gospodarcze. Aby ocenić szanse i wyzwania skutecznej polityki cyberbezpieczeństwa w skali globalnej, należy wskazać cel takiego działania. Nie obejmuje on wyłącznie obsługi incydentów, które już wystąpiły, ale także wdrożenie odpowiednich środków zapobiegawczych i ochronnych. Kluczowe jest również zaangażowanie wszystkich podmiotów, zarówno tych świadczących e-usługi, jak i z nich korzystających w zakresie ochrony cyberprzestrzeni przed cyberzagrożeniami[44]. Wreszcie trudno sobie wyobrazić brak reakcji ustawodawcy na pojawiające się nowe zagrożenia o cyberprzestępczym czy cyberterrorystycznym charakterze. W tym aspekcie zapewne niezbędna będzie rewizja katalogu e-przestępstw i ich penalizacji, tym bardziej że ofiary cyberprzestępstw to nie tylko dorośli użytkownicy internetu, lecz także dzieci. Ryzyko działań cyberprzestępców związane jest w tym przypadku z brakiem świadomości najmłodszych użytkowników sieci co do tego, jakie zachowania stanowią cyberzagrożenia (e-pedofilia, wyłudzenie danych osobowych, kradzież tożsamości)[45].

Sama penalizacja cyberzagrożeń niestety nie wystarczy. Kluczowe jest określenie i wdrożenie sposobów, tj. metod i technik, zwalczania cyberprzestępczości. Maciej Kiedrowicz wskazuje na pozytywne aspekty identyfikacji osób z wykorzystaniem dokumentów identyfikacyjnych, stosowania systemów biometrycznych, technologii wykorzystującej znaczniki (tagi) umożliwiającej identyfikację obiektów w sieci (etykiety RFID) czy technologii GPS[46]. Przedstawione technologie mogą być pomocne w zidentyfikowaniu sprawcy, a także ofiary cyberataku. W toku

[43] Zob. art. 8 u.k.s.c.
[44] D. Skoczylas, *The Act on the National Cybersecurity System and Other Legal Regulations in the Context of Ensuring State Cybersecurity. Selected Issues*, „Roczniki Nauk Prawnych" 2020/30(2), https://doi.org/10.18290/rnp20302-7, s. 109.
[45] S. Edwards, *Cyber-safety and COVID-19 in the early years: A research agenda,* „Journal of Early Childhood Research" 2021/19(3), https://doi.org/10.1177/1476718X211014908, s. 397.
[46] M. Kiedrowicz, *Wykorzystywanie technologii RFID i GPS do lokalizowania zasobów i osób*, [w:] *Internet. Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017, s. 205–214.

walki z cyberzagrożeniami stanowią również istotne komponenty polityki cyberbezpieczeństwa systemów i sieci, zarówno w obszarze działań prewencyjnych, jak i następczych.

4. Podsumowanie

Reasumując, penalizacja cyberzagrożeń oraz zadania podejmowane przez instytucje publiczne mają wpływ na kwestie cyberbezpieczeństwa. Co istotne, w tym względzie należy wziąć pod uwagę kilka elementów, tj. bezpieczeństwo świadczenia e-usług, infrastruktury krytycznej i użytkowników internetu. Nie można nie zgodzić się z Agnieszką Gryszczyńską, która stwierdza, że „działania przestępców stały się prostsze w miarę postępu technologicznego", „stosowanie technik anonimizacji (…), korzystanie z przejętych serwerów oraz skradzionej tożsamości utrudnia organom ich identyfikację i pociągnięcie do odpowiedzialności karnej"[47].

Jak zostało wskazane, współcześnie mamy do czynienia z intensyfikacją cyberzagrożeń o różnorodnym charakterze (cyberprzestępstwa, cyberterroryzm, incydenty). Konieczna jest w tym przypadku aktualizacja katalogu e-przestępstw, wdrożenie odpowiednich metod i technik zwalczania cyberprzestępczości bądź obsługi incydentów. Warto podkreślić, że wystarczającego zabiegu nie stanowi penalizacja owych czynów (w Kodeksie karnym). Należy również wziąć pod uwagę inne czynniki, które pozwolą zminimalizować negatywne skutki cyberzagrożeń. Dobrą koncepcją jest m.in. stworzenie polityki cyberbezpieczeństwa, określającej odpowiednie środki zapobiegawcze i ochronne, w tym zasady obsługi tzw. incydentów. Ponadto warto opracować adekwatne rozwiązania prawne, uwzględniające prawo unijne, kwestie technologiczne i społeczno-gospodarcze. Nadal najsłabszym ogniwem w świecie nowych technologii jest człowiek. Polityka cyberbezpieczeństwa stanowi kluczowy punkt odniesienia, zarówno dla zasad ochrony cyberprzestrzeni w skali makro, jak i jej bezpiecznego użytkowania przez indywidualnych użytkowników sieci.

Bibliografia

1. Aleksandrowicz T.R., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, Przegląd Bezpieczeństwa Wewnętrznego 2016, nr 15(8).
2. Badzińska E., *Technologie informacyjno-komunikacyjne w środowisku wirtualnym*, Zeszyty Naukowe Uniwersytetu Szczecińskiego 2014, nr 809, Ekonomiczne Problemy Usług, nr 113, Ekonomiczno-społeczne i techniczne wartości w gospodarce opartej na wiedzy, t. 2.
3. Banasiński C., Nowak W., *Europejski i krajowy system cyberbezpieczeństwa*, [w:] *Cyberbezpieczeństwo. Zarys wykładu*, red. C. Banasiński, Warszawa 2018.

[47] A. Gryszczyńska, *Nowe zagrożenia bezpieczeństwa rejestrów publicznych*, [w:] *Internet. Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017, s. 300–301.

4. Bielski K., *Cyberterroryzm – nowe zagrożenie bezpieczeństwa państwa w XXI wieku*, Zeszyty Naukowe Uniwersytetu Szczecińskiego, Acta Politica 2015, t. 34, nr 4, https://doi.org/10.18276/ap.2015.34-06.
5. *Cyberataki na Ukrainę. Ekspert: ich celem jest wywołanie paraliżu decyzyjnego*, https://www.polskieradio24.pl/5/1223/Artykul/2902870,Cyberataki-na-Ukraine-Ekspert-ich-celem-jest-wywolanie-paralizu-decyzyjnego.
6. Czyżak M., *Bezpieczeństwo w cyberprzestrzeni*, Teka Komisji Prawniczej 2018, t. 11, nr 2, https://doi.org/10.32084/tekapr.2018.11.2-7.
7. Czyżak M., *Wybrane aspekty zjawiska cyberterroryzmu*, Telekomunikacja i Techniki Informacyjne 2010, nr 1–2.
8. Edwards S., *Cyber-safety and COVID-19 in the early years: A research agenda*, Journal of Early Childhood Research 2021, t. 19, nr 3, https://doi.org/10.1177/1476718X211014908.
9. Ganczar M., *Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców*, Warszawa 2009.
10. *Global Landscape on Covid-19. Cyberthreat*, https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats.
11. Gołka M., *Czym jest społeczeństwo informacyjne?*, Ruch Prawniczy, Ekonomiczny i Socjologiczny 2005, nr 67, z. 4.
12. Groenendaal J., Helsloot I., *Cyber resilience during the COVID-19 pandemic crisis: A case study*, Journal of Contingencies and Crisis Management 2021, t. 29, nr 4, https://doi.org/10.1111/1468-5973.12360.
13. Gryszczyńska A., *Nowe zagrożenia bezpieczeństwa rejestrów publicznych*, [w:] *Internet. Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017.
14. Hoffmann T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań 2018.
15. Jagiełło D., *Karnoprawne ramy odpowiedzialności za przestępstwa popełnianie w cyberprzestrzeni*, [w:] *Cyberbezpieczeństwo. Zarys wykładu*, red. C. Banasiński, Warszawa 2018.
16. Kiedrowicz M., *Wykorzystywanie technologii RFID i GPS do lokalizowania zasobów i osób*, [w:] *Internet. Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017.
17. *Kolejny, przypuszczalnie rosyjski, cyberatak na posłów Bundestagu*, https://www.dw.com/pl/kolejny-przypuszczalnie-rosyjski-cyberatak-na-pos%C5%82%C3%B3w-bundestagu/a-57019102.
18. Łapczyński M., *Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*, Pulaski Policy Papers. Komentarz Międzynarodowy Pułaskiego 2009, nr 7, https://pulaski.pl/wp-content/uploads/2015/02/Pulaski_Policy_Papers_No_7_09.pdf.
19. Monarcha-Matlak A., *Pojęcie komunikacji elektronicznej w doktrynie i aktach prawnych*, Lingwistyka Stosowana. Applied Linguistics. Angewandte Linguistik 2017, nr 24.
20. *Raport Głównego Urzędu Statystycznego, Społeczeństwo informacyjne w Polsce w 2018 roku*, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-

-społeczenstwo-informacyjne/społeczenstwo-informacyjne/społeczenstwo-informacyjne-w-polsce-w-2018-roku,2,8.html.
21. *Raport Głównego Urzędu Statystycznego, Społeczeństwo informacyjne w Polsce w 2019 roku*, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-społeczenstwo-informacyjne/społeczenstwo-informacyjne/społeczenstwo-informacyjne-w-polsce-w-2019-roku,2,9.html.
22. Rolbiecka A., *Cyberterrozyzm w Polsc*e, http://www.knbm.amw.gdynia.pl/wp-content/uploads/2014/12/Rolbiecka-Agnieszka-Cyberterroryzm-w-Polsce.pdf.
23. Sierakowska D., *Cyberatak na kluczowy rurociąg z paliwem w USA*, https://www.pb.pl/cyberatak-na-kluczowy-rurociag-z-paliwem-w-usa-1116048.
24. Siwek Ł., *Najgroźniejsze ataki hakerskie i największe wycieki danych w 2020 r.*, https://www.vida.pl/najgrozniejsze-ataki-hakerskie-i-najwieksze-wycieki-danych-w-2020-r/.
25. Skoczylas D., *Interoperacyjność, cyfrowość, transgraniczność technologii informacyjno-komunikacyjnych jako determinanty zrównoważonego rozwoju w XXI wieku*, [w:] *Zrównoważony rozwój i europejski zielony ład wektorami na drodze doskonalenia warsztatu naukowca*, red. M. Staniszewski, H.E. Kretek, Gliwice 2021.
26. Skoczylas D., *The Act on the National Cybersecurity System and Other Legal Regulations in the Context of Ensuring State Cybersecurity. Selected Issues*, Roczniki Nauk Prawnych 2020, t. 30, nr 2, https://doi.org/10.18290/rnp20302-7.
27. Skolimowski M., *Polityka cyberbezpieczeństwa w świetle zagrożenia cyberterroryzmem*, [w:] *Internet. Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017.
28. Staręga M., *Stalking jako nowy czyn zabroniony w polskim kodeksie karnym. Aspekt prawny oraz znaczenie społeczne*, Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria: Administracja i Zarządzanie 2012, nr 94.
29. Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.
30. Szczepaniec M., *Komputer jako narzędzie przestępstwa*, Zeszyty Prawnicze 2012, t. 12, nr 2.
31. Szyja P., *Funkcjonowanie administracji publicznej w sytuacji kryzysu spowodowanego czynnikami zewnętrznymi – studium przypadku COVID-19*, Rocznik Administracji Publicznej 2020, nr 6, https://doi.org/10.4467/24497800RAP.20.015.12909.
32. Taczkowska-Olszewska J., Chałubińska-Jentkiewicz K., Nowikowska M., *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019.
33. Wierzbicki S., *Wojny cybernetyczne jako element niekonwencjonalnej konfrontacji międzypaństwowej. Pragmatyczna rzeczywistość, nieunikniona przyszłość*, De Securitate et Defensione. O Bezpieczeństwie i Obronności 2015, nr 2(1).
34. Witek K., *Przestępczość komputerowa – aspekty prawne*, Edukacja – Technika – Informatyka 2018, nr 2(24), https://doi.org/10.15584/eti.2018.2.4.

35. *Wykorzystanie technologii informacyjno-komunikacyjnych w przedsiębiorstwach i gospodarstwach domowych: Badanie współfinansowane przez Unię Europejską*, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/wykorzystanie-technologii-informacyjno-komunikacyjnych-w-jednostkach-administracji-publicznej-przedsiebiorstwach-i-gospodarstwach-domowych-w-2021-roku,3,20.html#.