PRAWO W DZIAŁANIU
SPRAWY KARNE
55/2023
DOI: 10.32041/pwd.5504

s. 72–87

Wojciech Filipkowski

Cyberprzestępstwa o charakterze terrorystycznym w polskim prawie karnym

Cybercrimes of a terrorist character in Polish criminal law

Abstract

The author of the article analyzes the mutual relations between the concepts of cybercrime and cyberterrorism in the context of Polish criminal law, drawing on criminological knowledge. The aim of the study is to describe this problem from a normative perspective and propose appropriate changes in the criminal policy of the Polish legislature. The main subject of the doctrinal research, which is also based on a review of relevant domestic and foreign literature, is the scope of the concept of cybercrime in relation to the fulfillment of the conditions specified in Article 115 § 20 of the Criminal Code, which pertain to terrorist offenses. Based on the conducted research, it has been observed that not all cybercrimes covered by the Polish Criminal Code meet the conditions described in Article 155 § 20 of the Criminal Code and therefore cannot be considered as cyberterrorism. This primarily stems from the formal criterion of a higher penalty, which cannot be lower than 5 years of imprisonment. Therefore, the author suggests abandoning this formal criterion and focusing solely on the intentions of the perpetrator, which may contribute to a greater effectiveness of the criminal policy in combating cyberterrorism.

Keywords: *cyberterrorism, cybercrimes, criminal law*

Streszczenie

Autor artykułu przeprowadza analizę wzajemnych relacji między pojęciami cyberprzestępczości i cyberterroryzmu w kontekście polskiego prawa karnego, korzystając z wiedzy kryminologicznej. Celem opracowania jest opisanie tego problemu z perspektywy normatywnej oraz zaproponowanie odpowiednich zmian w polityce karnej polskiego ustawodawcy. Głównym przedmiotem badań dogmatycznych, opartych również na przeglądzie stosownej literatury krajowej i zagranicznej,

Dr hab. Wojciech Filipkowski, jest profesorem na Uniwersytecie w Białymstoku, Dyrektorem Międzynarodowego Centrum Badań i Ekspertyz Kryminologicznych, Katedra Prawa Karnego i Kryminologii Wydziału Prawa Uniwersytetu w Białymstoku, Polska, ORCID: 0000-0001-6248-0888, e-mail: w.filipkowski@uwb.edu.pl
Data zgłoszenia tekstu przez autora: 18.07.2023 r.; data zaakceptowania do publikacji: 28.08.2023 r.

są zakresy pojęcia „cyberprzestępstwa" w odniesieniu do spełnienia przesłanek określonych w art. 115 § 20 Kodeksu karnego, które dotyczą przestępstw o charakterze terrorystycznym. Na podstawie przeprowadzonych badań stwierdzono, że nie wszystkie cyberprzestępstwa objęte polskim Kodeksem karnym spełniają przesłanki opisane w art. 155 § 20 k.k. i nie można ich zatem uznać za cyberterroryzm. Wynika to przede wszystkim z formalnej przesłanki górnego zagrożenia karą, która nie może być niższa niż 5 lat pozbawienia wolności. W związku z tym autor sugeruje rezygnację z tej formalnej przesłanki i skupienie się wyłącznie na celach sprawcy, co może przyczynić się do większej skuteczności polityki karnej w zwalczaniu cyberterroryzmu.

Słowa kluczowe: *cyberterroryzm, cyberprzestępstwa, prawo karne*

1. Uwagi wstępne

Podstawowym problemem o charakterze teoretycznym i praktycznym jest definicja cyberprzestępstwa i powiązanej z nim cyberprzestępczości[1]. Uwidacznia się tutaj korelacja kategorii pojęciowych z zakresu języka prawniczego (i prawnego) oraz kryminologii[2]. Problem ten wynika z szybkiego rozwoju sieci teleinformatycznych – w tym przede wszystkim internetu – oraz różnorodności oferowanych przez nie usług, które znajdują zastosowanie w rozmaitych obszarach życia społecznego: od jednostek przez ich grupy aż po całe państwa. Analizując zmiany postrzegania i definiowania zachowań w tej przestrzeni, można dojść do wniosku, że mamy do czynienia z ewolucją wszelkiego rodzaju nadużyć z jej wykorzystaniem[3]. Dzieje się tak wraz z każdą nową usługą oferowaną poprzez internet, a wykorzystywaną przez użytkowników za pośrednictwem komputerów, urządzeń mobilnych (także internetu rzeczy – *Internet of Things*[4]), które są podłączone do sieci globalnej, rozległej lub lokalnej. Prowadzi to do chaosu terminologicznego wzmacnianego przez kolejne akty prawne w skali jednego kraju, regionu lub globu, gdyż przygotowane na ich potrzeby definicje dewaluują się z czasem. W związku z tym mamy do czynienia z wieloznacznymi pojęciami „cyberprzestępstwa" i „cyberprzestępczości", które określane są raczej poprzez kazuistyczne wymienienie ich elementów składowych niż poprzez syntetyczną, opisową definicję[5].

Nawiązując do tytułu opracowania, należy zauważyć, że powyższe problemy nakładają się na równie kontrowersyjne pojęcie „terroryzmu". Intuicyjnie można przyjąć, że ich część wspólna prowadzi do pojawienia się i stosowania pojęcia „cyberterroryzmu", który mieści się znaczeniowo w cyberprzestępczości ujmowanej w kategoriach kryminologicznych – jako zjawisko społeczne[6]. Wynika to z tego, że

---

[1] Por. P. Lewulis, *O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych*, „Prokuratura i Prawo" 2021/3, s. 13–14.

[2] S. Ranjan Srivastava, S. Dube, *Cyberattacks, Cybercrime and Cyberterrorism*, [w:] *Handbook of Research on Network Forensics and Analysis Techniques*, red. G. Shrivastava, P. Kumar, B.B. Gupta, S. Bala, N. Dey, Hershey 2018, s. 162 i n., https://doi.org/10.4018/978-1-5225-4100-4.ch010 (dostęp: 18.07.2023 r.).

[3] P. Lewulis, *O rozgraniczeniu…*, s. 21.

[4] Por. D. Evans, *The Internet of Things. How the Next Evolution of the Internet is Changing Everything*, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (dostęp: 18.07.2023 r.); A. Belov, M. Delembovsky, V. Shklyar, *Simulation of cyber threats for the Internet of Things*, „Transfer of Innovative Technologies" 2021/4(1), s. 92 i n., https://doi.org/10.32347/tit2141.0303 (dostęp: 18.07.2023 r.).

[5] P. Lewulis, *O rozgraniczeniu…*, s. 14–16.

[6] Por. S. Woszek, *Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2022/14(27), s. 202–203, https://doi.org/10.4467/20801335PBW.22.056.16947 (dostęp: 18.07.2023 r.); I.G. Seissa, J. Ibrahim, N.-Z. Yahaya, *Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review*, „International Journal of Science and Research" 2017/6(1), s. 180–181, https://doi.org/10.21275/art20163936 (dostęp: 18.07.2023 r.); Ł. Skoneczny, *Rola Agencji Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2009/1, s. 26; C.B. Foltz, *Cyberterrorism, computer crime, and reality*, „Information Management & Computer Security" 2004/12(2), s. 154 i n.; S. Gordon, R. Ford, *Cyberterrorism?*, „Computers & Security" 2002/21(7), s. 636 i n., https://doi.org/10.1016/S0167-4048(02)01116-1 (dostęp: 18.07.2023 r.); D. Denning, *Cyberterrorism, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services*, 23.05.2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (dostęp: 18.07.2023 r.).

nie ma desygnatów terroryzmu, które nie należałyby do zbioru przestępstw[7]. Należy zaznaczyć, że jednocześnie są takie desygnaty pojęcia „terroryzmu", które nie wiążą się z przedrostkiem „cyber-", gdyż są realizowane poza sieciami teleinformatycznymi. Powyżej przytoczone okoliczności czynią przedmiot badań niezwykle interesującym z punktu widzenia teoretycznego. Jednocześnie zdarzenia i trendy, z którymi mamy współcześnie do czynienia, nadają mu wymiar praktyczny[8], chociażby w kwestii kreowania polityki karnej wymierzonej w sprawców przestępstw o charakterze terrorystycznym w cyberprzestrzeni, ale także ustalenia właściwej sytuacji prawnej osoby oskarżonej i skazanej za cyberterroryzm.

Z tego też względu za przedmiot rozważań niniejszego opracowania uczyniono dogmatyczną analizę zakresów desygnatów pojęcia „cyberprzestępstwo" w kontekście spełnienia przez nie przesłanek określonych w art. 115 § 20 Kodeksu karnego[9], czyli przestępstwa o charakterze terrorystycznym[10]. Jest to więc ujęcie normatywne. Zasadnym byłoby oczekiwać, że wszelkie przejawy terroryzmu – w tym też w cyberprzestrzeni[11] – powinny być objęte powyższą definicją ustawową. Pozwala to na prowadzenie krajowej polityki karnej w sposób spójny względem sprawców tego typu zachowań. Postawiono główny teoretyczny problem badawczy: Które z tzw. cyberprzestępstw zamieszczonych w polskim Kodeksie karnym spełniają definicję legalną przestępstwa o charakterze terrorystycznym (art. 115 § 20 k.k.)? Szczegółowe teoretyczne problemy obejmują następujące pytania: Które z czynów zabronionych należą do zakresu pojęciowego cyberprzestępstwa? Jakie są kryteria definicji przestępstwa o charakterze terrorystycznym? Jak należy je interpretować, gdy są realizowane w cyberprzestrzeni?

2. Analiza literatury przedmiotu

Już na początku należy zauważyć, że w obcej literaturze przedmiotu bardzo rzadko zdarzają się analizy o charakterze dogmatycznym, gdzie łącznie prowadzone są rozważania dotyczące obu typów czynów zabronionych[12]. Częściej są to rozważania na temat zjawisk z punktu widzenia kryminologii, nauk o bezpieczeństwie

[7] N. Khaeriah Kadir, Judhariksawan, Maskun, *Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes*, „Fiat Justisia" 2019/13(4), s. 337, https://doi.org/10.25041/fiatjustisia.v13no4.1735 (dostęp: 18.07.2023 r.).

[8] *The European Union Terrorism Situation and Trend Report (TE-SAT)*, EUROPOL 2022, s. 89.

[9] Ustawa z 6.06.1997 r. – Kodeks karny (tekst jedn.: Dz.U. z 2022 r. poz. 1138 ze zm.) – dalej k.k.

[10] Por. M. Smarzewski, *Cyberterroryzm a cyberprzestępstwa o charakterze terrorystycznym*, „Ius Novum" 2017/1, s. 67 i n.; K. Burdziak, *Definicja przestępstwa o charakterze terrorystycznym przewidziana w polskim Kodeksie karnym w świetle rozwiązań Unii Europejskiej, Rady Europy i Organizacji Narodów Zjednoczonych – raport z projektu badawczego*, Warszawa 2021, s. 5 i n.

[11] I.A. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni*, Olsztyn 2017, s. 4 i n.

[12] Por. M. Conway, *What is Cyberterrorism and How Real is the Threat?: A Review of the Academic Literature, 1996–2009*, [w:] *Cyber Behavior: Concepts, Methodologies, Tools, and Applications, Management Association*, Information Resources, Hershey 2014, s. 217 i n., https://doi.org/10.4018/978-1-4666-5942-1 (dostęp: 18.07.2023 r.); S. Khan, T. Saleh, M. Dorasamy, N. Khan, O. Tan Swee Leng, R. Gale Vergara, *A systematic literature review on cybercrime legislation*, „F1000Research" 2022/11:971, https://doi.org/10.12688/f1000research.123098.1 (dostęp: 18.07.2023 r.).

lub informatyki[13]. Skupiają się one jednak na kwestii wykrywania zagrożeń lub ataków (niezależnie od motywacji ich sprawców) i środkach profilaktycznych lub naprawczych. Kwestie polityki prawnokarnej są bardzo rzadko w nich przedstawiane, co wskazuje na jej często marginalne znaczenie w ramach narodowych strategii cyberbezpieczeństwa[14].

Najważniejszym aktem prawa międzynarodowego dotyczącym przestępstw popełnianych w sieci jest Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23.11.2001 r.[15] Ma ona na celu harmonizację krajowych przepisów dotyczących cyberprzestępczości i poprawę współpracy międzynarodowej w zakresie ścigania i dochodzenia tego typu przestępstw. Konwencja nie odnosi się konkretnie do aktów terroru, ale raczej koncentruje się na przestępstwach popełnianych przy użyciu systemów komputerowych[16]. Na pewno jednak nie klasyfikuje tychże przestępstw jako aktów terroru i nie odnosi się wprost do przejawów terroryzmu. Jest to zadanie pozostawione innym aktom prawa międzynarodowego lub krajowego, które definiują typy przestępstw związanych z terroryzmem. Natomiast Protokół dodatkowy do Konwencji Rady Europy o cyberprzestępczości dotyczący penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych, sporządzony w Strasburgu dnia 28.01.2003 r.[17], stanowi nawiązanie do propagandy terrorystycznej realizowanej poprzez sieć internet[18].

Na podstawie przeprowadzonej analizy literatury można dojść do następujących wniosków w kontekście podobieństw i różnic między cyberprzestępczością i cyberterroryzmem[19]. Obydwa zjawiska:

---

[13] Por. M. Kopczewski, *Elementy infrastruktury krytycznej państwa /organizacji/ – jako obiekty narażone na ataki cyberterrorystyczne*, Zakopane 2011, s. 582 i n., http://www.ptzp.org.pl/'les/konferencje/kzz/artyk_pdf_2011/054.pdf (dostęp: 18.07.2023 r.); A. Al Mazari, A.H. Anjariny, S.A. Habib, E. Nyakwende, *Cyber Terrorism Taxonomies: Definition, Targets, Patterns, Risk Factors, and Mitigation Strategies*, „International Journal of Cyber Warfare and Terrorism" 2016/6(1), s. 2 i n., https://doi.org/10.4018/IJCWT.2016010101 (dostęp: 18.07.2023 r.).

[14] Por. M. Mahinderjit Singh, A. Abu Bakar, *A Systemic Cybercrime Stakeholders Architectural Model*, „Procedia Computer Science" 2019/161, s. 1154, https://doi.org/10.1016/j.procs.2019.11.227 (dostęp: 18.07.2023 r.); F.S. Neagu, A. Savu, *The costs of cyberterrorism for the national economy: United States of America vs Egypt*, [w:] *Proceedings of the 13th International Conference on Business Excellence 2019*, s. 991, https://doi.org/10.2478/picbe-2019-0086 (dostęp: 18.07.2023 r.); M. Constantin, A. Bortea, D. Mema, *Risks and Vulnerabilities in Digital Public Services. Threat of Cyberterrorism Vs Romania's Cybersecurity Strategy*, „Holistica – Journal of Business and Public Administration" 2020/11, s. 74 i n.

[15] Dz.U. z 2015 r. poz. 728 – dalej Konwencja o cyberprzestępczości.

[16] M. Samodulska, *Crimes Committed via the Internet – Selected Aspects*, „Teka Komisji Prawniczej" 2014/7, s. 110.

[17] Dz.U. z 2015 r. poz. 730.

[18] Y. Akdeniz, *An Advocacy Handbook for the Non Governmental Organisations, The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems*, 2003, s. 23 i n., https://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf (dostęp: 18.07.2023 r.).

[19] Por. M. Konieczny, *Cyberprzestępczość – krótka historia, współczesne oblicza i trudna do przewidzenia przyszłość*, „Roczniki Administracji i Prawa" 2023/23(1), s. 39, https://doi.org/10.5604/01.3001.0016.3776 (dostęp: 18.07.2023 r.); M. Conway, *What is…*, [w:] *Cyber…*, s. 217 i n.; F.S. Neagu, A. Savu, *The costs…*, [w:] *Proceedings…*, s. 984; M. Constantin, A. Bortea, D. Mema, *Risks…*, s. 74 i n.

1) zachodzą w cyberprzestrzeni i wymagają użycia jakiejś odmiany technologii telekomunikacyjnej;
2) mogą powodować istotne krzywdy i straty w życiu jednostek, organizacji czy też całych gospodarek;
3) wymagają podejmowania daleko idących działań w zakresie przeciwdziałania i zwalczania ich przejawów, m.in. w drodze właściwej polityki cyberbezpieczeństwa i kryminalnej państwa.

W literaturze podkreślana jest jedna podstawowa różnica. Jest nią motywacja sprawców[20]. W przypadku cyberprzestępstw ma ona charakter przede wszystkim ekonomiczny. Natomiast ataki terrorystyczne są motywowane ideologicznie, w tym politycznie czy religijnie. Konstatacja ta jest istotna z punktu widzenia prowadzonych badań.

Powyższe rozważania prowadzą do wniosku, że konieczne jest podjęcie analiz dogmatycznych na temat polskich rozwiązań prawnych na tle zasygnalizowanego w literaturze obcej problemu wzajemnych relacji między cyberprzestępczością a cyberterroryzmem na płaszczyźnie normatywnej. Należy nadmienić, że w literaturze polskiej ostatnie opracowanie dotyczące podobnych problemów badawczych zostało opublikowane przez Marka Smarzewskiego w 2017 r.[21]

3. Zakres czynów zabronionych mieszczących się w pojęciu „cyberprzestępstwo"

Maciej Siwicki i Piotr Lewulis dokonali bardzo szerokiej analizy typologii przestępstw popełnianych z wykorzystaniem komputerów i ich sieci, również tzw. cyberprzestępstw[22]. Zaproponowane tam poglądy należy uznać za wartościowe i zostaną one wykorzystane – oraz rozwinięte w niniejszym opracowaniu – do prowadzenia analiz służących odpowiedzi na pytania badawcze.

Za cyberprzestępstwa M. Siwicki uznał następujące czyny:

- polegające na posługiwaniu się systemami lub sieciami informatycznymi w celu naruszania jakiegokolwiek dobra prawnego chronionego przez prawo karne;
- polegające na zamachach na systemy komputerowe i sieci teleinformatyczne, dane i programy komputerowe (tzw. przestępstwa *stricte* komputerowe lub przeciwko bezpieczeństwu przetwarzania informacji).

Jednocześnie zastrzegł, że cyberprzestępstw nie należy utożsamiać z przestępstwami internetowymi. Wynika to z tego, że te ostatnie dotyczą jedynie tych czynów, które są realizowane w internecie lub poprzez internet. Tym samym to pojęcie mieści się w pierwszym. Stanowi to także potwierdzenie, że definicja ma charakter eklektyczny, składający się z wyraźnych grup czynów. Ponadto do jej opisu użyto

[20] I. Bernik, *Cybercrime and Cyberwarefare*, London 2014, s. 25 i n. oraz 103 i n.
[21] M. Smarzewski, *Cyberterroryzm*…, s. 68 i n.
[22] Por. M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012/7–8, s. 249–251; P. Lewulis, *O rozgraniczeniu*…, s. 19 i n.

pojęć mających swoje definicje legalne, o czym w dalszych częściach opracowania. Jednocześnie brak jest w proponowanym opisie odniesień do motywacji sprawcy jako okoliczności irrelewantnej.

Natomiast P. Lewulis słusznie zauważa, że cyberprzestępstwo to każde z desygnatów znajdujących się w opisywanej przez niego typologii przestępstw komputerowych *sensu largo* (podzielone dychotomicznie na przestępstwa *stricte* komputerowe lub przestępstwa komputerowe), o ile do ich popełnienia wykorzystano sieć teleinformatyczną[23]. W tym podejściu pominięto również kwestię motywacji sprawców.

W literaturze podnosi się także problem definicji cyberprzestrzeni jako pewnej płaszczyzny, na której dokonywane są powyższe czyny zabronione. Nie jest to pojęcie często używane w aktach normatywnych[24]. Natomiast, w przypadku regulacji o charakterze regionalnym, w art. 1 lit. a Konwencji o cyberprzestępczości zdefiniowany został termin „system informatyczny" jako każde urządzenie lub grupa wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych[25]. Nie tylko komputery mogą stanowić element systemów lub sieci, ale także jakiekolwiek urządzenie wykonujące program (lub też kod). Wydaje się, że termin ten jest stosunkowo najszerszy pod względem zakresu pojęciowego w porównaniu z innymi znamionami użytymi chociażby przez krajowego ustawodawcę.

W związku z tym należy wskazać[26], że „systemem informacyjnym" jest zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z 16.07.2004 r. – Prawo telekomunikacyjne[27] wraz z przetwarzanymi w nim danymi w postaci elektronicznej. Definicja ta została odtworzona na podstawie art. 2 pkt 14 ustawy z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa[28] oraz art. 3 pkt 3 ustawy z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[29].

Natomiast „system teleinformatyczny" został opisany w art. 2 pkt 6 ustawy z 5.08.2010 r. o ochronie informacji niejawnych[30] jako system teleinformatyczny

---

[23] P. Lewulis, *O rozgraniczeniu…*, s. 27–28.

[24] Por. J. Worona, *Prace naczelnych organów administracji państwowej a cyberbezpieczeństwo Polski*, „Białostockie Studia Prawnicze" 2016/20, s. 466; M. Kośka, *Cyberterroryzm – zadania antyterrorystyczne Sił Zbrojnych Rzeczypospolitej Polskiej w kontekście obowiązujących aktów prawnych*, „Wiedza Obronna" 2022/279(2), s. 198, https://doi.org/10.34752/2022-j279 (dostęp: 18.07.2023 r.); P. Lewulis, *O rozgraniczeniu…*, s. 23 i 25.

[25] Por. A. Adamski, *Buszujący w sieci. Cybernowelizacja prawa karnego*, „Rzeczpospolita" z 27.10.2003 r.; S. Foldes, *Comments on the notion of information system in the Budapest Convention on Cybercrime, the EU directive, and selected penal codes*, 2017, https://hal.archives-ouvertes.fr/hal-01588889 (dostęp: 18.07.2023 r.).

[26] G. Szpor, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, K. Czaplicki, Warszawa 2019, s. 56–57.

[27] Tekst jedn.: Dz.U. z 2022 r. poz. 1648 ze zm.

[28] Ustawa z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jedn.: Dz.U. z 2023 r. poz. 913).

[29] Ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn.: Dz.U. z 2023 r. poz. 57 ze zm.).

[30] Ustawa z 5.08.2010 r. o ochronie informacji niejawnych (tekst jedn.: Dz.U. z 2023 r. poz. 756 ze zm.).

w rozumieniu art. 2 pkt 3 ustawy z 18.07.2002 r. o świadczeniu usług drogą elektroniczną[31], który to artykuł jest identyczny co do treści z wymienianym wyżej art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

Podsumowując tę część rozważań, należy zauważyć, że „systemem" i „siecią" jest pewien układ urządzeń (określanych w szczególności jako komputer, serwer, urządzenie sieciowe, końcowe) połączonych ze sobą w całość, podporządkowanych realizacji określonego rodzaju usługi lub usług. Pozwala to przyjąć, że „system" jest definiowany przez funkcję, jaką ma realizować. Natomiast użycie pojęcia „sieć" służy podkreśleniu faktu połączenia przewodowo lub bezprzewodowo wielu urządzeń i wymiany danych lub informacji między nimi. Ze względu na obszar oraz liczbę urządzeń może mieć ona charakter np. lokalny lub rozległy (szczególnym przykładem tego ostatniego jest internet)[32]. Przymiotnik „teleinformatyczny" należy odnieść do jednej z dziedzin nauk inżynieryjno-technicznych zajmującej się wykorzystaniem telekomunikacji w informatyce i informatyki w telekomunikacji. Przedrostek „tele-" wskazuje na działanie na odległość, np. przesyłanie danych lub informacji pomiędzy urządzeniem nadającym a odbierającym. Niezależnie od skali sieci i odległości pomiędzy urządzeniami końcowymi tworzą one jednak system teleinformatyczny[33]. Natomiast zakres regulacji powyżej wymienionych ustaw wymagał od ustawodawcy doprecyzowania rodzaju sieci lub systemu poprzez użycie przymiotnika „telekomunikacyjny" właśnie ze względu na ich skalę. Z tego też względu w zaproponowanej typologii, po pierwsze, opisy strony przedmiotowej czynów zabronionych opisywanych przez prawo karne wprost wskazują „systemy" i „sieci" z odpowiednim przymiotnikiem doprecyzowującym ich znaczenia jako narzędzia (płaszczyzny) zamachu albo przedmiot zamachu (przedmiot wykonawczy czynu). Po drugie, „dane" lub „programy komputerowe" są narzędziem lub przedmiotem zamachu.

Biorąc pod uwagę powyższe wyniki analiz, można przedstawić za M. Siwickim zaktualizowaną – w porównaniu z przedstawionym przez tego autora stanem prawnym – typologię czynów zabronionych będących desygnatami pojęcia cyberprzestępstwo[34]. Są to zatem czyny:

- przeciwko bezpieczeństwu przetwarzanej informacji lub jako przestępstwa *stricte* komputerowe na gruncie polskiego Kodeksu karnego:
  - *hacking* (art. 267 § 1 i 2 k.k.);
  - nielegalne przechwytywanie informacji (art. 267 § 3 k.k.);
  - ujawnienie nielegalnie uzyskanej informacji (art. 267 § 4 k.k.);

[31] Ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (tekst jedn.: Dz.U. z 2020 r. poz. 344).
[32] Szerzej na ten temat zob. P. Lewulis, *O rozgraniczeniu…*, s. 23; F. Radoniewicz, *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w Działaniu" 2013/13, s. 126–127, https://iws.gov.pl/wp-content/uploads/2018/09/Filip-Radoniewicz-Odpowiedzialno%C5%9B%C4%87-karna-za-przest%C4%99pstwo-hackingu-121.pdf (dostęp: 18.07.2023 r.); S. Hoc, *Postanowienia dyrektywy Parlamentu Europejskiego i Rady dotyczącej ataków na systemy informatyczne*, „Przegląd Prawa Publicznego" 2015/3, s. 53.
[33] P. Lewulis, *O rozgraniczeniu…*, s. 25.
[34] Por. M. Siwicki, *Podział…*, s. 250–251; W. Filipkowski, L. Picarela, *Criminalizing Cybercrimes: Italian and Polish Experiences*, „Bialystok Legal Studies" 2021/26(3), s. 179–180, https://doi.org/10.15290/bsp.2021.26.03.09 (dostęp: 18.07.2023 r.).

- zakłócenie dostępu do informacji (art. 268 k.k.);
- ingerencja w dane i system (art. 268a k.k.);
- sabotaż informatyczny (art. 269 § 1 i 2 k.k.);
- zakłócenie systemu komputerowego (art. 269a k.k.);
- narzędzia *hackerskie* (art. 269b k.k.);

- związane z użyciem internetu w celu rozpowszechniania lub prezentowania informacji zakazanych przez prawo (tzw. przestępstwa związane z treścią informacji):
  - utrwalanie lub sprowadzanie, przechowywanie lub posiadanie albo rozpowszechnianie lub prezentowanie określonych treści pornograficznych (art. 202 § 3 k.k.);
  - posiadanie określonych treści pornograficznych (art. 202 § 4a k.k.);
  - produkowanie, rozpowszechnianie, prezentowanie, przechowywanie lub posiadanie treści pornograficznych przedstawiających wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej (art. 202 § 4b k.k.);
  - znieważenie i zniesławienie (art. 212 i 216 k.k.);
  - podżeganie do popełnienia przestępstwa (art. 255 k.k.);
  - nawoływanie do nienawiści (art. 256 k.k.);
- pozostałe (tj. takie, w których to realizacja strony przedmiotowej wiąże się z możliwością wykorzystania sieci i systemów informatycznych, aby naruszyć chronione dobra prawne):
  - sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach, które jest następstwem zakłócania, uniemożliwiania lub w inny sposób wpływania na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji (art. 165 § 1 pkt 4 k.k.);
  - fałszerstwo dokumentów (art. 270 § 1 k.k.) oraz inne przestępstwa przeciwko wiarygodności dokumentów określone w rozdziale XXXIV k.k.,
  - oszustwo (art. 286 k.k.);
  - oszustwo komputerowe (art. 287 k.k.).

Zdaniem autora typologię M. Siwickiego należy jednak uzupełnić o następujące czyny:

- szpiegostwo komputerowe (art. 130 § 3 k.k.), elektroniczny kontakt z osobą małoletnią w celach pedofilskich (art. 200a k.k.) – dodając je do pierwszej z powyższych grup ze względu na znamię oprogramowania, systemu lub sieci informatycznych, teleinformatycznych lub telekomunikacyjnych;
- rozpowszechnianie treści mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym (art. 255a k.k.) – dodając je do grupy drugiej ze względu na nielegalną treść;
- *cyberstalking* (art. 190a § 1 k.k.), kradzież tożsamości (art. 190a § 2 k.k.), kradzież programu komputerowego i kradzież karty bankomatowej (art. 278 § 2 i 5 k.k.), oszustwo telekomunikacyjne (art. 285 § 1 k.k.), paserstwo programu komputerowego (art. 293 k.k.) – dodając je do trzeciej z powyższych grup ze względu na przedmiot wykonawczy czynu.

4. Definicja przestępstwa o charakterze terrorystycznym

Artykuł 115 § 20 k.k. zawiera opis dwóch podstawowych kryteriów[35], które muszą być zrealizowane łącznie, tj.:

- formalne – wysokość sankcji karnej, czyli górna granica zagrożenia ustawowego to co najmniej 5 lat kary pozbawienia wolności; oraz
- materialne (zawierające wiele znamion wartościujących) – cel charakteryzujący stronę podmiotową czynu, czyli cel:
  „1) poważnego zastraszenia wielu osób,
  2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,
  3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej
  – a także groźba popełnienia takiego czynu".

Należy zaznaczyć, że definicja legalna w żaden sposób nie ogranicza zakresu odpowiadających jej czynów ani co do płaszczyzny lub przestrzeni zamachu, ani co do zakresu dóbr chronionych. Natomiast w literaturze przedmiotu można znaleźć listę typów czynów zabronionych spełniających kryminologiczne definicje terroryzmu[36], które wykraczają poza wąską grupę samych aktów terroru lub zamachów. Z tego też względu należy zgłosić postulat uaktualnienia kryminologicznego pojęcia „cyberterroryzmu" o te nowe rodzaje czynów i tym samym uwzględnienie ich w polityce kryminalnej dotyczącej tego zjawiska.

Spośród wcześniej wymienionych cyberprzestępstw tylko część ma jakikolwiek bezpośredni związek ze zjawiskiem terroryzmu. Dlatego też, po pierwsze, dalsze analizy będą odnosić się do wybranych czynów zabronionych przeciwko bezpieczeństwu przetwarzanej informacji (czyli *stricte* komputerowych). Są one najczęściej kojarzone ze zjawiskiem cyberterroryzmu w ujęciu kryminologicznym. Po drugie, przedstawione zostaną wnioski z badań nad niektórymi czynami związanymi z zakazanymi treściami (art. 212, 216, 255, 255a, 256 k.k.). Po trzecie, uwzględnione zostaną czyny zabronione, które wiążą się z możliwością wykorzystania sieci i systemów informatycznych do osiągnięcia celów terrorystycznych (art. 165 § 1 pkt 4, art. 190a, art. 270 § 1, art. 287 k.k.).

4.1. Zakres ustawowego zagrożenia karą

Ponieważ kryterium formalne ma tylko jeden warunek, tylko nieliczne typy wymienionych czynów je spełniają[37]. W przypadku pierwszej grupy są nimi:

- utrudnianie zapoznania się z informacją, ale tylko wtedy, gdy wyrządza to znaczną szkodę majątkową (art. 268 § 3 k.k.) – do 5 lat kary pozbawienia wolności;

[35] M. Smarzewski, *Cyberterroryzm*…, s. 68 i n.
[36] W. Filipkowski, R. Lonca, *Analiza zamachów samobójczych w aspekcie kryminologicznym i prawnym, Część III*, „Przegląd Bezpieczeństwa Wewnętrznego" 2011/4(3), s. 116–117.
[37] M. Smarzewski, *Cyberterroryzm*…, s. 69–70.

- niszczenie danych informatycznych, jeżeli sprawca wyrządził znaczną szkodę majątkową (art. 268a § 2 k.k.) – do 5 lat kary pozbawienia wolności;
- uszkodzenie danych informatycznych (art. 269 k.k.) – do 8 lat kary pozbawienia wolności;
- zakłócenie systemu komputerowego (art. 269a k.k.) – do 5 lat kary pozbawienia wolności;
- narzędzia *hackerskie* (art. 269b k.k.) – do 5 lat kary pozbawienia wolności.

W drugiej grupie jest tylko jeden artykuł spełniający formalną przesłankę. Artykuł 255a k.k. w § 1 opisuje czyn polegający na rozpowszechnianiu treści mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym. Jest on zagrożony karą od 3 miesięcy do 5 lat pozbawienia wolności. Artykuł 255a § 2 k.k. również powinien być rozpatrywany w kontekście cyberterroryzmu, gdyż dotyczy uczestnictwa w szkoleniu mogącym umożliwić popełnienie przestępstwa o charakterze terrorystycznym lub samodzielnego zapoznawania się z treściami opisanymi w § 1 tego artykułu. Zagrożony jest on identyczną sankcją karną.

W trzeciej grupie czynów zabronionych warunek formalny spełniają tylko cztery artykuły:

- sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach, które jest następstwem zakłócania, uniemożliwiania lub w inny sposób wpływania na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji (art. 165 § 1 pkt 4 k.k.) – do 8 lat kary pozbawienia wolności; jeżeli następstwem tego czynu jest śmierć człowieka lub ciężki uszczerbek na zdrowiu wielu osób, to górna granica sankcji wzrasta do 15 lat kary pozbawienia wolności (art. 165 § 3 k.k.);
- *cyberstalking* (art. 190a § 1 k.k.) – do 8 lat kary pozbawienia wolności;
- kradzież tożsamości (art. 190a § 2 k.k.) – do 8 lat kary pozbawienia wolności;
- fałszerstwo materialne dokumentu w jego elektronicznej postaci (art. 270 § 1 k.k.) – do 5 lat kary pozbawienia wolności;
- oszustwo komputerowe (art. 287 § 1 k.k.) – do 5 lat kary pozbawienia wolności.

W kontekście ścigania powyższych przestępstw należy zauważyć, że trzy z nich wymagają wniosku pokrzywdzonego, aby wszcząć lub kontynuować postępowanie karne (art. 190a § 4, art. 268 § 4, art. 268a § 3 k.k.).

4.2. Cel zachowania sprawcy

Wszystkie powyższe czyny spełniające przesłankę formalną zagrożenia karą pozbawienia wolności mają charakter umyślny. W takich przypadkach wykazanie celu opisanego w art. 115 § 20 k.k. nie będzie miało wyłącznie wpływu na wymierzenie kary w górnej granicy ustawowego zagrożenia jako czyny umyślne w zamiarze bezpośrednim. Okoliczność ta będzie powodowała spełnienie przesłanki materialnej w jednej z trzech odmian celu wymienionych w tym artykule. Tym samym spowoduje to obostrzenie odpowiedzialności karnej w związku z treścią art. 65 § 1 k.k.

Pozostałe czyny są dokonywane w zamiarze bezpośrednim, kierunkowym. Jedynie znamiona art. 255a § 1 i 2 k.k. wymieniają cel, jakim jest popełnienie przestępstwa o charakterze terrorystycznym. Natomiast w przypadku pozostałych cele dotyczą:

- „wyrządzenia jej szkody majątkowej lub osobistej" (art. 190a § 2 k.k.);
- „użycia za autentyczny" dokumentu fałszywego (art. 270 § 1 k.k.);
- „osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody" (art. 287 § 1 k.k.).

W przypadku zachowań terrorystycznych cele opisane w art. 115 § 20 k.k. mają charakter główny i nadrzędny względem innych. To sytuacja, w której sprawca zdaje sobie sprawę, że wyrządzenie szkody majątkowej lub osobistej, użycie fałszywego dokumentu jako autentycznego czy też osiągnięcie korzyści majątkowej ma charakter drugorzędny, ale akceptowalny, czasami wręcz konieczny, aby zrealizować jeden z celów głównych opisanych w art. 115 § 20 k.k.

5. Podsumowanie

Przeprowadzone analizy dogmatyczne wsparte rozważaniami kryminologicznymi wskazują na następujące wnioski. Udało się wyodrębnić 12 czynów zabronionych z polskiego Kodeksu karnego, które jednocześnie spełniają warunki uznania ich za cyberprzestępstwa (w ujęciu doktrynalnym lub kryminologicznym) oraz przesłanki z art. 115 § 20 k.k. jako przestępstwa o charakterze terrorystycznym. Pięć z nich uznawanych jest w literaturze za przestępstwa *stricte* komputerowe, które mogą być popełnione w cyberprzestrzeni.

W dużej mierze wpływ na przyporządkowanie cyberprzestępstw do zbioru desygnatów przestępstwa o charakterze terrorystycznym ma przesłanka formalna górnej wysokości granicy zagrożenia ustawowego na poziomie co najmniej 5 lat pozbawienia wolności. Z jednej strony można mieć pewność, że art. 115 § 20 k.k. wyklucza z tego zakresu czyny o niskim poziomie społecznej szkodliwości, przewidując obostrzenie prawnokarnej reakcji wobec poważnych czynów. Z drugiej strony jest to dosyć arbitralne i formalne podejście. Powoduje ono, że część czynów, które są podejmowane w ramach działalności w cyberprzestrzeni pojedynczych osób (tzw. samotnych wilków) albo grup lub związków mających na celu popełnienie przestępstwa o charakterze terrorystycznym, pozostaje poza zakresem tej definicji legalnej (chociażby cały art. 267 k.k. obejmujący: *hacking* – § 1 i 2, nielegalne przechwytywanie informacji – § 3, ujawnienie nielegalnie uzyskanej informacji – § 4)[38]. Mniejsze znaczenie selekcyjne ma relacja między kształtem strony podmiotowej (formy zamiarów) opisywanych czynów i celów zawartych w art. 115 § 20 k.k. W związku z tym należy postulować zrezygnowanie z tego kryterium formalnego uznania czynu za przestępstwo

[38] Na marginesie należy zauważyć, że nowelizacja kodeksu Karnego wprowadzona ustawą z 7.07.2022 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U. z 2022 r. poz. 2600 ze zm.) nie będzie miała wpływu na objęcie nowych czynów kwalifikacją z art. 115 § 20 k.k. Wynika to z tego, że podniesienie górnej granicy ustawowego zagrożenia dla znacznej liczby czynów zabronionych nie będzie miało akurat znaczenia dla aktualności niniejszych badań.

o charakterze terrorystycznym. Tym samym o konsekwencjach przyjęcia tej kwalifikacji będzie decydował tylko motyw, co jest słuszną przesłanką uwzględniającą podejście kryminologiczne do cyberterroryzmu, wyrażaną w literaturze przedmiotu.

W Kodeksie karnym ustawodawca słusznie nie posługuje się terminami „cyberprzestępstwo", „cyberterroryzm" czy „cyberprzestrzeń", gdyż mają one czasami trudne do jednoznacznego określenia zakresy pojęciowe. Używa jednak wyrażeń „system" lub „sieć", których interpretacja jest co najmniej kłopotliwa, z uwagi na ich definiowanie w różnych aktach prawa krajowego i międzynarodowego.

Okoliczności te powodują, że prawnokarna reakcja na działalność terrorystyczną w cyberprzestrzeni może nie być skutecznym sposobem walki z nią. Nie jest jednak pewne, czy kiedykolwiek powyższe przepisy będą zastosowane względem przestępstw mających swoje źródło na terytorium Polski lub powodujących tam skutki.

Relacje znaczeniowe pomiędzy cyberterroryzmem a cyberprzestępczością stanowią złożone zagadnienie, które wymaga dalszych badań[39]. Wynika to z konstatacji, że nadal istnieją luki w zakresie prawniczej i kryminologicznej wiedzy dotyczącej tej relacji. Przedstawione polskie regulacje prawne są tego przykładem. Brak jednolitej definicji cyberprzestępczości utrudnia znalezienie globalnych rozwiązań. Ponadto brakuje jednolitego zrozumienia zorganizowanej cyberprzestępczości oraz jasnych definicji i międzynarodowych standardów w zwalczaniu cyberterroryzmu. Wzrost znaczenia technologii informacyjnych w życiu społecznym oraz skala i zakres zagrożeń dla bezpieczeństwa narodowego wymaga ciągłego doskonalenia regulacji prawnych, w tym o charakterze karnym. Konieczne jest dalsze wypełnianie tych luk wiedzą teoretyczną i empiryczną, co pozwoli na poszukiwanie skuteczniejszych rozwiązań w walce z cyberprzestępczością i cyberterroryzmem, także na poziomie polityki karnej.

Bibliografia

1. Adamski A., *Buszujący w sieci. Cybernowelizacja prawa karnego*, Rzeczpospolita z 27.10.2003 r.
2. Akdeniz Y., *An Advocacy Handbook for the Non Governmental Organisations, The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems*, 2003, https://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf.
3. Al Mazari A., Anjariny A.H., Habib S.A., Nyakwende E., *Cyber Terrorism Taxonomies: Definition, Targets, Patterns, Risk Factors, and Mitigation Strategies*, International Journal of Cyber Warfare and Terrorism 2016, t. 6, nr 1, https://doi.org/10.4018/IJCWT.2016010101.

[39] Nie jest to jednak problem nowy; zob. S. Ozeren, *Global response to cyberterrorism and cybercrime: A matrix for international cooperation and vulnerability assessment*, rozprawa doktorska, University of North Texas 2005, s. 177–179, https://digital.library.unt.edu/ark:/67531/metadc4847/m2/1/high_res_d/dissertation.pdf (dostęp: 18.07.2023 r.).

4. Belov A., Delembovsky M., Shklyar V., *Simulation of cyber threats for the Internet of Things*, Transfer of Innovative Technologies 2021, t. 4, nr 1, https://doi.org/10.32347/tit2141.0303.
5. Bernik I., *Cybercrime and Cyberwarefare*, London 2014.
6. Burdziak K., *Definicja przestępstwa o charakterze terrorystycznym przewidziana w polskim Kodeksie karnym w świetle rozwiązań Unii Europejskiej, Rady Europy i Organizacji Narodów Zjednoczonych – raport z projektu badawczego*, Warszawa 2021.
7. Constantin M., Bortea A., Mema D., *Risks and Vulnerabilities in Digital Public Services. Threat of Cyberterrorism Vs Romania's Cybersecurity Strategy*, Holistica – Journal of Business and Public Administration 2020, nr 11.
8. Conway M., *What is Cyberterrorism and How Real is the Threat?: A Review of the Academic Literature, 1996–2009*, [w:] *Cyber Behavior: Concepts, Methodologies, Tools, and Applications*, Management Association, Information Resources, Hershey 2014, https://doi.org/10.4018/978-1-4666-5942-1.
9. Denning D., *Cyberterrorism*, *Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services*, 23.05.2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.
10. Evans D., *The Internet of Things. How the Next Evolution of the Internet is Changing Everything, White paper*, 2011, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
11. Filipkowski W., Lonca R., *Analiza zamachów samobójczych w aspekcie kryminologicznym i prawnym, Część III*, Przegląd Bezpieczeństwa Wewnętrznego 2011, nr 4(3).
12. Filipkowski W., Picarela L., *Criminalizing Cybercrimes: Italian and Polish Experiences*, Bialystok Legal Studies 2021, t. 26, nr 3, https://doi.org/10.15290/bsp.2021.26.03.09.
13. Foldes S., *Comments on the notion of information system in the Budapest Convention on Cybercrime, the EU directive, and selected penal codes*, 2017, https://hal.archives-ouvertes.fr/hal-01588889.
14. Foltz C.B., *Cyberterrorism, computer crime, and reality*, Information Management & Computer Security 2004, t. 12, nr 2.
15. Gordon S., Ford R., *Cyberterrorism?*, Computers & Security 2002, t. 21, nr 7, https://doi.org/10.1016/S0167-4048(02)01116-1.
16. Hoc S., *Postanowienia dyrektywy Parlamentu Europejskiego i Rady dotyczącej ataków na systemy informatyczne*, Przegląd Prawa Publicznego 2015, nr 3.
17. Jaroszewska I.A., *Wybrane aspekty przestępczości w cyberprzestrzeni*, Olsztyn 2017.
18. Khaeriah Kadir N., Judhariksawan, Maskun, *Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes*, Fiat Justisia 2019, t. 13, nr 4, https://doi.org/10.25041/fiatjustisia.v13no4.1735.
19. Khan S., Saleh T., Dorasamy M., Khan N., Tan Swee Leng O., Gale Vergara R., *A systematic literature review on cybercrime legislation*, F1000Research 2022, nr 11:971, https://doi.org/10.12688/f1000research.123098.1.

20. Konieczny M., *Cyberprzestępczość – krótka historia, współczesne oblicza i trudna do przewidzenia przyszłość*, Roczniki Administracji i Prawa 2023, t. 23, z. 1, https://doi.org/10.5604/01.3001.0016.3776.
21. Kopczewski M., *Elementy infrastruktury krytycznej państwa /organizacji/ – jako obiekty narażone na ataki cyberterrorystyczne*, Zakopane 2011, http://www.ptzp.org.pl/'les/konferencje/kzz/artyk_pdf_2011/054.pdf.
22. Kośka M., *Cyberterroryzm – zadania antyterrorystyczne Sił Zbrojnych Rzeczypospolitej Polskiej w kontekście obowiązujących aktów prawnych*, Wiedza Obronna 2022, t. 279, nr 2, https://doi.org/10.34752/2022-j279.
23. Lewulis P., *O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych*, Prokuratura i Prawo 2021, nr 3.
24. Mahinderjit Singh M., Abu Bakar A., *A Systemic Cybercrime Stakeholders Architectural Model*, Procedia Computer Science 2019, t. 161, https://doi.org/10.1016/j.procs.2019.11.227.
25. Neagu F.S., Savu A., *The costs of cyberterrorism for the national economy: United States of America vs Egypt*, [w:] *Proceedings of the 13th International Conference on Business Excellence 2019*, https://doi.org/10.2478/picbe-2019-0086.
26. Ozeren S., *Global response to cyberterrorism and cybercrime: A matrix for international cooperation and vulnerability assessment*, rozprawa doktorska, University of North Texas 2005, https://digital.library.unt.edu/ark:/67531/metadc4847/m2/1/high_res_d/dissertation.pdf.
27. Radoniewicz F., *Odpowiedzialność karna za przestępstwo hackingu*, Prawo w Działaniu 2013, t. 13, https://iws.gov.pl/wp-content/uploads/2018/09/Filip-Radoniewicz-Odpowiedzialno%C5%9B%C4%87-karna-za-przest%C4%99pstwo-hackingu-121.pdf.
28. Ranjan Srivastava S., Dube S., *Cyberattacks, Cybercrime and Cyberterrorism*, [w:] *Handbook of Research on Network Forensics and Analysis Techniques*, red. G. Shrivastava, P. Kumar, B.B. Gupta, S. Bala, N. Dey, Hershey 2018, https://doi.org/10.4018/978-1-5225-4100-4.ch010.
29. Samodulska M., *Crimes Committed via the Internet – Selected Aspects*, Teka Komisji Prawniczej 2014, t. 7.
30. Seissa I.G., Ibrahim J., Yahaya N.-Z., *Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review*, International Journal of Science and Research 2017, t. 6, nr 1, https://doi.org/10.21275/art20163936.
31. Siwicki M., *Podział i definicja cyberprzestępstw*, Prokuratura i Prawo 2012, nr 7–8.
32. Skoneczny Ł., *Rola Agencji Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa Rzeczypospolitej Polskiej*, Przegląd Bezpieczeństwa Wewnętrznego 2009, nr 1.
33. Smarzewski M., *Cyberterroryzm a cyberprzestępstwa o charakterze terrorystycznym*, Ius Novum 2017, nr 1.
34. Szpor G., [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, K. Czaplicki, Warszawa 2019.
35. Worona J., *Prace naczelnych organów administracji państwowej a cyberbezpieczeństwo Polski*, Białostockie Studia Prawnicze 2016, nr 20.

36. Woszek S., *Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej*, Przegląd Bezpieczeństwa Wewnętrznego 2022, t. 14, nr 27, https://doi.org/10.4467/20801335PBW.22.056.16947.