DOI: 10.31648/sp.12554

Paweł Olber
Akademia Policji w Szczytnie
ORCID: 0000-0002-4614-9527
p.olber@apol.edu.pl

Cyberprzestępczość – od niejednoznaczności pojęciowej do szerokiego ujęcia definicyjnego

Wstęp

Rozwój przestępczości z wykorzystaniem technologii informacyjno-komunikacyjnych przyczynił się do wykształcenia pojęcia „cyberprzestępczość". Termin ten, mimo licznych kontrowersji związanych z jego zakresem znaczeniowym, stał się niezwykle popularny i jest powszechnie używany w sferze publicznej. W literaturze naukowej wskazuje się jednak na to, że „cyberprzestępczość" stanowi pojęcie o charakterze medialnym, a nie kategorię oddającą istotę przestępstw popełnianych w przestrzeni cyfrowej[1]. Nie dziwi więc fakt, że w środowisku naukowym formułowane są postulaty przemawiające za rezygnacją z tego terminu. W rzeczywistości jednak okazuje się to niemożliwe, gdyż pojęcie „cyberprzestępczość" zbyt mocno zakorzeniło się w świadomości społecznej jak i w praktyce instytucjonalnej.

Definicyjna niejednoznaczność cyberprzestępczości znajduje odzwierciedlenie w stosowanej terminologii. Zarówno w literaturze naukowej, jak i w dokumentach instytucjonalnych stosowane są różnorodne określenia, takie jak: przestępczość komputerowa[2], przestępczość w cyberprzestrzeni[3], przestępczość teleinformatyczna[4], przestępczość związana z informacjami

[1] R. Bryant, *The challenge of digital crime*, [w:] R. Bryant (red.), *Investigating digital crime*, Chichester 2008, s. 1.

[2] A. Adamski (red.), *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji*, Toruń 1994, s. 7.

[3] J. Sobczak, *Przestępczość w cyberprzestrzeni między przepisami polskimi a międzynarodowymi*, „Cybersecurity and Law" 2021, t. 1, nr 1, s. 159.

[4] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, Toruń 2001, s. 7.

komputerowymi[5] czy też przestępczość internetowa[6]. Interesujący jest przy tym fakt, że wspomniane określenia stosowane są zamiennie[7], a przestępczość związana z informacjami komputerowymi uznana została przez wielu za cyberprzestępczość[8]. Brak jednolitego ujęcia definicyjnego widoczny jest także na poziomie regulacji prawnych. Zarówno Konwencja Rady Europy o cyberprzestępczości[9], jak również Konwencja ONZ o zwalczaniu cyberprzestępczości[10] nie rozstrzygają sporu definicyjnego przez sformułowanie jednej ogólnej definicji. Akty te przyjmują podejście funkcjonalne poprzez określenie katalogu czynów wymagających penalizacji, regulację instrumentów współpracy międzynarodowej oraz odniesienie do zabezpieczania i udostępniania dowodów elektronicznych. Podobnie polskie prawo karne nie posługuje się legalną definicją cyberprzestępczości[11] i dodatkowo pozostaje bierne wobec specyfiki dowodów elektronicznych[12].

Wieloznaczność pojęcia cyberprzestępczość stała się przedmiotem intensywnej debaty naukowej, poświęconej rozumieniu i konceptualizacji zjawiska[13]. Prowadzony dotychczas dyskurs naukowy nie rozstrzygnął jednak sporów związanych z ujęciem definicyjnym cyberprzestępczości[14]. Brak zgodności w tym zakresie przekłada się więc na trudności związane ze zwalczaniem tego zjawiska oraz prowadzeniem badań naukowych[15].

---

[5] Agreement on Cooperation among the States Members of the Commonwealth of Independent States in Combating Offences Relating to Computer Information, sporządzone w Mińsku dnia 1 czerwca 2001 r., https://cis-legislation.com/document.fwx?rgn=4129 (data dostępu: 22.05.2026).

[6] Najwyższa Izba Kontroli, *Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości*, Informacja o wynikach kontroli, nr ewid. 125/2022/P/21/042/KPB, Warszawa 2022, s. 55.

[7] J. Clough, *Principles of cybercrime*, Cambridge 2010, s. 8–11.

[8] K. Phillips i in., *Conceptualizing cybercrime: definitions, typologies and taxonomies*, „Forensic Sciences" 2022, t. 2, nr 2, s. 383; N. Akdemir, B. Sungur, B.U. Başaranel, *Examining the challenges of policing economic cybercrime in the UK*, „Güvenlik Bilimleri Dergisi" 2020, s. 117; B. Akhgar i in., *Consolidated taxonomy and research roadmap for cybercrime and cyberterrorism*, [w:] B. Akhgar, B. Brewster (red.), *Combatting cybercrime and cyberterrorism: challenges, trends and priorities*, Cham 2016, s. 298.

[9] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r., poz. 728).

[10] Konwencja ONZ o zwalczaniu cyberprzestępczości, przyjęta przez Zgromadzenie Ogólne ONZ dnia 24 grudnia 2024 r. Rezolucją 79/243, https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html (data dostępu: 22.05.2026).

[11] M. Zbrojewska i in., *Jak definiujemy cyberprzestępstwo?*, „Informatics, Control, Measurement in Economy and Environment Protection" 2016, t. 6, nr 2, s. 65.

[12] M. Kusak, *Dostęp do danych elektronicznych dotyczących treści w postępowaniu karnym – wyzwania krajowe i międzynarodowe*, „Gdańskie Studia Prawnicze" 2024, nr 2(63), s. 74.

[13] Zob. M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8.

[14] Zob. J. Wasilewski, *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15(8); P. Lewulis, *O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych*, „Prokuratura i Prawo" 2021, nr 3.

[15] B. Dupont, C. Whelan, *Enhancing relationships between criminology and cybersecurity*, „Journal of Criminology" 2021, t. 54, nr 1, s. 79.

Wspomniane trudności wynikają przede wszystkim z zabiegu historycznego, polegającego na instrumentalizacji pojęcia „cyberprzestępczość", utrwalonego w oficjalnym raporcie badawczym brytyjskiego Ministerstwa Spraw Wewnętrznych. W przedmiotowym raporcie sformułowano bowiem dwie kategorie cyberprzestępczości: przestępstwa zależne od systemów teleinformatycznych (ang. *cyber-dependent crimes*) oraz przestępstwa popełniane z wykorzystaniem systemów teleinformatycznych (ang. *cyber-enabled crimes*)[16]. Kategorie te, mimo że nie oddają istoty i złożoności zjawiska, zaczęły pełnić funkcję porządkującą i organizacyjną, wpływając m.in. na struktury organów ścigania[17] oraz sposób gromadzenia i przetwarzania danych w systemach statystycznych[18]. Formalny charakter wspomnianej klasyfikacji potwierdza jej wykorzystanie w dokumentach i opracowaniach instytucji publicznych wielu państw, w tym m.in. Kanady[19], Australii[20], Irlandii[21] i Niderlandów[22], w szczególności przy opisie skali cyberprzestępczości oraz problemów w zakresie pomiaru zjawiska. Klasyfikacja cyberprzestępczości oparta na kategoriach *cyber-dependent crimes* i *cyber-enabled crimes* zyskała zatem znaczenie międzynarodowe, wykraczające poza pierwotny kontekst brytyjskiego raportu badawczego.

Utrwalone w ten sposób błędne założenia dotyczące cyberprzestępczości wymagają rewizji. Celem niniejszej publikacji jest więc analiza dotychczasowych ujęć cyberprzestępczości, ukazanie złożoności tego zjawiska oraz wykazanie, w jaki sposób szeroko akceptowany podział na przestępstwa zależne od systemów teleinformatycznych i przestępstwa popełniane z wykorzystaniem tych systemów wpływa na praktykę instytucjonalną. Ustalenia te przemawiają za przyjęciem szerokiego ujęcia definicyjnego, które trafniej oddaje rzeczywisty charakter cyberprzestępczości.

---

[16] M. McGuire, S. Dowling, *Cyber crime: a review of the evidence. Research Report 75. Summary of key findings and implications*, London 2013.

[17] Protokół z XXIX posiedzenia Rady do Spraw Cyfryzacji, 17 kwietnia 2025 r., https://www.gov.pl/attachment/099033ff-3e39-4536-80a5-68bf847d14e2 (data dostępu: 20.02.2026).

[18] N. Urbańska, *Cyberprzestępczość i wynikające z niej zagrożenia*, „Cybersecurity & Cybercrime" 2025, t. 1, nr 7, s. 3.

[19] Department of Justice Canada, Evaluation of the investigative *Powers for the 21st century initiative*, https://www.justice.gc.ca/eng/rp-pr/cp-pm/eval/rep-rap/2020/ip21c-pe21s/p4.html (data dostępu: 30.06.2026).

[20] Australian Government, Department of Home Affairs, *National plan to combat cybercrime 2022*, s. 4–5, https://www.homeaffairs.gov.au/criminal-justice/files/national-plan-combat-cybercrime-2022.pdf (data dostępu: 2.07.2026).

[21] An Garda Síochána, Garda National Cyber Crime Bureau, *Cybercrime risks & prevention tips*, Dublin [b.d.], s. 2, https://www.garda.ie/en/about-us/organised-serious-crime/garda-national-cyber-crime-bureau-gnccb-/cyber-crime-risks-and-prevention-tips.pdf (data dostępu: 2.07.2026).

[22] R. Leukfeldt, R. Notté, M. Malsch, *Slachtofferschap van online criminaliteit: een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit. Samenvatting*, Amsterdam 2018, s. 2, https://open.overheid.nl/documenten/ronl-3cc3344c-c5c9-4184-8886-7a9333800228/pdf (data dostępu: 2.07.2026).

Na potrzeby niniejszego opracowania przyjęto perspektywę definicyjną, uzupełnioną odniesieniami do praktyki zwalczania cyberprzestępczości oraz prawa karnego materialnego. Zasadniczym przedmiotem podjętych rozważań jest analiza ujęć definicyjnych i klasyfikacyjnych cyberprzestępczości. Z kolei odniesienie do praktyki służy wykazaniu, że ujęcia definicyjne oraz klasyfikacje cyberprzestępczości znajdują odzwierciedlenie w strukturach organów ścigania. Odwołanie do prawa karnego materialnego ma natomiast charakter pomocniczy, pokazując, że cyberprzestępczość wymyka się szeroko akceptowanym klasyfikacjom tego zjawiska.

Początki debaty naukowej

Charakterystyka cyberprzestępczości wymaga odwołania się do wczesnej dyskusji naukowej poświęconej temu zjawisku, zapoczątkowanej pod koniec lat 90. XX w. w pracach Davida S. Walla[23] i rozwiniętej przez Petera N. Grabosky'ego[24] oraz Majida Yara[25]. Pierwsze próby ujęcia cyberprzestępczości charakteryzowały się wykorzystaniem metafory cyberprzestrzeni, rozumianej jako domena, w której następuje oddzielenie treści od formy materialnej[26]. Prowadzona debata obejmowała zasadniczo trzy odrębne stanowiska. Pierwsza perspektywa to uznanie cyberprzestępczości za przestrzeń, w której dotychczas znane przestępstwa przyjmują nowe formy, a także pojawiają się całkowicie nowe rodzaje działalności przestępczej[27]. W drugim ujęciu cyberprzestępczość zdefiniowano jako znane formy przestępczości tradycyjnej, realizowane za pośrednictwem nowych technologii. Stanowisko to zostało poparte analizą konkretnych przykładów przestępstw (np. oszustw inwestycyjnych), przeglądem motywacji sprawców oraz refleksją na temat kwestii jurysdykcyjnych. Zauważono przy tym, że przesłanki działania sprawców cyberprzestępstw są tożsame z motywacjami sprawców przestępstw tradycyjnych. Ostatecznie uznano zatem, że cyberprzestępczość nie zmienia istoty samego przestępstwa, a jedynie zmienia kontekst egzekwowania prawa oraz zwiększa transgraniczny wymiar przestępczości[28]. Ostatni głos w przedmiotowej debacie

---

[23] D.S. Wall, *Cybercrimes: new wine, no bottles?*, [w:] P. Davies, P. Francis, V. Jupp (red.), *Invisible crimes*, London 1999, s. 105; idem, *Catching cybercriminals: policing the Internet*, „International Review of Law, Computers & Technology" 1998, t. 12, nr 2, s. 201–202.

[24] P.N. Grabosky, *Virtual criminality: old wine in new bottles?*, „Social & Legal Studies" 2001, t. 10, nr 2, s. 243–244.

[25] M. Yar, *The novelty of 'cybercrime': an assessment in light of routine activity theory*, „European Journal of Criminology" 2005, t. 2, nr 4, s. 424.

[26] J.P. Barlow, *Selling wine without bottles: the economy of mind on the global net*, „Duke Law & Technology Review" 2019, t. 18, s. 10.

[27] D.S. Wall, *Catching cybercriminals…*, s. 201–202.

[28] P.N. Grabosky, op. cit., s. 243–244.

dotyczył perspektywy, według której cyberprzestrzeń nie zmienia istoty przestępstw, jednakże problem stanowi przypisanie ich do konkretnego systemu prawnego[29].

Pierwsze podejście przyczyniło się do ukształtowania konsensusu. Za cyberprzestępczość uznano ostatecznie zjawisko o szerokim i zróżnicowanym charakterze, rozumiane jako szereg działań przestępczych popełnianych w cyberprzestrzeni[30]. Co istotne, wspomniana dyskusja doprowadziła do wyodrębnienia głównych kategorii cyberprzestępczości, będących podstawą wielu definicji i klasyfikacji zarówno akademickich[31], jak i instytucjonalnych[32]. Dalszy dyskurs naukowy nie koncentrował się już wyłącznie na rozumieniu zjawiska cyberprzestępczości, lecz na rozstrzygnięciu, które jej formy stanowią cyberprzestępstwa *sensu stricto*, a które są tradycyjnymi przestępstwami popełnianymi w cyberprzestrzeni[33].

Pierwotne ujęcia klasyfikacyjne

Pierwsza naukowa klasyfikacja cyberprzestępczości, opracowana przez Stevena Furnella, obejmuje podział zjawiska na przestępstwa wspomagane komputerowo (ang. *computer-assisted crimes*) oraz przestępstwa ukierunkowane na systemy komputerowe (ang. *computer-focused crimes*). Za przestępstwa wspomagane komputerowo uznano czyny, w których komputer stanowi narzędzie ułatwiające popełnienie przestępstwa podstawowego. Do tej kategorii przestępstw zaliczyć można m.in. oszustwa, kradzieże oraz rozpowszechnianie treści pornograficznych. Z kolei przestępstwa przeciwko systemom komputerowym obejmują czyny zabronione, które powstały w wyniku rozwoju technologii informatycznych i nie mają odpowiednika w świecie rzeczywistym. Do tej kategorii zalicza się m.in. sabotaż komputerowy oraz ataki skierowane przeciwko systemom teleinformatycznym[34].

---

29 M. Yar, op. cit. s. 424.

30 A.M. Bossler, T. Berenblum, *Introduction: new directions in cybercrime research*, „Journal of Crime and Justice" 2019, t. 42, nr 5, s. 495.

31 Zob. B.-J. Koops, *The Internet and its opportunities for cybercrime*, „SSRN Electronic Journal" 2010, s. 1; N. Kshetri, *The global cybercrime industry: economic, institutional and strategic perspectives*, Berlin 2010, s. 3; S.W. Brenner, *Toward a criminal law for cyberspace: distributed security*, „Boston University Journal of Science & Technology Law" 2004, t. 10, s. 101.

32 Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, United Nations, 19 lipca 2000 r., s. 4; Shanghai Cooperation Organization, Shanghai Cooperation Organization (SCO) Agreement, 2010, s. 12; European Union Agency for Law Enforcement Cooperation, Internet Organised Crime Threat Assessment: IOCTA 2017, Publications Office 2017, s. 14.

33 T.J. Holt, A.M. Bossler, *An assessment of the current state of cybercrime scholarship*, „Deviant Behavior" 2014, t. 35, nr 1, s. 21.

34 S. Furnell, *Cybercrime: vandalizing the information society*, London 2002, s. 22.

Kolejna, druga klasyfikacja cyberprzestępczości, przedstawiana jako spektrum różnych działań przestępczych, opiera się na szerokim ujęciu zjawiska, w którym komputer lub inne urządzenie teleinformatyczne może być celem popełnienia przestępstwa, narzędziem umożliwiającym popełnienie czynu zabronionego lub może mieć znaczenie incydentalne[35]. Biorąc pod uwagę szeroki zakres zjawiska, wyróżniono cyberprzestępczość typu I i II. Cyberprzestępczość typu I (z dominującym komponentem technicznym) ulokowano na początku spektrum i zdefiniowano jako zjawisko obejmujące zdarzenia jednostkowe, postrzegane przez pokrzywdzonego jako pojedyncze incydenty, często związane z użyciem złośliwego oprogramowania, a niekiedy także z wykorzystaniem podatności systemu informatycznego. Do kategorii I zaliczono niektóre przestępstwa przeciwko ochronie informacji, w tym m.in. naruszenie integralności zapisu informacji czy też bezprawne niszczenie informacji[36].

Z kolei cyberprzestępczość typu II (z dominującym komponentem ludzkim) przyporządkowano na końcu spektrum. Kategoria ta obejmuje działania przestępcze, ułatwiane przez oprogramowanie użytkowe (np. komunikatory internetowe, programy pocztowe itd.), poprzedzane nawiązaniem relacji z potencjalną ofiarą. Przykładem tego rodzaju przestępstwa może być oszustwo, groźba karalna czy też uporczywe nękanie[37].

W toku dalszej dyskusji naukowej opracowano propozycję klasyfikacji cyberprzestępczości według trzech kategorii, które obejmują:

- przestępstwa przeciwko integralności systemów komputerowych (ang. *computer integrity crimes*),
- przestępstwa wspomagane komputerowo lub powiązane z komputerami (ang. *computer-assisted/related crimes*),
- przestępstwa komputerowe związane z treścią przetwarzanej informacji (ang. *computer content crimes*)[38].

Za przestępstwa przeciwko integralności systemów komputerowych (ang. *computer integrity crimes*) uznano czyny godzące w bezpieczeństwo mechanizmów dostępu do sieci informatycznych oraz w prawidłowe funkcjonowanie infrastruktury teleinformatycznej. Obejmują one m.in.: nieuprawniony dostęp do systemu informatycznego, utrudnianie dostępu i niszczenie informacji, ingerencję w dane i system, zakłócanie pracy systemu komputerowego lub sieci teleinformatycznej. Przestępstwa te mogą poprzedzać popełnienie poważniejszych czynów zabronionych. Z kolei za przestępstwa wspomagane

[35] M. Szczepaniec, *Komputer jako narzędzie przestępstwa*, „Zeszyty Prawnicze" 2012, t. 12, nr 2, s. 168.

[36] S. Gordon, R. Ford, *On the definition and classification of cybercrime*, „Journal in Computer Virology" 2006, t. 2, nr 1, s. 14–16.

[37] Ibidem.

[38] D.S. Wall, *Cybercrime: the transformation of crime in the information age*, Cambridge 2007, s. 49–50.

komputerowo lub powiązane z komputerami (ang. *computer-assisted/related crimes*) uznano zachowania polegające na wykorzystywaniu sprzętu komputerowego oraz sieci teleinformatycznej do bezprawnego uzyskiwania korzyści majątkowych. Przestępstwa te dotyczą oszustw internetowych oraz ich odmian opartych na manipulacji społecznej, takich jak *phishing*, fałszywe inwestycje oraz nadużycia związane z funkcjonowaniem internetowych platform sprzedażowych. Do ostatniej trzeciej kategorii przestępstw związanych z treścią przetwarzanej informacji zaliczono czyny polegające na wytwarzaniu, utrwalaniu, sprowadzaniu, przechowywaniu, rozpowszechnianiu lub publicznym prezentowaniu bezprawnych treści za pośrednictwem systemów teleinformatycznych, w szczególności materiałów pornograficznych oraz materiałów propagujących zachowania o charakterze rasistowskim lub ksenofobicznym, bądź inne formy przestępstw z nienawiści[39].

Formalizacja klasyfikacji

Zaprezentowany dyskurs naukowy miał charakter teoretyczny i stworzył podstawy dla formalnej klasyfikacji cyberprzestępczości przedstawionej w raporcie brytyjskiego Ministerstwa Spraw Wewnętrznych. W dokumencie tym stwierdzono, że cyberprzestępczość jest szerokim pojęciem, które obejmuje grupę ściśle powiązanych ze sobą działań przestępczych, tj. przestępstw zależnych od systemów teleinformatycznych (ang. *cyber-dependent crimes*) oraz przestępstw popełnianych z wykorzystaniem systemów teleinformatycznych (ang. *cyber-enabled crimes*)[40].

W przywołanym raporcie uznano, że przestępstwa zależne od systemów teleinformatycznych (ang. *cyber-dependent crimes*) to czyny zabronione, które można popełnić wyłącznie przy użyciu komputera, sieci komputerowych lub za pomocą innych form technologii informacyjno-komunikacyjnych. Przestępstwa te dotyczą m.in. przełamywania zabezpieczeń, dystrybucji złośliwego oprogramowania czy też ataków odmowy usługi (ang. *Denial of Service* – DoS) oraz rozproszonych ataków odmowy usługi (ang. *Distributed Denial of Service* – DDoS). Czyny te stanowią przede wszystkim działania wymierzone w komputery lub zasoby sieciowe. Z kolei za przestępstwa popełniane z wykorzystaniem systemów teleinformatycznych (ang. *cyber-enabled crimes*) uznano tradycyjne przestępstwa, których skala lub zasięg zostały zwiększone dzięki wykorzystaniu komputerów, sieci komputerowych lub innych technologii informacyjno-komunikacyjnych. W przeciwieństwie do przestępstw zależnych od systemów teleinformatycznych (ang. *cyber-dependent crimes*) czyny te

[39] Ibidem.

[40] M. McGuire, S. Dowling, op. cit., s. 5.

mogą być popełniane bez użycia technologii informacyjno-komunikacyjnych. Kategoria ta obejmuje m.in. wszelkiego rodzaju oszustwa, kradzieże oraz wybrane przestępstwa przeciwko wolności seksualnej i obyczajności (np. rozpowszechnianie treści pornograficznych)[41].

Wspomniany raport, będący *de facto* dokumentem o charakterze systematyzującym, sformalizował dwie powiązane ze sobą kategorie cyberprzestępczości, będące do tego momentu wyłącznie przedmiotem debaty naukowej. Tym samym podział cyberprzestępczości według kategorii *cyber-dependent crimes* i *cyber-enabled crimes* wszedł do języka debaty publicznej i został utrwalony w prowadzonym dyskursie naukowym[42]. Podział ten zaczął być wykorzystywany w praktyce instytucjonalnej wielu państw, w tym m.in. w opracowywanych statystykach i w dokumentach strategicznych[43], mimo że może prowadzi do istotnych błędów metodologicznych. Klasyfikacja ta dokonuje bowiem agregacji różnych przestępstw (np. przeciwko mieniu i wolności seksualnej) w ramach jednej kategorii, tj. przestępstw popełnianych z wykorzystaniem systemów teleinformatycznych (ang. *cyber-enabled*). W związku z tym kategoria ta jest bardzo szeroka, tracąc jednocześnie swą precyzję analityczną.

Warto także zauważyć, że w praktyce zjawisko cyberprzestępczości nie dzieli się na dwie odrębne kategorie, co zostało potwierdzone licznymi badaniami. Uzyskane wyniki z prowadzonych badań podważają zasadność dalszego stosowania podziału cyberprzestępczości na przestępstwa zależne od systemów teleinformatycznych (ang. *cyber-dependent crimes*) oraz przestępstwa popełniane z wykorzystaniem takich systemów (ang. *cyber-enabled crimes*)[44]. Wspomniane ustalenia prowadzą do wniosku, że definiowanie cyberprzestępczości wymaga pewnej elastyczności. Cyberprzestępczości jest zbyt złożona, aby wpisywać ją w prostą dychotomię przestępstw *cyber-dependent crimes* i *cyber-enabled crimes*. Rozróżnienie cyberprzestępczości według wskazanych kategorii ma zatem ograniczoną wartość analityczną, ponieważ w praktyce granica między nimi ulega zatarciu. Kategorie te mogą pełnić funkcję porządkującą, nie powinny jednak stanowić samodzielnej podstawy konceptualizacji cyberprzestępczości. Zasadne jest raczej odwołanie się do analizy rzeczywistych mechanizmów działania sprawców oraz roli technologii w strukturze czynu zabronionego[45].

---

41 Ibidem.

42 R. Sarre, L.Y.-C. Lau, L.Y.C. Chang, *Responding to cybercrime: current trends*, „Police Practice and Research" 2018, t. 19, nr 6, s. 515.

43 M. Button i in., *Assessing the seriousness of cybercrime: the case of computer misuse crime in the United Kingdom and the victims' perspective*, „Criminology & Criminal Justice" 2025, t. 25, nr 2, s. 3; I. Voce, A. Morga, *Cybercrime in Australia 2023*, Statistical Report 43, Canberra 2023; M. McGuire, S. Dowling, op. cit.

44 J. Lusthaus, *Reconsidering crime and technology: what is this thing we call cybercrime?*, „Annual Review of Law and Social Science" 2024, t. 20 nr 1, s. 372–373.

45 K.F. Steinmetz, *Against cybercrime: toward a realist criminology of computer crime*, London 2023, s. 13–14.

Mimo istniejących badań empirycznych, które ukazują rzeczywistą charakterystykę cyberprzestępczości, polityka publiczna nadal utrwala stare ramy klasyfikacyjne. Przykładem jest chociażby ujęcie definicyjne Komisji Europejskiej[46], według której cyberprzestępczość to czyny przestępcze dokonywane za pośrednictwem sieci komputerowej lub przy wykorzystaniu sieci komunikacji elektronicznej i systemów informatycznych. Dodatkowo Komisja klasyfikuje cyberprzestępczość według trzech następujących kategorii:

– przestępstwa specyficzne dla Internetu: ataki na systemy informacyjne lub *phishing* (np. fałszywe strony bankowe służące wyłudzaniu haseł umożliwiających dostęp do rachunków bankowych ofiar),
– oszustwa i fałszerstwa internetowe: przestępstwa o znacznej skali, które mogą być popełniane za pośrednictwem sieci teleinformatycznych poprzez mechanizmy kradzieży tożsamości, *phishing*, dystrybucję spamu czy też złośliwego oprogramowania,
– nielegalne treści w Internecie, w tym materiały przedstawiające seksualne wykorzystywanie nieletnich, nawoływanie do nienawiści na tle różnic rasowych, nawoływanie do popełnienia przestępstw o charakterze terrorystycznym oraz publiczne pochwalanie przemocy, terroryzmu, rasizmu i ksenofobii[47].

Powyższa klasyfikacja, mimo stosowania innej terminologii, odzwierciedla więc logikę podziału cyberprzestępczości na *cyber-enabled crimes* i *cyber-dependent crimes*. Ujęcie Komisji Europejskiej można zatem uznać za współczesną odsłonę wcześniejszych założeń klasyfikacyjnych, osadzoną w szerszych ramach normatywnych, wyznaczonych m.in. przez Konwencję Rady Europy o cyberprzestępczości. Konwencja ta, choć nie posługuje się terminologią *cyber-enabled crimes* i *cyber-dependent crimes*, wyodrębnia podstawowe grupy czynów związanych z systemami i danymi informatycznymi, w tym przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów, przestępstwa komputerowe, przestępstwa ze względu na charakter zawartych informacji oraz przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych[48].

Kwalifikacja prawna wybranych cyberprzestępstw

Warto zauważyć, że *phishing* został uwzględniony w klasyfikacji Komisji Europejskiej w dwóch różnych kategoriach. Oznacza to, że cyberprzestępczość nie jest zbiorem sztywnych ram, lecz zjawiskiem o złożonej strukturze, które

[46] Komisja Europejska, *Cybercrime*, https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en (data dostępu: 25.02.2026).
[47] Ibidem.
[48] Konwencja Rady Europy o cyberprzestępczości…

wymyka się jednoznacznym podziałom. Powyższe dowodzi także, że granice między kategoriami cyberprzestępczości są płynne, ponieważ to samo działanie może stanowić odrębne przestępstwo lub być elementem szerszego schematu przestępczego.

Kwestia ta może mieć istotne znaczenie prawne, gdyż *phishing*, w zależności od skutków jakie wywołał, może być kwalifikowany jako oszustwo (art. 286 § 1 k.k.), oszustwo komputerowe (art. 287 § 1 k.k.) lub kradzież z włamaniem art. 279 § 1 k.k.)[49].

Podobny problem ujawnia się przy kwalifikacji czynów polegających na ingerencji w informacje, dane informatyczne lub funkcjonowanie systemów teleinformatycznych. Przykładem jest przestępstwo utrudniania zapoznania się z informacją (art. 268 § 2 k.k.), polegające na niszczeniu, uszkadzaniu, usuwaniu lub zmienianiu zapisu istotnej informacji na informatycznym nośniku danych. Przedmiotem czynności wykonawczej analizowanego przestępstwa są więc dane informatyczne zapisane na nośniku danych. Jeżeli natomiast utrudnienie w zapoznaniu się z informacją będzie rezultatem zachowań polegających na zakłócaniu pracy sieci, czyn ten zostanie zakwalifikowany jako niszczenie danych informatycznych (art. 268a § 1 k.k.) lub zakłócanie systemu komputerowego (art. 269a k.k.)[50].

Instytucjonalne skutki klasyfikacji cyberprzestępczości

Warto także zauważyć, że Steven Furnell, twórca pierwszej klasyfikacji cyberprzestępczości na *computer-assisted crimes* i *computer-focused crimes*, zwracał uwagę na zacieranie się granic między tymi kategoriami[51]. Wydaje się jednak, że refleksja ta została pominięta podczas formułowania klasyfikacji cyberprzestępczości według kategorii *cyber-dependent crimes* i *cyber--enabled crimes*. Istotny jest również fakt, że rozróżnienie cyberprzestępczości na *cyber-dependent crimes* i *cyber-enabled crimes* zostało przyjęte w praktyce publicznej. W związku z tym przestępstwa popełniane z wykorzystaniem systemów teleinformatycznych (ang. *cyber-dependent crimes*) zaczęto traktować jako *stricte* cyberprzestępczość, marginalizując przy tym skalę i znaczenie tradycyjnych przestępstw popełnianych z wykorzystaniem sieci teleinformatycznych (ang. *cyber-enabled crimes*), czego przykładem są wszelkiego rodzaju oszustwa[52]. Takie podejście może budzić pewne wątpliwości

[49] P. Opitek, *Kwalifikacja prawna i opis znamion przestępstw teleinformatycznych. Studium prawno-kryminalistyczne*, Kraków 2023, s. 208–210.

[50] F. Radoniewicz, *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w Działaniu" 2013, nr 13, s. 135–136.

[51] S. Furnell, op. cit., s. 22–23.

[52] J. Lusthaus, op. cit., s. 380.

w świetle ustaleń Furnella, który wskazywał, że oszustwa są popełniane częściej niż technicznie zaawansowane ataki sieciowe[53].

Spostrzeżenie to pozostaje aktualne współcześnie. Z danych opublikowanych przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CERT Polska (ang. *Computer Emergency Response Team*) wynika, że najczęściej zgłaszanym incydentem w 2024 r. było oszustwo komputerowe. Tego rodzaju przestępstwa stanowiły 94,7% wszystkich zgłoszeń (97 995), z czego *phishing* stanowił 40 120 incydentów[54]. Ustalenia te znajdują także potwierdzenie w literaturze naukowej[55] oraz w doniesieniach medialnych[56]. Przyjęło się jednak, że tzw. *stricte* cyberprzestępczość (ang. *cyber-dependent crimes*) powinna być zwalczana przez wyspecjalizowane jednostki, a przestępstwa ułatwiane przez nowe technologie, w szczególności oszustwa (ang. *cyber-enabled crimes*) pozostawiono jednostkom niższego szczebla[57].

Przykładowo, w polskim systemie organów ścigania utworzono Biuro dw. z Cyberprzestępczością Komendy Głównej Policji, a następnie Centralne Biuro Zwalczania Cyberprzestępczości (dalej jako CBZC). Podstawowym zadaniem CBZC jest rozpoznawanie i zwalczanie przestępstw popełnianych przy użyciu systemów informatycznych, systemów teleinformatycznych lub sieci teleinformatycznych oraz zapobieganie takim przestępstwom, a także wykrywanie i ściganie sprawców tych przestępstw[58]. Formalny zakres zadań CBZC jest zatem szeroki i obejmuje zwalczanie zarówno przestępstw, które można popełnić wyłącznie z wykorzystaniem technologii informatycznych, np. DDoS, jak również przestępstw tradycyjnych, które można popełnić dzięki wsparciu technologii cyfrowych, np. oszustwa internetowe[59]. Choć ustawowe zadania CBZC obejmują przestępstwa *cyber-dependent crimes* i *cyber-enabled crimes*, wybrane dokumenty legislacyjne[60] wskazują na to, że działalność CBZC koncentruje się przede wszystkim na sprawach o wysokim stopniu skomplikowania, trudnych technicznie i wielowątkowych oraz mających międzynarodowy charakter[61].

---

[53] S. Furnell, op. cit., s. 22–23.

[54] *Analiza bezpieczeństwa polskiego internetu w 2024 roku*, https://www.gov.pl/web/baza-wiedzy/analiza-bezpieczenstwa-polskiego-internetu-w-2024-roku (data dostępu: 22.03.2026).

[55] I.A. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni: studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 26.

[56] N. Bochyńska, *Cyberprzestępczość. Policja ujawnia dane*, https://cyberdefence24.pl/armia-i-sluzby/cyberprzestepczosc-policja-ujawnia-dane (data dostępu: 26.02.2026)

[57] Home Office, *Cybercrime strategy*, London 2010, s. 21–22.

[58] M. Pomykała, *The Central Cybercrime Bureau as a new Police service established to combat cybercrime*, „Humanities and Social Sciences Quarterly" 2024, t. 31, nr 2, s. 133.

[59] M. Tomczak, *Zwalczanie cyberprzestępczości przez polską Policję*, „Kwartalnik Policyjny" 2024, nr 2(69), s. 7.

[60] Uzasadnienie do rządowego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości, druk sejmowy nr 1742, Sejm RP IX kadencji, s. 3.

[61] M. Przestrzelska, *Służba w walce z cyberprzestępczością*, „Gazeta Policyjna" 2025, nr 1(49), s. 43.

Tym samym postępowania w sprawie prostych oszustw internetowych prowadzone są w jednostkach terenowych Policji, które nie mają odpowiednich zasobów (kadrowych, finansowych i sprzętowych) niezbędnych do realizacji zadań w zakresie zapobiegania oraz minimalizowania skutków przestępstw internetowych[62]. Potwierdza to funkcjonalny podział kompetencji Policji, który nie jest adekwatny do rzeczywistej skali i charakteru cyberprzestępczości. Za rozwiązanie stwierdzonej luki strukturalnej należy jednak uznać utworzenie z dniem 1 marca 2026 r. w strukturach polskiej Policji wydziałów do walki z przestępczością cyfrową. Nowo powołane wydziały będą wspierały m.in. komórki i jednostki organizacyjne Policji w obszarze cyberprzestępczości, a także będą współpracowały z CBZC[63].

Polemika

Zaprezentowane w niniejszej publikacji zagadnienie dotyczy konceptualizacji cyberprzestępczości. Zwrócono uwagę na problem instrumentalizacji pojęcia „cyberprzestępczość" oraz kwestię wyodrębnienia dwóch formalnych kategorii klasyfikacyjnych: *cyber-dependent crimes i cyber-enabled crimes*. Kategorie te, mimo że nie odzwierciedlają rzeczywistej struktury zjawiska, wpływają na kształt struktur organizacyjnych podmiotów odpowiedzialnych za zwalczanie cyberprzestępczości oraz na sposób gromadzenia danych statystycznych i narrację ekspercką[64]. Publikacja rządowego raportu badawczego brytyjskiego Ministerstwa Spraw Wewnętrznych na temat cyberprzestępczości przyczyniła się zatem do powstania błędu kategorialnego. Błąd ten polega na przyjęciu klasyfikacji *cyber-dependent crimes* i *cyber-enabled crimes* jako uniwersalnych kategorii opisujących cyberprzestępczość, bez wyraźnego podkreślenia, że podział ten ma przede wszystkim charakter pomocniczy, porządkujący i pragmatyczny, związany z potrzebami polityki publicznej. Brak przedmiotowej informacji sprawił, że kategorie *cyber-dependent crimes* i *cyber-enabled crimes* zaczęto traktować jako kategorie naukowe, odzwierciedlające rzeczywistą strukturę zjawiska. Wydaje się również, że w procesie formułowania wspomnianych kategorii nie uwzględniono refleksji S. Furnella, który podkreślał, że granice między wyróżnionymi przez niego kategoriami *computer-assisted crimes* i *computer-focused crimes* są niejednoznaczne. Zaproponowany przez niego podział nie opisywał trwałej struktury zjawiska,

62 Najwyższa Izba Kontroli, op. cit., s. 8.

63 *W strukturach Policji powstały wydziały do walki z przestępczością cyfrową*, https://policja.pl/pol/aktualnosci/274058,W-strukturach-Policji-powstaly-wydzialy-do-walki-z-przestepczoscia-cyfrowa.html (data dostępu: 27.02.2026).

64 M. McGuire, S. Dowling, op. cit., s. 5.

lecz miał charakter porządkujący[65]. Głównym celem klasyfikacji Furnella było więc usystematyzowanie problematyki związanej z cyberprzestępczością na potrzeby analizy naukowej. Jej wykorzystanie w sferze publicznej wymaga natomiast uwzględnienia pomocniczego charakteru tego podziału, a także braku jednoznacznych granic między wyróżnionymi kategoriami.

Wnioski

Istotnym problemem badawczym dotyczącym cyberprzestępczości jest konceptualizacja zjawiska oraz wypracowanie jednej uniwersalnej definicji. Brak zgody w przedmiotowym zakresie przyczynił się do formułowania postulatów dotyczących rezygnacji z terminu „cyberprzestępczość" i zmiany sposobu myślenia o tym zjawisku[66]. Przyczyn istniejących nieporozumień należy upatrywać m.in. w instrumentalizacji samego pojęcia, a także w formalizacji kategorii *cyber-dependent crimes* i *cyber-enabled crimes*, które nie odzwierciedlają rzeczywistej struktury zjawiska.

Cyberprzestępczość nie powinna być postrzegana jako nowe i odrębne zjawisko, lecz jako kolejny etap rozwoju przestępczości, wynikający z cyfryzacji społeczeństwa. W rezultacie zasadne jest odwołanie się do szerokiego ujęcia definicyjnego zaproponowanego przez Jonathana Lusthausa, zgodnie z którym cyberprzestępczość to zjawisko obejmujące te formy przestępczości, w których technologia cyfrowa odgrywa istotną rolę w realizacji czynu zabronionego[67], pozostając w funkcjonalnym związku z jego popełnieniem, zwłaszcza gdy komponent cyfrowy stanowi przedmiot zamachu, środek przestępstwa albo czynnik determinujący sposób działania sprawcy. Przez komponent cyfrowy należy przy tym rozumieć element związany z technologią cyfrową, w szczególności system teleinformatyczny, sieć, dane cyfrowe, oprogramowanie, urządzenie lub usługę cyfrową, który może stanowić przedmiot zamachu, środek popełnienia przestępstwa albo element wpływający na sposób działania sprawcy.

Powyższa propozycja ujęcia cyberprzestępczości jest więc wyraźnym postulatem odejścia od sztywnego podziału zjawiska na kategorie. Dalsze postrzeganie cyberprzestępczości przez pryzmat kategorii prowadzi bowiem do mało wartościowych wniosków, które są często rezultatem sporów dotyczących tego, czy dany czyn stanowi *stricte* cyberprzestępstwo, czy jest to raczej tradycyjne przestępstwo popełnione z użyciem nowych technologii. Taki sposób postrzegania cyberprzestępczości utrudnia jej konceptualizację oraz zniekształca obraz rzeczywistej skali zjawiska. Przyjęcie szerokiego ujęcia

[65] S. Furnell, op. cit., s. 22–23.
[66] K.F. Steinmetz, op. cit., s. 13.
[67] J. Lusthaus, op. cit., s. 381.

definicyjnego cyberprzestępczości, a także klasyfikacja przestępstw w oparciu o komponent cyfrowy pozwoliłyby uzyskać bardziej wiarygodny obraz rzeczywistej skali zjawiska.

Należy jednak zaznaczyć, że przytoczona definicja nie powinna być traktowana jako kategoria obejmująca każdy czyn, w którego okolicznościach pojawia się technologia cyfrowa. Problem definiowania cyberprzestępczości nie ma bowiem wyłącznie charakteru terminologicznego, lecz wiąże się z określoną funkcją. W ujęciu analitycznym zaproponowana definicja powinna służyć wyodrębnieniu tych czynów zabronionych, w których komponent cyfrowy ma znaczenie dla sposobu popełnienia przestępstwa. Z kolei w debacie medialnej i politycznej termin ten może pełnić funkcję kategorii zagrożenia, uzasadniającą potrzebę wprowadzania odpowiednich regulacji prawnych.

Warto także zauważyć, że zarówno definicja cyberprzestępczości, jak i podział na kategorie *cyber-enabled* i *cyber-dependent* nie zostały uwzględnione w podstawowych aktach prawa międzynarodowego dotyczących cyberprzestępczości. Zarówno Konwencja Rady Europy o cyberprzestępczości, jak i Konwencja ONZ przeciwko cyberprzestępczości zawierają opis czynów wymagających penalizacji, instrumentów proceduralnych oraz mechanizmów współpracy międzynarodowej. Z kolei inaczej przedstawia się to na poziomie polityki publicznej i dokumentów instytucjonalnych, gdzie nadal widoczna jest logika klasyfikacji cyberprzestępczości.

Przyjęcie komponentu cyfrowego, jako głównego kryterium wyróżniającego cyberprzestępstwa, miałoby także określone implikacje w obszarze polityki publicznej. Bardziej wiarygodny obraz zjawiska cyberprzestępczości przyczyniłby się do zmiany dyskursu naukowego. Można przypuszczać, że skutkowałoby to przesunięciem rozmów z zagadnień dotyczących spektakularnych i technicznie zaawansowanych ataków sieciowych na kwestie poświęcone przestępczości, która jest dominująca i najbardziej uciążliwa społecznie.

Przedstawione szerokie ujęcie definicyjne cyberprzestępczości pozwala na odejście od sztucznie skonstruowanej złożoności zjawiska, która wynika z formalizacji dwóch kategorii: *cyber-enabled crimes* i *cyber-dependent crimes*. Ograniczenie dominującej roli perspektywy opartej na wspomnianych kategoriach sprzyjałoby lepszemu rozumieniu i konceptualizacji cyberprzestępczości. Przedstawiona definicja ma przede wszystkim odpowiadać na potrzeby nauki oraz praktyki instytucjonalnej, zwłaszcza w zakresie rozpoznawania rzeczywistej roli technologii cyfrowej w mechanizmach przestępczych oraz ukierunkowania czynności wykrywczych oraz prawidłowego zabezpieczania dowodów cyfrowych.

Brak jednej szeroko akceptowanej definicji stanowi główny, choć nie jedyny problem w konceptualizacji cyberprzestępczości[68]. Zróżnicowane podejście

[68] R. Barn, B. Barn, *An ontological representation of a taxonomy for cybercrime*, [w:] *Proceedings of the 24th European Conference on Information Systems (ECIS 2016)*, Istanbul 2016, s. 1.

do cyberprzestępczości przekłada się także na stosowanie różnorodnej terminologii[69] oraz niejednoznaczną ocenę zjawiska, zależną od jurysdykcji poszczególnych państw[70].

Przyjęcie szerokiego ujęcia definicyjnego cyberprzestępczości nie oznacza jednak konieczności całkowitego odrzucenia dotychczasowych klasyfikacji. Podział cyberprzestępczości na *cyber-dependent crimes* i *cyber-enabled crimes* zachowuje bowiem określoną wartość analityczną, o ile jest traktowany jako narzędzie pomocnicze, a nie jako wyczerpujący opis struktury zjawiska. Wspomniana klasyfikacja ma bowiem wartość porządkująca, a więc pozwala odróżnić czyny, które nie mogłyby istnieć bez technologii cyfrowej, od czynów tradycyjnych, których skala, zasięg albo sposób popełnienia zostały zmienione przez technologie cyfrowe. Znaczenie omawianego podziału ujawnia się również z punktu widzenia oceny obowiązującego stanu prawnego. Wyodrębnienie przestępstw, w których technologia cyfrowa odgrywa istotną rolę, pozwala ocenić adekwatność obowiązujących regulacji prawnych oraz ewentualną potrzebę formułowania postulatów *de lege ferenda*. Kolejny walor wspomnianego podziału ujawnia się na płaszczyźnie badawczej, choć ma ograniczony zakres. Skupienie uwagi na przestępstwach *cyber-dependent* pozwala wyodrębnić i analizować te formy cyberprzestępczości, które cechuje wyraźny komponent cyfrowy.

Wykaz literatury

Adamski A., *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, TNOiK, Toruń 2001.

Adamski A. (red.), *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji*, TNOiK, Toruń 1994.

Akdemir N., Sungur B., Başaranel B.U., *Examining the challenges of policing economic cybercrime in the UK*, „Güvenlik Bilimleri Dergisi" 2020.

Akhgar B. i in., *Consolidated taxonomy and research roadmap for cybercrime and cyberterrorism*, [w:] B. Akhgar, B. Brewster (red.), *Combatting cybercrime and cyberterrorism: challenges, trends and priorities*, Springer, Cham 2016.

Barlow J.P., *Selling wine without bottles: the economy of mind on the global net*, „Duke Law & Technology Review" 2019, t. 18.

Barn R., Barn B., *An ontological representation of a taxonomy for cybercrime*, [w:] *Proceedings of the 24th European Conference on Information Systems (ECIS 2016)*, AIS Electronic Library, Istanbul 2016.

Bochyńska N., *Cyberprzestępczość. Policja ujawnia dane*, https://cyberdefence24.pl/armia-i-sluzby/cyberprzestepczosc-policja-ujawnia-dane.

[69] M. McGuire, *It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime*, [w:] R. Leukfeldt, T.J. Holt (red.), *The human factor of cybercrime*, New York 2020, s. 6.

[70] E.C. Viano, *Cybercrime: definition, typology, and criminalization*, [w:] E.C. Viano (red.), *Cybercrime, organized crime, and societal responses. International approaches to prevention and intervention*, Cham 2020, s. 3.

Bossler A.M., Berenblum T., *Introduction: new directions in cybercrime research*, „Journal of Crime and Justice" 2019, t. 42, nr 5.
Brenner S.W., *Toward a criminal law for cyberspace: distributed security*, „Boston University Journal of Science & Technology Law" 2004, t. 10.
Bryant R., *The challenge of digital crime*, [w:] R. Bryant (red.), *Investigating digital crime*, John Wiley & Sons, Chichester 2008.
Button M. i in., *Assessing the seriousness of cybercrime: the case of computer misuse crime in the United Kingdom and the victims' perspective*, „Criminology & Criminal Justice" 2025, t. 25, nr 2.
Clough J., *Principles of cybercrime*, Cambridge University Press, Cambridge 2010.
Dupont B., Whelan C., *Enhancing relationships between criminology and cybersecurity*, „Journal of Criminology" 2021, t. 54, nr 1.
Furnell S., *Cybercrime: vandalizing the information society*, Pearson Education Limited, London 2002.
Gordon S., Ford R., *On the definition and classification of cybercrime*, „Journal in Computer Virology" 2006, t. 2, nr 1.
Grabosky P.N., *Virtual criminality: old wine in new bottles?*, „Social & Legal Studies" 2001, t. 10, nr 2.
Holt T.J., Bossler A.M., *An assessment of the current state of cybercrime scholarship*, „Deviant Behavior" 2014, t. 35, nr 1.
Home Office, *Cybercrime strategy*, The Stationery Office, London 2010.
Jaroszewska I.A., *Wybrane aspekty przestępczości w cyberprzestrzeni: studium prawnokarne i kryminologiczne*, WPiA UWM, Olsztyn 2017.
Koops B.-J., *The Internet and its opportunities for cybercrime*, „SSRN Electronic Journal" 2010.
Kshetri N., *The global cybercrime industry: economic, institutional and strategic perspectives*, Springer, Berlin 2010.
Kusak M., *Dostęp do danych elektronicznych dotyczących treści w postępowaniu karnym – wyzwania krajowe i międzynarodowe*, „Gdańskie Studia Prawnicze" 2024, nr 2(63).
Leukfeldt R., Notté R., Malsch M., *Slachtofferschap van online criminaliteit: een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit. Samenvatting*, Amsterdam 2018, https://open.overheid.nl/documenten/ronl-3cc3344c-c5c9-4184-8886-7a9333800228/pdf.
Lewulis P., *O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych*, „Prokuratura i Prawo" 2021, nr 3.
Lusthaus J., *Reconsidering crime and technology: what is this thing we call cybercrime?*, „Annual Review of Law and Social Science" 2024, t. 20 nr 1.
McGuire M., *It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime*, [w:] R. Leukfeldt, T.J. Holt (red.), *The human factor of cybercrime*, Routledge, New York 2020.
McGuire M., Dowling S., *Cybercrime: a review of the evidence. Research Report 75. Summary of key findings and implications*, Home Office, London 2013.
Najwyższa Izba Kontroli, *Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości*, Informacja o wynikach kontroli, nr ewid. 125/2022/P/21/042/KPB, NIK, Warszawa 2022.
Opitek P., *Kwalifikacja prawna i opis znamion przestępstw teleinformatycznych. Studium prawno-kryminalistyczne*, KSSiP, Kraków 2023.
Phillips K. i in., *Conceptualizing cybercrime: definitions, typologies and taxonomies*, „Forensic Sciences" 2022, t. 2, nr 2.

Pomykała M., *The Central Cybercrime Bureau as a new Police service established to combat cybercrime*, „Humanities and Social Sciences Quarterly" 2024, t. 31, nr 2.
Przestrzelska M., *Służba w walce z cyberprzestępczością*, „Gazeta Policyjna" 2025, nr 1(49).
Radoniewicz F., *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w Działaniu" 2013, nr 13.
Sarre R., Lau L.Y.-C., Chang L.Y.C., *Responding to cybercrime: current trends*, „Police Practice and Research" 2018, t. 19, nr 6.
Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8.
Sobczak J., *Przestępczość w cyberprzestrzeni między przepisami polskimi a międzynarodowymi*, „Cybersecurity and Law" 2021, t. 1, nr 1.
Steinmetz K.F., *Against cybercrime: toward a realist criminology of computer crime*, Routledge, London 2023.
Szczepaniec M., *Komputer jako narzędzie przestępstwa*, „Zeszyty Prawnicze" 2012, t. 12, nr 2.
Tomczak M., *Zwalczanie cyberprzestępczości przez polską Policję*, „Kwartalnik Policyjny" 2024, nr 2(69).
Urbańska N., *Cyberprzestępczość i wynikające z niej zagrożenia*, „Cybersecurity & Cybercrime" 2025, t. 1, nr 7.
Viano E.C., *Cybercrime: definition, typology, and criminalization*, [w:] E.C. Viano (red.), *Cybercrime, organized crime, and societal responses. International approaches to prevention and intervention*, Springer, Cham 2020.
Voce I., Morga A., *Cybercrime in Australia 2023, Statistical Report 43*, Australian Institute of Criminology, Canberra 2023.
Wall D.S., *Catching cybercriminals: policing the Internet*, „International Review of Law, Computers & Technology" 1998, t. 12, nr 2.
Wall D.S., *Cybercrime: the transformation of crime in the information age*, Polity Press, Cambridge 2007.
Wall D.S., *Cybercrimes: new wine, no bottles?*, [w:] P. Davies, P. Francis, V. Jupp (red.), *Invisible crimes*, Macmillan Press, London 1999.
Wasilewski J., *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15(8).
Yar M., *The novelty of 'cybercrime': an assessment in light of routine activity theory*, „European Journal of Criminology" 2005, t. 2, nr 4.
Zbrojewska M. i in., *Jak definiujemy cyberprzestępstwo?*, „Informatics, Control, Measurement in Economy and Environment Protection" 2016, t. 6, nr 2.

Summary

Cybercrime – from conceptual ambiguity to a broad definition

Keywords: criminal law, cybercrime, cybercrime definition, classification of cybercrime, cybercrime conceptualisation, digital technologies.

The development of crime involving information and communication technologies has given rise to the concept of cybercrime. Despite the numerous controversies surrounding its semantic scope, the term is widely used in the public sphere. This state of affairs gives rise to difficulties in the

conceptualisation of cybercrime and, consequently, in combating it and conducting scientific research. With the above in mind, the main aim of this publication is to analyse existing approaches to cybercrime, to demonstrate the complexity of the phenomenon, and to show how the widely accepted distinction between cyber-dependent crimes and cyber-enabled crimes affects institutional practice. These findings provide the basis for formulating a broad definitional understanding of cybercrime. To address the research problem, the study employs the monographic method, supplemented by critical literature analysis. On the basis of both domestic and international scholarly literature, it is argued that the principal source of misunderstandings surrounding this issue lies in the instrumentalisation of the concept of cybercrime and in the formalised classification of the phenomenon into two categories, namely cyber-dependent crimes and cyber-enabled crimes. Although these categories do not reflect the actual structure of cybercrime, they nevertheless perform an ordering and organisational function. The solution to the existing problem is therefore to limit the dominant role of a perspective based on a rigid division of the phenomenon and to adopt a broad definition of cybercrime, according to which it encompasses those forms of crime in which digital technology plays a significant role in the commission of prohibited act.