Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury
Quarterly of the National School of Judiciary and Public Prosecution
Zeszyt 1 (45)/2022

Wybrane aspekty prawnokarne, kryminalistyczne i kryminologiczne cyberprzestępczości

DOI:10.53024/2.1.45.2022

ANDRZEJ LEBIEDOWICZ*

STRESZCZENIE

Powołanie do istnienia Centralnego Biura Zwalczania Cyberprzestępczości potraktować należy jako wzmożenie – w ramach polityki karnej – wysiłków ukierunkowanych na zwalczanie nasilającej się w ostatnich latach cyberprzestępczości. Przy okazji tego wydarzenia zasadne jest odnieść się w ramach niniejszej publikacji do szeregu aspektów natury prawno-karnej, kryminalistycznej oraz kryminologicznej, dotyczących tego wyspecjalizowanego rodzaju przestępczości. Poruszono w niej zatem kwestię definiowania cyberprzestępczości, przestępczości komputerowej, synonimiczności tych terminów, podziału cyberprzestępstw oraz przestępstw komputerowych, jak też technik ich popełnienia, typów sprawców oraz technik zacierania przez nich śladów popełnionych przestępstw. Odniesiono się także do zagadnień natury metodologicznej w zakresie prowadzenia postępowań przygotowawczych w przypadkach ataków phishingowych oraz ataków typu odmowa dostępu DoS. Zaakcentowano też rolę współczesnej informatyki śledczej w badaniu śladów cyfrowych traktowanych jako pełnoprawne ślady kryminalistyczne. Końcowo zaś nawiązano do kwestii kryptowalut w cyberprzestrzeni, w kontekście popełnianej na tej płaszczyźnie przestępczości.

Słowa kluczowe: cyberprzestępstwo, cyberprzestrzeń, informatyka, kryptowaluta, haker, Ddos atack

* Prokurator Prokuratury Okręgowej w Lublinie, Zastępca Prokuratora Okręgowego w Lublinie.

WSTĘP

Istnienie współczesnego świata jest w całości uzależnione od funkcjonowania komputerów, jako że niemal każda dziedzina życia codziennego, gospodarczego czy też politycznego jest obecnie skomputeryzowana, co oczywiście rzutuje na obraz współczesnego świata przestępczego[1]. Dynamicznie postępujący rozwój społeczeństwa informacyjnego i zarazem informatycznego w dobie rosnącego znaczenia informacji określanego mianem rewolucji informacyjnej generuje potrzebę nadania niematerialnej z natury rzeczy informacji rangi autonomicznego dobra prawnego zasługującego na ochronę, jaka przysługuje energii czy też materii[2]. „Internet stał się uznanym i najbardziej demokratycznym środkiem przekazu ze względu na znikomy zakres cenzury przekazywanych informacji. Niesie to ze sobą wiele niebezpieczeństw i potencjalnie każda z istniejących setek milionów skrzynek elektronicznych może posłużyć jako narzędzie do popełnienia przestępstwa"[3]. Wykreowana przez komputery zespolone w sieci teleinformatycznej cyberprzestrzeń stała się zdaniem amerykańskich strategów, specjalizujących się w bezpieczeństwie informacji, jedną z pięciu przestrzeni; pozostałe to: morze, kosmos, ziemia i powietrze[4]. Analogicznie jak w przypadku świata przestępczego, w świecie cyberprzestrzeni pojawiło się cyberprzestępstwo jako zjawisko nowe, niemniej jednak rozwijające się w dość zastraszającym tempie w krajach silnie zinformatyzowanych oraz określanych jako wysoko rozwinięte[5]. Jako kwestię wciąż otwartą należy traktować zakreślenie ram samego cyberprzestępstwa, jego zakresu przedmiotowego, w kontekście ścierających się koncepcji, z których jedna zakłada, że czynnikiem determinującym jest wymóg zaistnienia przestępstwa w całości, w tym także ze swoimi skutkami w cyberprzestrzeni, druga zaś, że wystarczającym do zakwalifikowania danego zachowania do kategorii cyberprzestępstwa jest wystąpienie w cyberprzestrzeni jedynie niektórych fragmentów składających się na opis danego przestępstwa[6]. Koncentrując się na kwestii cyberprzestrzeni, należy mieć na uwadze okoliczność, że „komputery i sieć komputerowa mogą służyć do popełnienia przestępstwa na kilka sposobów: komputer lub sieć mogą być narzędziem

---

1 Zob. M. Bubeła, *Informatyka śledcza i techniki anti-forensic w świetle polskiego prawa*, [w:] *Przestępstwa rzadko podejmowane przez organy ścigania. Aspekty kryminalistyczne, materialnoprawne i procesowe*, M. Trybus, T. Wilk (red.) Rzeszów 2013, s. 53.

2 Zob. U. Siebert, *Informationrecht und Recht der Informationstechnik*, „Neue Juridische Wochenchrift" 1989, Heft 41, s. 2572-2573.

3 W.A. Kasprzak, *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Warszawa 2015, s. 50.

4 Zob. T. Formicki, *Wywiad i kontrwywiad jako kluczowe komponenty walki informacyjnej*, Warszawa 2020, s. 202.

5 Zob. M. Zbrojewska, V. Morozov, S. Biedron, T. Panskyi, *Jak definiujemy cyberprzestępstwo?*, „Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska" 2016, nr 2, s. 65.

6 Zob. B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Kraków 2000, s. 25.

przestępstwa (zostają użyte do jego popełnienia), komputer lub sieć mogą być celem przestępstwa (ofiarą), komputer lub sieć mogą być użyte do zadań dodatkowych związanych z popełnieniem przestępstwa (na przykład do przechowywania informacji o nielegalnej sprzedaży narkotyków)"[7]. Zagrożenie cyberprzestępczością jest tym bardziej poważne, jeśli zważy się na towarzyszące jej aspekty takie jak: transgraniczność (przestępstwo może być dokonane z dowolnego miejsca na ziemi), ogólnodostępność (do popełnienia przestępstwa wystarczy podstawowa wiedza informatyczna oraz posiadanie urządzenia końcowego, anonimowość (świat wirtualny daje ogromne szanse na zachowanie anonimowości), niematerialny charakter (dane funkcjonujące w cyberprzestrzeni mają charakter niematerialny), brak scentralizowanego ośrodka kontroli (transgraniczny charakter popełnianych przestępstw oraz biurokratyczne bariery na płaszczyźnie współpracy międzynarodowej nierzadko są przyczyną braku sukcesów na polu walki z tym rodzajem przestępczości)[8]. Skutecznie działający system prawny winien obronić trzy główne aspekty bezpieczeństwa informacji, danych komputerowych, a także systemów informatycznych, takich jak: dostępność, integralność oraz poufność[9]. Mając na uwadze powyższe, pozytywnie należy ocenić powołanie – na podstawie ustawy z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości[10] – nowego organu do walki z cyberprzestępczością w postaci Centralnego Biura Zwalczania Cyberprzestępczości, czemu towarzyszą zmiany organizacyjne także w obrębie prokuratury. Należy przypuszczać, że nowa jednostka policyjna stanie się skutecznym narzędziem do walki z cyberprzestępcami.

DEFINICJE CYBERPRZESTĘPCZOŚCI I PRZESTĘPCZOŚCI KOMPUTEROWEJ ORAZ ICH WZAJEMNE RELACJE

Mimo że takie terminy jak cyberprzestępczość, czy też przestępczość komputerowa nie funkcjonują w obowiązującym stanie prawnym w roli wyrażeń ustawowych, odnoszą się one do jednego z największych zjawisk przestępczych w dzisiejszych czasach[11].

---

7 B. Hołyst, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, „Prokuratura i Prawo" 2011, nr 1. s. 17.

8 Zob. M. Zbrojewska, V. Morozov, S. Biedron, T. Panskyi, *Jak definiujemy…*, s. 65.

9 F. Radoniewicz, *Odpowiedzialność karna za przestępstwa hackingu*, „Prawo w działaniu. Sprawy karne" 2013, nr 13, s. 124.

10 Ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz. U. z 2021 r. poz. 2447).

11 Zob. J. Wasilewski, *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15/16, s. 149.

Cyberprzestępczość może być definiowana na różne sposoby, a do jej podstawowych znamion należy zaliczyć działanie w cyberprzestrzeni oraz generowanie śladów cyfrowych[12].

Punktem wyjścia do dalszych rozważań na temat definicji omawianych pojęć należy uczynić termin „cyberprzestrzeń". „Cyberprzestrzeń bowiem w ujęciu funkcjonalnym tworzona jest najogólniej przez: a) technologiczną infrastrukturę umożliwiającą jej funkcjonowanie, w tym zachodzenie procesów wymiany danych oraz informacji (m.in. wszystkie elementy tworzące sieci komputerowe oraz sieci telekomunikacyjne – komputery, serwery, centrale, łącza, wraz z oprogramowaniem wyposażonym w interfejsy użytkownika), b) specyficzne reguły, zarówno prawne, jak też i te niesformalizowane, rządzące zachowaniami w jej obszarze, oraz c) działania użytkowników poruszających się po jej zasobach oraz podejmujących wzajemne interakcje. W uproszczeniu zatem uznać należy, że cyberprzestrzeń jest obszarem społecznego doświadczenia podejmowanego za pośrednictwem technologii informatycznych – głównie komputerów z zainstalowanym oprogramowaniem, gdzie jednostki, z pominięciem geograficznych granic oraz wymiarów, mogą wzajemnie oddziaływać na siebie, wywołując także określone (jak najbardziej rzeczywiste) skutki prawne"[13].

W tym miejscu tylko hasłowo odnieść się należy do najbardziej mrocznego obszaru cyberprzestrzeni, czyli Darknetu. E. Omsby zauważa, że „w gęstwinie prywatnych sieci zapewniających poziom anonimowości nieosiągalny w sieci zindeksowanej kwitnie handel narkotykami i bronią, reklamują się płatni zabójcy i hakerzy gotowi włamać się do komputera naszego wroga, a najbardziej zdeprawowani dewianci mogą zaspokoić apetyt, ściągając najdziwniejsze materiały pornograficzne"[14].

Komisja Europejska w swoim Komunikacie do Parlamentu Europejskiego, Rady oraz Komitetu Regionów o kierunku ogólnej strategii zwalczania cyberprzestępczości z dnia 25 lipca 2007 r. posłużyła się pojęciem *cybercime* (ang. cyberprzestępczość), przez który rozumie czyny o charakterze przestępczym popełnione z wykorzystaniem sieci łączności elektronicznej oraz systemów informatycznych, względnie skierowane przeciwko takim systemom i sieciom, przy czym rozróżnia ich podział na trzy grupy:

---

[12] Zob. P. Opitek, *Przestępczość w pracy prokuratora*, „Prokuratura i Prawo" (wydanie specjalne) 2018, s. 5.

[13] J. Wasilewski, *Cyberprzestrzeń – wybrane aspekty prawno karne i kryminalistyczne*, Białystok 2017, s. 40-41.

[14] E. Omsby, *Darknet*, Kraków 2019, s. 20.

1) pierwszą, skupiającą „tradycyjne" formy przestępstw (oszustwa, fałszerstwa popełnione z wykorzystaniem elektronicznych sieci informatycznych oraz systemów informatycznych);

2) drugą, do której zalicza publikację nielegalnych treści za pośrednictwem mediów elektronicznych (np. materiałów nawołujących do nienawiści na tle rasowym lub treści związanych z seksualnym wykorzystaniem dzieci);

3) trzecią, w której obrębie mieszczą się przestępstwa typowe dla sieci łączności elektronicznej, takie jak sabotaż komputerowy, ataki *denial of service* czy też ataki przeciwko systemom informatycznym[15].

Jednocześnie na gruncie wskazanego dokumentu zaznaczono, że z uwagi na brak wypracowania jednolitej definicji cyberprzestępczości pojęcia takie jak: „przestępczość komputerowa", „cyberprzestępczość", „przestępczość przy użyciu zaawansowanych technologii" czy też „przestępczość związana z komputerami" są używane zamiennie[16].

Na gruncie polskiego prawodawstwa nie stworzono jednolitej definicji cyberprzestępczości, a samo pojęcie przestępczości komputerowej nie doczekało się nawet jednoznacznego zdefiniowania na gruncie ustawy – Kodeks karny z dnia 6 czerwca 1997 r.[17]. Lukę tę wypełniono natomiast wieloma – funkcjonującymi doraźnie (w zależności od potrzeb) – definicjami bazującymi na podstawowym założeniu, że są to czyny zabronione popełnione z wykorzystaniem komputerów oraz Internetu[18].

W ramach przyjętej w dniu 25 czerwca 2013 r., w drodze uchwały Rady Ministrów, Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej przyjęto, że cyberprzestępstwem jest czyn zabroniony popełniony w obrębie cyberprzestrzeni, czyli w obszarze przeznaczonym do przetwarzania i wymiany informacji, a tworzonej przez systemy teleinformatyczne opisane w art. 3 ust. 3 ustawy z dnia 17 maja 2005 r. o informatyzacji podmiotów realizujących zadania publiczne[19], jak też z powiązaniami zachodzącymi pomiędzy nimi oraz relacjami z użytkownikami[20]. Wskazany dokument został zastąpiony przez Krajowe Ramy Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022. Natomiast już 22 października 2019 r.

---

15 Zob. M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7-8, s. 247.

16 Zob. B. Oręziak, *Cyberprzestępczość w aspektach proceduralnych. Dowody elektroniczne, a nowoczesne formy przestępczości*, Warszawa 2019, s. 43.

17 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2021 r. poz. 2345, dalej: k.k.).

18 Zob. M. Stefanowicz, *Cyberprzestępczość – próba diagnozy zjawiska*, „Kwartalnik Policyjny" 2017, nr 4, s. 20.

19 Ustawa z dnia 17 maja 2005 r. o informatyzacji podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570, ze zm.).

20 Zob. M. Stefanowicz, *Cyberprzestępczość…*, s. 20.

Rada Ministrów podjęła uchwałę w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, który to dokument zaczął obowiązywać od 31 października 2019 r., zastępując tym samym Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-2022.

M. Stefanowicz słusznie zauważa, że sformułowana przez Interpol definicja cyberprzestępczości jest bardzo praktyczna, gdyż koncentruje się na określeniu tego zjawiska w dwóch ujęciach:

a) wertykalnym (dotyczącym przestępstw specyficznych dla cyberprzestrzeni, a więc takich, które tam mogą być dokonywane, np. sabotaż komputerowy, *hacking*),

b) horyzontalnym (jego istotą jest założenie popełniania przestępstw z wykorzystaniem technik komputerowych, np. pranie lub fałszowanie pieniędzy czy też oszustwa komputerowe)[21].

Z kolei wypracowana podczas X Kongresu ONZ w sprawie Zapobiegania przestępczości i traktowaniu przestępstw (*Tenth United Nation Congress on the Prevention of Crime and the Treatment of Offenders*) definicja wprowadziła podział na:

– cyberprzestępstwo *sensu largo* (przestępstwo dotyczące komputerów), obejmujące wszystkie nielegalne działania, które są popełniane przy zastosowaniu, względnie skierowane przeciwko sieciom komputerowym, w tym m.in. nielegalne posiadanie, rozpowszechnianie lub udostępnianie informacji przy pomocy komputera bądź sieci;

– cyberprzestępstwo *sensu stricto* (przestępstwo komputerowe), które obejmuje wszystkie działania noszące znamiona nielegalności wymierzone przeciwko bezpieczeństwu systemów komputerowych oraz elektronicznie przetwarzanych przez te systemy danych, a dokonywane z wykorzystaniem operacji elektronicznych[22].

Na gruncie Konwencji Rady Europy o cyberprzestępczości sporządzonej w Budapeszcie dnia 23 listopada 2001 r. w obrębie definicji cyberprzestępczości ulokowano takie jej przejawy jak:

1) umyślny, bezprawny dostęp do całości lub części systemu informatycznego (popełniony poprzez naruszenie zabezpieczeń, z zamiarem pozyskania danych informatycznych lub innym nieuczciwym zamiarem czy też w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym);
2) umyślne, bezprawne przechwytywanie za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych, do, z lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi

[21] Zob. *ibidem*, s. 20.

[22] Zob. K. Witek, *Przestępczość komputerowa – aspekty prawne*, „Edukacja – Technika – Informatyka" 2018, nr 2/24, s. 41.

z systemu informatycznego przekazującego takie dane informatyczne (przestępstwo musi zostać popełnione z nieuczciwym zamiarem lub w związku z systemem informatycznym, który jest połączony z innym systemem informatycznym);
3) umyślne, bezprawne niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych;
4) umyślne, bezprawne, poważne zakłócenie funkcjonowania systemu informatycznego poprzez wprowadzenie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych;
5) produkcja, sprzedaż, pozyskiwanie z zamiarem wykorzystania, importowanie, dystrybucja lub inne udostępnianie urządzenia, w tym również programu komputerowego, przeznaczonego, względnie przystosowanego przede wszystkim dla celów popełnienia któregokolwiek z przestępstw, czy też hasła komputerowego, kodu dostępu, jak również podobnych danych umożliwiających dostęp do całości lub części systemu informatycznego z zamiarem wykorzystania dla popełnienia któregokolwiek z przestępstw[23].

Konkludując, stwierdzić należy, że cyberprzestępczość to przestępczość mająca miejsce w cyberprzestrzeni (stanowiącej przestrzeń do przechowywania, przetwarzania jak też obrotu informacji generowanej przez systemy elektroniczne, w tym przede wszystkim Internet). W szerokim ujęciu obejmuje ona ogół inkryminowanych zachowań dokonywanych przy wykorzystaniu urządzeń teleinformatycznych, a w ujęciu wąskim tylko takie zamachy na dobra prawne, których realizacja nie będzie możliwa poza cyberprzestrzenią[24].

P. Lewulis zwrócił uwagę, że pojęcia „cyberprzestępczość" i „przestępczość komputerowa", pomimo braku ścisłych definicji legalnych, są szeroko obecne w piśmiennictwie naukowym, publicystyce, a także dokumentach oficjalnych[25].

Na mnogość synonimów oraz nieostrość znaczenia „przestępczości komputerowej" zwrócił uwagę już A. Adamski w 2000 r., akcentując bardziej publicystyczny niż naukowy charakter tych pojęć[26].

Z kolei przestępczość komputerowa jest definiowana jako zjawisko kryminologiczne, które obejmuje wszelkie zachowania o charakterze przestępczym powiązane z funkcjonowaniem elektronicznego przetwarzania danych, godzące

---

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

[24] Zob. J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 88.

[25] Zob. P. Lewulis, *O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych*, „Prokuratura i Prawo" 2021, nr 3, s. 12.

[26] Zob. A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 30.

w sposób bezpośredni w przetwarzaną informację czy też w jej nośnik, jak też w obieg w komputerze oraz całym systemie połączeń komputerowych i prawo do programu komputerowego[27].

Nie sposób jest odmówić słuszności twierdzeniom wysuwanym przez P. Lewulisa proponującego odstąpienie od traktowania na zasadzie synonimiczności cyberprzestępczości oraz przestępczości komputerowej. Autor ten podniósł bowiem na gruncie literatury przedmiotu, że: „(…) cyber to pierwszy człon wyrazów złożonych wskazujący na ich związek z informatyką, a zwłaszcza z Internetem, albo wręcz, że jest to «cząstka dodawana do rzeczowników i przymiotników oznaczająca, że są one związane z komunikowaniem się przez sieć komputerową lub z wirtualną rzeczywistością». W świetle takiego założenia przedrostek cyber (w tym w wyrazie cyberprzestępczość) nie powinien być stosowany do określania zjawisk i zdarzeń oderwanych od związku z siecią informatyczną, czyli mających miejsce poza «cyberprzestrzenią» tworzoną przez więcej niż jeden system komputerowy (…). W konsekwencji «cyberprzestępczość» nie może stanowić prawidłowego zamiennika dla «przestępczości komputerowej» na gruncie merytorycznym wynikającym z analizy logicznej. Wykorzystanie sieci jest oczywiście bardzo częstym elementem *modus operandi* sprawców np. włamania do systemów komputerowych, lecz nie stanowi niezbędnego znamienia takiego czynu. Wywołanie szkód poprzez wprowadzenie do sytemu złośliwego oprogramowania czy też uszkodzenie danych, uzyskanie nieautoryzowanego dostępu do systemu lub danych czy digitalizacja dziecięcej pornografii na domowym komputerze – wszystkie te i wiele innych czynów bezpośrednio związanych z wykorzystaniem komputera może być popełnionych *offline*"[28].

Powyższe uwagi – ze wszech miar zasadne i celne jako dotykające istoty tej skądinąd złożonej materii – winny zatem być wykorzystane w przyszłości w przypadku ewentualnego formułowania ustawowych definicji legalnych „cyberprzestępczości" oraz „przestępczości komputerowej".

Dynamiczny rozwój technologiczny doprowadził do wykreowania kolejnej przestrzeni, tzw. cyberprzestrzeni. Stała się ona nowego typu przestrzenią społeczną opartą na kontakcie zdalnym (nierzadko anonimowym), w której zagościła przestępczość, a taki stan rzeczy sprzyja konwergencji technologii komputerowej i przestępczości. Autor niniejszej publikacji jest zwolennikiem prowadzenia przez organy ścigania w trybie czynności operacyjno-rozpoznawczych wzmożonej, jak najszerszej inwigilacji najbardziej kryminogennego jej obszaru w postaci Darknetu,

---

[27] Zob. M. Białkowski, *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Warszawa 2020, s. 43.

[28] P. Lewulis, *O rozgraniczeniu definicyjnym…*, s. 23-24.

stanowiącego platformę wymiany m.in.: przedmiotów, których posiadanie oraz którymi obrót jest zabroniony, owoców popełnianych czynów zabronionych, jak też myśli przestępczej, swoistego *know-how* popełniania przestępstw. Wnikliwe oraz przede wszystkim stałe monitorowanie tej płaszczyzny może dostarczyć wielu cennych informacji, które po poddaniu analizie kryminalnej ułatwią opracowanie szerszej koncepcji walki z cyberprzestępczością nie tylko na poziomie operacyjnym, lecz także taktycznym i strategicznym, co winno wymiernie przyczynić się do oczyszczenia cyberprzestrzeni z negatywnych zachowywań prawnokarnie relewantnych.

RODZAJE CYBERPRZESTĘPSTW ORAZ PRZESTĘPSTW KOMPUTEROWYCH

Cyberprzestępstwa czy też przestępstwa komputerowe nie mają jednorodnego charakteru i podlegają różnorodnym podziałom na podkategorie wynikającym z ich specyfiki. Odnosząc się bowiem do kwestii podziału cyberprzestępstw, można wyróżnić dwie ich podstawowe kategorie:

1) charakterystyczne dla cyberprzestępczości, w których przedmiotem ataku jest komputer, jak też szeroko pojęte przetwarzanie danych w systemach informatycznych (w ramach tej grupy można wyróżnić takie czyny jak: podsłuch komputerowy – *sniffing*, nieuprawnione uzyskanie informacji – *hacking*, podawanie się za inną osobę w ramach funkcjonowania fałszywego profilu, udaremnianie dostępu do danych informatycznych, sabotaż komputerowy, oszustwo komputerowe, rozpowszechnienie złośliwych programów oraz *cracking*, stosowanie narzędzi hackerskich);
2) popełniane z wykorzystaniem sieci Internet, w których komputer jest wyłącznie środkiem do jego popełnienia (w obrębie tej grupy można wskazać takie przejawy inkryminowanej działalności jak: składanie propozycji obcowania płciowego z małoletnim, obrazę uczuć religijnych, handel fikcyjnymi kosztami, publiczne propagowanie lub pochwalanie zachowań o charakterze pedofilskim, zbywanie własnego lub cudzego dokumentu tożsamości, nawoływanie do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo z uwagi na bezwyznaniowość w ramach szeroko pojętej mowy nienawiści, publiczne propagowanie faszystowskiego lub innego totalitarnego ustroju państwa, oszustwa popełniane za pośrednictwem sieci Internet, najczęściej na portalach aukcyjnych)[29].

[29] M. Stefanowicz, *Cyberprzestępczość…*, s. 20.

Przytoczony już powyżej podział cyberprzestępstw (w ramach definicji przez egzemplifikację) wynikający z konwencji budapeszteńskiej obejmuje przestępstwa:

1) przeciwko poufności, integralności i dostępności danych informatycznych oraz systemów (nielegalny dostęp lub przechwytywanie danych, naruszenie integralności danych lub systemu, niewłaściwe użycie urządzeń);

2) komputerowe (fałszerstwo lub oszustwo komputerowe);

3) z uwagi na charakter zawartych danych (przestępstwa związane z pornografią dziecięcą);

4) związane z naruszaniem prawa autorskiego i praw pokrewnych[30].

W świetle ostatniej z przedstawionych klasyfikacji przestępstwa komputerowe stanowią zatem podkategorię cyberprzestępstw. Odmiennie natomiast uważają B. Hołyst oraz J. Pomykała, traktujący cyberprzestępczość (pojmowaną jako rodzaj przestępczości gospodarczej, w której komputer jest albo narzędziem, albo przedmiotem przestępstwa) jako podkategorię przestępczości komputerowej[31].

Międzynarodowa Organizacja Policji Kryminalnych Interpol z kolei podzieliła cyberprzestępstwa na:

a) zamachy, polegające na naruszeniu praw dostępu do zasobów (w szczególności chodzi tu o *hacking* polegający na nieuprawnionym wejściu do systemu informatycznego, przechwytywaniu danych, kradzież czasu polegającą na korzystaniu z systemu poza uprawnionymi godzinami, jak też na modyfikacji zasobów z wykorzystaniem konia trojańskiego, bomby logicznej, wirusa oraz robaka komputerowego),

b) oszustwa przy użyciu komputera (w szczególności chodzi tu o oszustwa bankomatowe, fałszowanie urządzeń wejścia/wyjścia, takich jak np. karty magnetyczne, oszustwa na maszynach wykorzystywanych do gier, oszustwa w systemach teleinformatycznych, oszustwa poprzez podanie fałszywych danych identyfikacyjnych),

c) powielanie programów komputerowych (w ramach tej grupy inkryminowanych czynów zabronionych wskazuje się powielanie gier we wszystkich ich postaciach, jak też wszelkich innych programów komputerowych czy też topografii układów scalonych),

d) sabotaż sprzętu oraz oprogramowania,

e) przechowywanie zbiorów zabronionych przez prawo,

f) przestępstwa popełnione w sieci (np. przestępstwa przeciwko wolności seksualnej i obyczajności popełnione za pośrednictwem systemu informatycznego) [32].

---

[30] Zob. B. Oręziak, *Cyberprzestępczość…*, s. 52-58.

[31] Zob. B. Hołyst, J. Pomykała, *Cyberprzestępczość…*, s. 17.

[32] Zob. M. Siwicki, *Podział i definicja…*, s. 249.

Z kolei w komunikacie Komisji Europejskiej[33] z 7 lutego 2013 r. uznano, że termin „cyberprzestępczość" „odnosi się do szerokiego wachlarza różnych rodzajów działalności przestępczej, w przypadku której komputery i systemy informatyczne stanowią podstawowe narzędzie przestępcze lub są głównym celem działania przestępczego", biorąc zaś pod uwagę rodzaj zamachu, możemy wyróżnić trzy grupy znamiennych czynów polegających na posługiwaniu się sieciami telekomunikacyjnymi z zamiarem naruszenia jakiegokolwiek dobra chronionego regulacjami prawnymi, tj. grup przestępstw:

1) pospolitych, stanowiących najczęściej zagrożenie dla bezpieczeństwa dla przetwarzanych informacji (np. fałszerstwo dokumentów czy też oszustwo), popełnionych z wykorzystaniem technologii komputerowej;
2) związanych z publikacją w mediach elektronicznych treści zakazanych przez przepisy powszechnie obowiązującego prawa, których istota przestępstw wiąże się z treścią informacji (np. publikowanie materiałów związanych z seksualnym wykorzystaniem dzieci, upublicznianie za pośrednictwem sieci materiałów nawołujących do nienawiści rasowej);
3) polegających na wykorzystaniu sieci łączności elektronicznej do naruszeń dóbr znajdujących się pod ochroną prawa karnego (np. hakerstwo, ataki przeciwko systemom informatycznym)[34].

Polska doktryna prawa karnego i nauk pokrewnych dzieli natomiast cyberprzestępstwa na dwie kategorie:

a) cyberprzestępstwa dokonywane z potencjalnym lub rzeczywistym użyciem przemocy (napaść poprzez zastraszenie, cyberterroryzm, pornografia dziecięca, cyberprześladowanie),

b) cyberprzestępstwa popełniane bez stosowania przemocy (cyberkradzieże, cyberzniszczenia, cyberwtargnięcia, cyberoszustwa, jak też inne cyberprzestępstwa)[35].

Odnosząc się natomiast do kwestii przestępstw komputerowych i ewentualnych podziałów definicyjnych samej przestępczości komputerowej, nawiązać należy do pozycji zajmującej czołowe miejsce w kanonie polskich rozważań prawniczych dotyczących opisywania zjawiska przestępczości komputerowej, tj. wydanego w 2000 r. opracowania autorstwa A. Adamskiego[36]. Autor ten, wprowadzając po-

---

[33] *Communication in the European Parliament, the Council. The European Economic and Social Committee and the Committee of The Regions: Cybersecurity Strategy on the European Union: An Open, Safe and Secure Cyberspace* (JOIN/2013/0001).

[34] Zob. J.A. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 11.

[35] Zob. B. Hołyst, J. Pomykała, *Cyberprzestępczość…*, s. 17-19.

[36] Zob. J. Wasilewski, *Przestępczość…*, s. 160.

dział definicyjny przestępczości komputerowej, wyróżnił na tej płaszczyźnie dwa podstawowe ujęcia:

1) materialnoprawne, a stosując kryterium roli, w jakiej mogą wystąpić komputery podczas podejmowania inkryminowanych działań, wprowadził dwie podkategorie przestępczości komputerowej:

a) *stricte* komputerowe, rozumiane jako czyny bezprawne, skierowane przeciwko danym, systemom czy też programom, a więc takie czyny, w przypadku których nowoczesne technologie informatyczne stanowią albo same w sobie przedmiot zamachu, albo środowisko do przeprowadzenia takiego ataku,

b) komputerowe w ujęciu szerokim, czyli takie czyny, w których ustawowa regulacja wprowadza wprost konieczność użycia komputera jako narzędzia do ich popełnienia, w zakwalifikowaniu do tej kategorii decyduje więc nie sam przedmiot zamachu, ale ustawowo wskazany sposób działania sprawcy;

2) procesowe, obejmujące przypadki, w ramach których system komputerowy jest przedmiotem oraz narzędziem zamachu, a więc wszystkie czyny penalizowane przez prawo karne, których ściganie wiąże się z ciążącym na organach wymiaru sprawiedliwości wymogiem pozyskania dostępu do danych przetwarzanych w ramach systemów teleinformatycznych lub komputerowych[37].

Dodatkowo w 2005 r. A. Adamski dokonał roboczego podziału cyberprzestępczości na cztery kategorie:

„1) przestępstwa przeciwko poufności, integralności i dostępności danych i systemów komputerowych (np. nieuprawniony dostęp do systemu, podsłuchiwanie transmisji danych lub zakłócanie funkcjonowania systemów);

2) przestępstwa przeciwko dostępowi warunkowemu do usług informatycznych (np. nieuprawniony dostęp do płatnej, kodowanej telewizji);

3) przestępstwa związane z wykorzystaniem komputerów (np. oszustwo komputerowe, fałszerstwo komputerowe);

4) przestępstwa związane z rozpowszechnieniem lub przesyłaniem określonych rodzajów informacji (np. propagowanie treści rasistowskich, pornografii dziecięcej lub choćby rozsyłanie niezamówionych informacji handlowych, np. spamów)"[38].

Autor niniejszej publikacji nie traktuje „cyberprzestępczości" (odpowiednio cyberprzestępstw), a także „przestępczości komputerowej" (odpowiednio przestępstw komputerowych) na zasadzie synonimiczności. W mojej ocenie cyberprzestępstwa to czyny zabronione popełnione w sieci teleinformatycznej, a przestępstwa komputerowe to czyny zabronione popełnione przy wykorzystaniu komputera

[37] Zob. A. Adamski, *Prawo karne…*, s. 31-32.

[38] J. Wasilewski, *Przestępczość…*, s. 168.

(zdefiniowanego na płaszczyźnie konwencji budapesztańskiej z 2001 r.) pracującego w trybie *offline* (bez wykorzystania dostępu do sieci teleinformatycznej). Uważam także za zbędne wprowadzanie do podstawowych aktów regulujących polskie prawo karne ustawowych definicji legalnych obu typów przestępstw (cyberprzestępstw oraz przestępstw komputerowych) – czego zresztą do chwili obecnej racjonalny ustawodawca nie uczynił – jako że z punktu widzenia pragmatyki zabieg ten nie miałby większego znaczenia praktycznego, skoro obecnie wiele przestępstw może być obecnie popełnionych w sieci teleinformatycznej (także tych „tradycyjnych"), jak też z wykorzystaniem komputera. Zabieg taki miałby natomiast znaczenie dla doktryny zawsze dążącej do ujednolicenia siatki pojęciowej, tak by była ona spójna i jednorodna.

Znaczącym rozdziałem k.k., którego zadaniem jest regulacja odpowiedzialności prawnokarnej z tytułu cyberprzestępczości, jest przede wszystkim rozdział XXXIII[39]. Na chwilę obecną ustawodawca w ramach wskazanego rozdziału zatytułowanego „Przestępstwa przeciwko ochronie informacji" penalizuje:

– bezprawne uzyskanie dostępu do informacji lub systemu informatycznego oraz działania z nimi związane (art. 267 k.k.);

– nieuprawnione zniszczenie, uszkodzenie, usuwanie, lub zmiana zapisu istotnej informacji w formie danych informatycznych, albo w inny sposób udaremnianie lub znaczne utrudnianie osobie uprawnionej zapoznania się z nią (art. 268 k.k.);

– nieuprawnione niszczenie, uszkadzanie, usuwanie, zmiana lub utrudnianie dostępu do danych informatycznych albo w istotnym stopniu zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych (art. 268a k.k.);

– niszczenie, uszkadzanie, usuwanie lub zmiana danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego bądź zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych, w tym niszczenie albo wymiana informatycznego nośnika danych, jak też niszczenie albo uszkadzanie urządzenia służącego do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych, czyli sabotaż informatyczny (art. 269 k.k.);

– dywersja informatyczna polegająca na zakłócaniu w istotnym stopniu pracy sieci teleinformatycznej lub systemu komputerowego (art. 269a k.k.);

---

[39] Zob. M. Zbrojewska, V. Morozov, S. Biedron, T. Panskyi, *Jak definiujemy…*, s. 64.

– działania sprowadzające się do wytwarzania w sposób bezprawny (lub w drodze czynności zbliżonych) programów komputerowych lub urządzeń przystosowanych do dokonywania określonych przestępstw, kodów dostępu, haseł komputerowych lub innych danych (art. 269b k.k.).

Dodatkowo ustawodawca w rozdziale XXXV k.k. unormował katalog przestępstw przeciwko mieniu:

– oszustwa komputerowe (art. 287 k.k.);

– kradzieże programu komputerowego (art. 278 § 2 k.k.);

– paserstwa programu komputerowego (art. 293 k.k.)[40].

Nie sposób jest także stracić z pola widzenia w kontekście omawianych zagadnień takich przestępstw jak:

– szpiegostwo komputerowe i wywiad komputerowy (art. 130 § 2-3 k.k.),

– sprowadzenie niebezpieczeństwa dla życia i zdrowia wielu osób lub mienia w znacznych rozmiarach poprzez zakłócanie, uniemożliwianie, wpływ na automatyczne przekazywanie i gromadzenie danych informatycznych (art. 165 § 1 pkt 5 k.k.),

– czy też wprowadzonego ustawą z 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości w art. 224a § 2 k.k. nowego typu przestępstwa, penalizującego zawiadomienie przez sprawcę o więcej niż jednym zdarzeniu, czyli fałszywe powiadomienie o tzw. kaskadowym charakterze.

Swoistym *novum* jest wprowadzenie na podstawie ustawy z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw[41] kontratypu działania w celu wykrycia błędów w zabezpieczeniach systemów informatycznych w odniesieniu do przestępstw: nieuprawnionego uzyskania dostępu do systemu informatycznego (art. 267 § 2 k.k.) oraz nieuprawnionego zakłócania pracy systemu (art. 269a k.k.). Kumulatywnymi warunkami niezbędnymi do skorzystania z klauzuli niepodlegania karze są:

1) działania sprawcy wyłącznie w co najmniej jednym z dwóch celów: albo w celu opracowania metody zabezpieczenia systemu teleinformatycznego, systemu informatycznego lub sieci teleinformatycznej, albo w celu zabezpieczenia takich systemów lub sieci;

2) powiadomienie dysponenta systemu lub sieci o ujawnionych zagrożeniach w sposób niezwłoczny;

---

[40] Zob. *ibidem*.

[41] Ustawa z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. z 2017 r. poz. 768).

3) brak naruszenia interesu prywatnego, interesu publicznego oraz niewyrządzenie szkody[42].

TECHNIKI POPEŁNIANIA CYBERPRZESTĘPSTW, TYPY SPRAWCÓW ORAZ SPOSOBY ZACIERANIA PRZEZ NICH ŚLADÓW

W dalszej części niniejszej publikacji zasadne jest odniesienie się do wybranych technik popełnienia cyberprzestępstw, typów ich sprawców oraz metod zacierania przez nich śladów ich popełnienia.

Na gruncie literatury przedmiotu funkcjonuje wiele podziałów i opisów metod przestępczego działania, które bezpośrednio rzutują na działanie systemów komputerowych.

R. Jedlińska do najbardziej rozpowszechnionych oraz najczęstszych zalicza:

– posługiwanie się takimi urządzeniami jak konie trojańskie, tzw. trojanami oraz innymi wirusami komputerowymi;

– niszczenie danych (przykładowo poprzez naruszanie oryginalnych zapisów, przerabianie lub podrabianie dokumentów);

– *superzapping* polegający na bezprawnym wykorzystaniu programów użytkowych przez zniszczenie, zmiany lub ujawnienie danych;

– metodę „salami", której istota sprowadza się do kradzieży małych sum pochodzących z różnych źródeł;

– przecieki danych;

– tzw. podnoszone drzwi (wykorzystanie urządzeń sprzyjających dokonaniu przestępstwa);

– podsłuch;

– tzw. bomby logiczne oraz asynchroniczne ataki;

– oczyszczanie polegające na przeszukaniu komputera;

– wykorzystanie komputera w charakterze narzędzia służącego do planowania, jak też kontroli przestępczości;

– impersonację, czyli podszywanie się pod uprawnionego użytkownika;

– *piggybacking,* sprowadzający się do nieuprawnionego wejścia do obiektów strzeżonych[43].

E. Gruza, M. Goc oraz J. Moszczyński z kolei do metod ataków w cyberprzestrzeni zaliczają: wirusy komputerowe, robaki komputerowe, konie trojańskie,

---

[42] Zob. *Kodeks karny. Komentarz zaktualizowany*, P. Kozłowska-Kalisz, M. Mozgawa (red.), LEX/el. 2021.

[43] Zob. R. Jedlińska, *Problem przestępczości elektronicznej*, „Ekonomiczne Problemy Usług" 2017, nr 1 (126), t. 2, s. 189.

bomby logiczne, *e-mail bombing, sniffing, spoofing*, DDoS, SYN Floyd, *phishing, pharming*[44].

M. Zbrojewska, V. Morosov, S. Biedron, T. Panskyi zwracają wyróżniają na takie metody popełnienia przestępstw, jak: użycie wirusa komputerowego, konia trojańskiego, robaka, sieci *botnet*, ataku DDoS, ataku *man-in-the-middle, phishing, pharming*[45].

T. Trejderowski zwraca uwagę na najczęstsze sposoby mające na celu zachęcić do uruchomienia złośliwego oprogramowania, takie jak:

„– oprogramowanie udostępniane w sieciach typu *peer-to-peer* (na przykład *BitTorrent, eMule*),

– rzekome rozszerzenie (ang. *plug-in*) do popularnych przeglądarek internetowych,

– programy rzekomo instalujące dodatkowe paski narzędziowe w przeglądarkach stron www,

– rzekome dekodery konieczne do odtwarzania określonych plików multimedialnych,

– fałszywe sterowniki do urządzeń zainstalowanych na komputerze,

– programy rzekomo ulepszające pracę komputera: antywirusowe, przyspieszacze, do czyszczenia z niepotrzebnych plików, do naprawiania rejestru *Windows*, udostępniane do pobrania za darmo ze strony www lub w wersji *on-line* do natychmiastowego użycia,

– załączniki do e-maili bazując na emocjach i regułach socjotechnicznych: obrazek, wygaszacz ekranu, prezentacja, zarchiwizowany plik"[46].

B. Hołyst pośród najpopularniejszych metod służących atakowaniu systemów komputerowych wskazuje: konia trojańskiego, niszczenie danych, wirusa, robaka komputerowego oraz bombę logiczną[47].

M. Mazur proponuje uzupełnienie wskazanej klasyfikacji dodatkowo o takie metody jak: *backdoor, e-mail bombing, phishing* (pozorowanie autentyczności), *sniffing* (podsłuch), *smishing, pharming, DDoS (Distributed Denial of Service*), *IP spoofing, SYN Floyd*, jak również takie przejawy przestępczej aktywności jak: cyberterroryzm czy też *social engenering* (socjotechnika)[48].

---

[44] Zob. E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka, czyli rzecz o metodach śledczych*, Warszawa 2008, s. 562.

[45] Zob. M. Zbrojewska, V. Morozov, S. Biedron, T. Panskyi, *Jak definiujemy…*, s. 66-67.

[46] T. Trejderowski, Kradzież *tożsamości. Terroryzm informatyczny. Cyberprzestępstwa. Internet, telefon, Facebook*, Warszawa 2013, s. 88-89.

[47] Zob. B. Hołyst, K*ryminalistyka*, Warszawa 2007, s. 244-248.

[48] Zob. M. Mazur, *Przestępstwa komputerowe – zarys problematyki*, www.kryminalistyka.org.pl (dostęp: 31.12.2021 r.).

M. Białkowski, dokonując podziału przestępstw komputerowych, jednocześnie prezentuje techniki ich popełnienia, wskazując na następujące.

I. Atak komputerowy mogący przybrać postać: „1. skanowania, 2. ataku na system operacyjny, 3. *spamingu*, 4. ataku na serwer, 5. odmowy serwisu, 6. ataku na system poczty,7. *social engineeringu*, 8. nielegalnego oprogramowania, 9. rozpowszechniania nielegalnych lub obraźliwych treści, itp."[49], którego celem mogą być systemy: przedsiębiorstw, wojskowe, naukowe, bankowo-finansowe, administracji rządowej i samorządowej, gdzie pośród technik przełamywania zabezpieczeń hasłowych wyróżnia się: atak słownikowy (*dictionarry attack*), maskaradę (*IP Spoofing*), brutalny atak słowny (*brute force attack*), podsłuchiwanie sieci (*IP Sniffer*), podmianę (*man-in- the middle*), poszukiwanie luk w systemie bezpieczeństwa (*logi*), blokadę serwera (*denial of service*), ataki fizyczne (*phisical attacks*), atak przez anonimowe FTP (*File Transfer Protocol*), atak typu *land* czy też atak przez aktywne rozsynchronizowanie TCP (*Transmission Control Protocol*) lub atak typu *FTP bounce* określany również mianem ataku odbijającego FTP.

II. Niszczenie danych i programów komputerowych, które mogą być dokonane metodą fizyczną lub informatyczną (stanowiącą najpowszechniej stosowaną metodę popełnienia przestępstw komputerowych polegającą na ogół na zmianie danych przed lub też w czasie wprowadzania ich do komputera w drodze umieszczania w innych programach segmentu wykonywalnego kodu o właściwościach samoreplikujących, czyli wirusa mogącego przybrać postać wirusa MBR, wirusa *boot* sektora lub infekcyjnego pliku, względnie samodzielnego programu wykonywalnego, czyli robaka).

III. Sabotaż i szantaż komputerowy, przy czym istota sabotażu komputerowego sprowadza się do rozmyślnego niszczenia lub uszkodzenia danych lub również sprzętu komputerowego poprzez takie przejawy przestępczej działalności jak: podnoszenie drzwi, oczyszczanie, asynchroniczne ataki, symulację i modelowanie; szantaż komputerowy polega na przemieszczeniu danych w inne miejsce, znane tylko sprawcy, w celu wymuszenia przekazania określonej kwoty pieniędzy w zamian za odwrócenie tego procesu.

IV. Nieuprawnione wejście do systemu komputerowego, gdzie nadrzędnym celem działania hakera staje się główny serwer sieci, jako że zawiera on wszystkie informacje na temat istniejącego systemu operacyjnego, sam zaś atak może przybrać postać pasywną lub aktywną, a środkami wiodącymi do realizacji tego założenia

[49] M. Białkowski, *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Warszawa 2021, s. 127-177.

stają się m.in.: *back door*, *expoil*, koń trojański, *sniffing*, *IP Spoofing*, blokowanie serwerów, socjotechnika hakera czy też zgadywanie haseł.

V. Podsłuch komputerowy sprowadzający się do:

a) działań ukierunkowanych na podsłuchiwanie, jak też zbieranie danych pochodzących z transmisji teleinformatycznej, co może przybrać postać czynną lub bierną,

b) działań podsłuchowych prowadzonych na podstawie przetwarzania promieniowania pochodzącego od aparatury komputerowej stanowiącej nośnik informacji przebierającej postać emitowanego przez nią pola oraz fal elektromagnetycznych.

VI. Szpiegostwo komputerowe, które sprowadza się do prostego kopiowania danych, względnie do zbierania nośników danych czy też wykorzystywania „danych resztkowych" lub przechwytywania promieniowania elektromagnetycznego pozyskanego uprzednio podczas dokonywania innego przestępstwa[50].

Zdaniem autora niniejszej publikacji logiczną konsekwencją dalszego rozwoju technologicznego będzie towarzyszący mu rozwój technik popełniania cyberprzestępstw. Organy ścigania muszą więc na bieżąco śledzić ten proces kreowania nowych sposobów przestępczego działania, a rolę służebną w tym procesie będzie odgrywać tak jak dotychczas informatyka śledcza. Ścisła współpraca organów ścigania, ekspertów z zakresu informatyki śledczej oraz z drugiej strony przedstawicieli branży IT odpowiedzialnych za uszczelnianie systemów bezpieczeństwa informatycznego może znacząco przyczynić się do pozbawienia technik popełniania cyberprzestępstw cechy skuteczności, czyniąc je finalnie bezużytecznymi.

W dalszej kolejności po prezentacji technik stosowanych przez sprawców cyberprzestępstw zasadne jest odnieść się do kwestii typologicznego podziału tych wyspecjalizowanych naruszycieli prawa.

R. Jedlińska wyróżnia podstawowy podział sprawców przestępstw komputerowych różnicując ich na:

1) przestępców używających zaawansowanych narzędzi informatycznych oraz wiedzy informatycznej do popełniania przestępstw, przy czym wskazana grupa dzieli się na:

a) hakerów, czyli ekspertów komputerowych dysponujących ogromnym zasobem wiedzy z dziedziny informatyki, dzielących się na: błyskotliwych programistów, przestępców – włamywaczy oraz ekspertów ds. bezpieczeństwa (początkowo pojęcie to funkcjonowało wyłącznie w pejoratywnym znaczeniu, ale z czasem zostało wzbogacone o elementy pozytywne, włączając do tej charakterystyki także

[50] Zob. *ibidem*, s. 127-177.

hakera rozumianego jako uzdolnionego programistę, który pomaga wyszukiwać oraz zabezpieczać luki w aplikacjach sieciowych),

b) *crackerów*, przy czym termin ten może być rozumiany w dwojaki sposób, gdyż może obejmować nie tylko osoby łamiące zabezpieczenia serwerów w sieci podejmowane z zamiarem kradzieży, ewentualnie zniszczenia danych, lecz także odnosić się do osoby zajmującej się analizowaniem kodów programów pod kątem ich zabezpieczania przed kopiowaniem w celu ich obejścia lub usunięcia;

2) przestępców traktujących komputer lub sieć jedynie jako dodatkowe narzędzie do popełnienia przestępstw (przykładowo sieć może być miejscem do poszukiwania przez nich ofiar, w sieci mogą przechowywać dane dotyczące działalności przestępczej, sieć może być też narzędziem do kontaktu drogą elektroniczną z innymi współsprawcami)[51].

Z kolei M. Mazur dzieli sprawców przestępstw komputerowych na siedem grup: I. *Hackerów*, II. *Crackerów*, III. Wandali (ich celem jest niszczenie systemów komputerowych, danych, przy czym działania te motywowane są względami emocjonalnymi czy też pragnieniem zemsty), IV. Pospolitych przestępców, V. *Phreakerów* (sprawców łamiących zabezpieczenia telefoniczne i uzyskujących połączenia na koszt innego abonenta), VI. Piratów komputerowych (tj. osoby zajmujące się rozpowszechnianiem programów, których zabezpieczenia zostały uprzednio złamane przez *crackerów*), VII. *Carderów* (zajmujących się kradzieżą numerów kart kredytowych lub ich podrabianiem)[52].

W moim przekonaniu dalszy rozwój technologiczny w branży IT – nieporównywalny z żadnym innym z uwagi na skalę dynamiki – mający wpływ na obraz cyberprzestępczości będzie rzutował na dalszą specjalizację zachowań inkryminowanych, powstawanie nowych typów sprawców cyberprzestępstw, jak też w obrębie tych samych typów także innych podkategorii. Naturalną zatem konsekwencją będzie rozrastanie się zaprezentowanych powyżej klasyfikacji, których wobec powyższego nie należy rozpatrywać na zasadzie katalogu zamkniętego. Nowe typy sprawców mogą także łączyć w sobie cechy innych typów w oparciu o model hybrydowy.

Popełnianie przestępstw w cyberprzestrzeni wymaga od dopuszczających się ich naruszycieli prawa podejmowania specjalnych zabiegów utrudniających organom ścigania identyfikację sprawców. Jak bowiem zauważył legendarny były amerykański haker K. Mitnick, „chcąc działać w sieci *incognito*, musisz stworzyć oddzielną tożsamość internetową, kompletnie niepowiązaną z prawdziwą"[53]

---

[51] Zob. R. Jedlińska, *Problem przestępczości…*, s. 190.

[52] Zob. M. Mazur, *Przestępstwa komputerowe…*

[53] K. Mitnick, R. Vamosi, *Niewidzialny w sieci. Sztuka zacierania śladów*, Bielsko-Biała 2017, s. 436.

Sprawcy przestępstw popełnianych w cyberprzestrzeni w sposób umiejętny zacierają za sobą ślady popełnionych przestępstw, korzystając z mnogich narzędzi służących do tego typu działań maskujących. Do najbardziej popularnych rozwiązań w tym zakresie zalicza się: „TOR (*The Onion Router*), system Tails (Linux), serwery *proxy*, generatory tożsamości oraz anonimowe skrzynki poczty elektronicznej"[54].

TOR stanowi zdecentralizowaną, wirtualną sieć komputerową, która wykorzystuje trasowanie cebulowe, polegające na przesyłaniu komunikatów (danych) za pomocą wielowarstwowego szyfrowania, zapobiegającego analizie ruchu użytkownika oraz zapewniająca mu niemal całkowitą anonimowość, przy czym wobec osób chcących poznać tożsamość internauty ujawnia się jedynie tzw. węzeł brzegowy stanowiący warstwę „widoczną"[55]. E. Snowden zauważa, że „TOR działa bowiem w oparciu o model społecznej współpracy, w którym kluczową rolę odgrywają komputerowo uzdolnieni ochotnicy z całego globu utrzymujący na swoich strychach, w piwnicach i garażach serwery TOR-a"[56].

Z kolei Linux TAILS to anonimizujący system operacyjny ułatwiający zachowanie anonimowości w Internecie, niewymagający instalowania aplikacji w systemie komputera służącego do łączenia się przez użytkownika z siecią. Cechą charakterystyczną tego narzędzia anonimizującego jest okoliczność, że po zakończeniu pracy z systemem TAILS na komputerze użytkownika nie pozostają jakiekolwiek ślady informatyczne, gdyż pamięć RAM jest automatycznie czyszczona podczas wyłączania komputera, natomiast pliki, na których operował użytkownik, zapisują się na dysku zewnętrznym, urządzeniu typu *pendrive* lub w chmurze[57].

Generatory fałszywej tożsamości pozwalają użytkownikowi dostarczać fikcyjne, kompletne dane nieistniejącej osoby, przydatne do tworzenia profilu na portalach aukcyjnych, społecznych i innych czy też kont poczty elektronicznej, gdzie wymagane jest podanie podczas procesu rejestracji pełnych danych osobowych (dla zainicjowania procesu generowania fikcyjnych danych wymagane jest jedynie podanie kraju zamieszkania, pochodzenia narodowego oraz płci)[58].

Anonimowe skrzynki e-mail dla ich funkcjonowania nie wymagają podania pełnych danych osobowych w toku procesu rejestracji. Korzystanie z nich jest

---

[54] C. Fiertek, K. Frąckowiak, T. Iwanowski, J. Motawski, P. Pawłowski, T. Piekarski, S. Stojak, W. Szelągowski, *Metodyki postępowań w sprawach o poszczególne rodzaje przestępstw*, Warszawa 2018, s. 465.

[55] *Ibidem*, s. 465-466.

[56] E. Snowden, *Pamięć ulotna*, Kraków 2019, s. 207.

[57] Zob. C. Fiertek, K. Frąckowiak, T. Iwanowski, J. Motawski, P. Pawłowski, T. Piekarski, S. Stojak, W. Szelągowski, *Metodyki postępowań…*, s. 472-473.

[58] Zob. *ibidem*, s. 475.

obwarowane jedynie koniecznością aktywacji w drodze kliknięcia linku aktywacyjnego wysyłanego na wskazany przez użytkownika adres e-mail, a w celu zachowania anonimowości pomocne jest skorzystanie z serwisu służącego do jednorazowego odbioru poczty elektronicznej[59].

Ukrycie tożsamości za pomocą serwera *proxy* sprowadza się do ustawienia połączenia transmisji danych w sieci teleinformatycznej z wykorzystaniem serwera pośredniczącego. Połączenie się z serwerem *proxy* generuje powstanie połączenia sieciowego w odpowiedzi na żądanie użytkownika, a tym samym w sieci widoczna jest tylko tożsamość serwera *proxy* ukrywającego rzeczywisty adres IP użytkownika[60].

Autor niniejszej publikacji, pochylając się nad zagadnieniem obszaru dotyczącego sposobów zacierania śladów w cyberprzestrzeni, stoi na stanowisku, że proces ten (jako kluczowy dla zachowania przez sprawcę anonimowości i gwarantujący mu uniknięcie odpowiedzialności karnej) będzie zmierzał w negatywnym kierunku, na niekorzyść organów ścigania, któremu może nie sprostać nawet stojąca na zaawansowanym poziomie informatyka śledcza. Zaprezentowane powyżej narzędzia uniemożliwiające lub znacząco utrudniające analizę ruchu sieciowego, korzystające dodatkowo z występowania takich czynnikach jak stosunkowo krótki okres przechowywania telekomunikacyjnych danych retencyjnych oraz opieszałość we współpracy międzynarodowej, mogą znacząco ograniczyć wykrywalność sprawców cyberprzestępstw. Tak długo, jak w tym zakresie nie nastąpią zmiany o charakterze globalnym, czas postrzegany przez E. Locarda jako prawda, która znika przed nami, będzie działał na korzyść cyberprzestępców, zapewniając im bezkarność w cyberprzestrzeni.

METODYKA PROWADZENIA ŚLEDZTW W SPRAWACH CYBERPRZESTĘPSTW WYKORZYSTUJĄCYCH TECHNIKI PHISHINGOWE, A TAKŻE POLEGAJĄCYCH NA ATAKU TYPU ODMOWA DOSTĘPU DOS

W dalszej części niniejszej publikacji zasadne jest odnieść się do metodyki prowadzenia śledztw w sprawach tych cyberprzestępstw, które są popełniane z wykorzystaniem jednych z najpowszechniej powszechnych technik przestępczych, tj. technik *phishingowych* oraz polegających na ataku typu odmowa dostępu DoS.

Metodyka (z gr. *methodos* – badanie) to zbiór reguł, które dotyczą postępowania w pewnej sytuacji, metody osiągania określonego celu (metodyka badań naukowych)[61].

---

[59] Zob. *ibidem*, s. 476-477.

[60] Zob. *ibidem*, s. 474.

[61] Zob. D. Samek (red. koordynujący), *Język polski. Kieszonkowy słownik wyrazów obcych*, Warszawa 2007, s. 320.

Pozyskane przez powszechne jednostki organizacyjne prokuratury informacje o cyberprzestępstwach mogą pochodzić z różnorakich źródeł (w szczególności chodzi tu o: 1) wyspecjalizowane Biura, Wydziały jednostek Policji zajmujących się walką z cyberprzestępczością; 2) rządowe oraz naukowe zespoły zajmujące się reagowaniem na poszczególne incydenty komputerowe, tzw. CERT; 3) podmioty oraz instytucje dysponujące wyspecjalizowanymi zespołami zajmującymi się cyberbezpieczeństwem, a nawet własnymi zespołami przeznaczonymi do reagowania na incydenty; 4) podmioty oraz instytucje nieposiadające wyspecjalizowanych zespołów do spraw cyberbezpieczeństwa, jak również osoby fizyczne)[62].

W literaturze przedmiotu podkreśla się istotność znaczenia czynności, które są podejmowane bezpośrednio po wejściu w posiadanie informacji o incydencie wskazującym na możliwość popełnienia czynu zabronionego, co w szczególności odnosi się do analizy zdarzenia, jak też zgromadzenia jak największego zbioru informacji o takich okolicznościach jak: sposób działania sprawcy, wykorzystane przez niego złośliwe oprogramowanie oraz danych o jego funkcjach. Dzięki przeanalizowaniu tych informacji możliwe staje się właściwe określenie kwalifikacji prawnej czynu stanowiącego przedmiot postępowania, a także pełne wykorzystanie pozostającego w dyspozycji organów ścigania potencjału procesowego i operacyjnego. Pamiętać należy, że poprawne ukierunkowanie śledztwa ma niebagatelne znaczenie w kontekście czynnika upływu czasu generującego utratę dowodów istotnych dla wyjaśnienia sprawy w postaci: logów, zapisów na informatycznych nośnikach informacji, danych retencyjnych[63]. W przypadku gdy materiały przekazane łącznie z zawiadomieniem nie zawierają poniższych ustaleń, prokurator, inicjując postępowanie sprawdzające, winien – w przypadku ataków wykorzystujących techniki *phishingowe* – polecić organom ścigania dokonanie takich ustaleń jak:

1) uzyskanie szczegółowego opisu ujawnionego ataku, na który składa się ustalony mechanizm działania złośliwego oprogramowania (wyekstrahowane pliki zawierające złośliwe oprogramowanie, adresy IP, za pomocą których nawiązywano komunikację, katalogi docelowe plików, odpytywane adresy internetowe), jak też sposób jego wykrycia oraz dane osób dysponujących wiedzą w przedmiocie zaistniałego incydentu;

2) określenie działań, jakie zostały podjęte przez pokrzywdzonego i były ukierunkowane na wykrycie złośliwego oprogramowania oraz zabezpieczenie danych z własnych zasobów informacyjnych;

---

[62] Zob. C. Fiertek, K. Frąckowiak, T. Iwanowski, J. Motawski, P. Pawłowski, T. Piekarski, S. Stojak, W. Szeląg owski, *Metodyki postępowań…*, s. 245-246.

[63] Zob. *ibidem*, s. 246.

3) pozyskanie danych osoby wybranej do kontaktu z organami ścigania w ramach obsługi incydentu;

4) zabezpieczenie raportów powłamaniowych oraz analiz, które zostały sporządzone przez pracowników pokrzywdzonego, względnie podmioty zewnętrzne;

5) wygenerowanie listy obejmującej komputery oraz nośniki danych zawierające ślady złośliwego oprogramowania, względnie nawiązujących komunikację z numerami IP hostów wraz z *malwarem*;

6) sporządzenie listy osób przypisanych do zainfekowanych komputerów powiązanej z informacjami o stanowiskach zajmowanych przez te osoby i ich uprawnieniach;

7) pozyskanie informacji odnoszących się do wykazu przejętych kont użytkowników systemów informatycznych, jak też informacji o stanowisku zajmowanym przez te osoby i ich uprawnieniach;

8) zgromadzenie danych na temat przejętych serwerów oraz informacji o zakresie danych zawartych na przejętym serwerze;

9) ustalenie adresów IP, do których i z których prowadzono komunikację z przejętych stacji roboczych, w tym numery portów;

10) zgromadzenie informacji na temat strony internetowej mogącej służyć do przekierowywania na skompromitowany serwer;

11) ustalenie pełnych logów zawierających informacje o komunikacji sieciowej w zakresie danych o sesji, tj.: ile danych wysłano na dany adres IP, ile zostało odebranych z danego adresu IP, w jaki sposób zakończono sesję, z jakim *hostem* z instytucji nawiązywano połączenia w okresie od rozpoczęcia aż do ukończenia ataku;

12) poczynienie ustaleń w kwestii charakteru, treści, a tkże wolumenu wyłudzonych danych, które były przesyłane z *hostów* należących do instytucji;

13) uzyskanie informacji, czy zidentyfikowano komputer zainfekowany jako pierwszy oraz czy doszło do identyfikacji komputera, który posłużył jako wewnętrzne *proxy* i był wykorzystywany do komunikacji z hostami z *malwerem*;

14) zgromadzenie wykazu dokumentacji (skorelowanego z jej zabezpieczeniem) znajdującej się w dyspozycji instytucji, a określającej jej politykę bezpieczeństwa, opisujących zabezpieczenia poszczególnych systemów informatycznych oraz sposobu ich działania, dokumentów zawierających sposób przydzielania i zakres uprawnień dla poszczególnych grup użytkowników i pozostałych dokumentów, które mogą mieć znaczenie dla danej sprawy[64].

[64] Zob. *ibidem*, s. 246-248.

Działania na etapie czynności sprawdzających – analogiczne jak w przypadku ataków wykorzystujących techniki *phishingowe* – w odniesieniu do ataków typów odmowa dostępu DoS obejmują:

1) poczynienie ustaleń co do funkcji, jaką pełni osoba dokonująca zgłoszenia, uzyskanie jej danych kontaktowych;

2) uzyskanie informacji, w jaki sposób doszło do rozpoznania ataku;

3) zgromadzenie jak najpełniejszych danych na okoliczność czasu ataku (wskazanie ram czasowych wyznaczanych przez rozpoczęcie oraz jego zakończenie, wskazanie, czy atak trwa nadal, rozpoznanie, czy ataki mają charakter powtarzalny);

4) ustalenie danych personalnych i kontaktowych osoby zajmującej się administrowaniem infrastruktury sieciowej;

5) zgromadzenie informacji odnoszących się do ruchu sieciowego w trakcie ataku (źródła oraz docelowe adresy IP i numery portów, rodzaj ruchu: DNS, TCP, ICMP, UDP, aplikacja, rozmiar pakietów, szybkość przesyłania pakietów, szerokość pasma zużywanego przez ruch ataku, rodzaj żądania: GET, http.);

6) pozyskanie od osoby zgłaszającej istotnych danych, takich jak: zapis komunikacji sieciowej, względnie zrzutów logów pochodzących z serwera, ISP/IDS, serwera *Apache, firewall*, ewentualnie innego urządzenia sieciowego zajmującego się rejestrowaniem ruchu sieciowego opisującego ruch nie tylko w trakcie ataku, lecz także przez nim oraz po nim, schemat sieci obejmujący wskazanie urządzeń rejestrujących ruch sieciowy, a także dokumentację techniczną urządzeń, z których dokonuje się zrzutów logów, jak też sam zrzut logów obrazujący ruch sieciowy;

7) ustalenie w ramach kontaktów z osobą zgłaszającą z instytucji, czy doszło do zgłoszeń niedostępności usługi przez użytkowników;

8) poczynienie ustaleń odnośnie kwestii, czy zaatakowana instytucja lub podmiot dokonały we własnym zakresie analizy nagłówków, logów, pakietów oraz jakie wnioski towarzyszyły tej syntezie;

9) ustalenie kwestii celowości ataku (czy atak był poprzedzony takimi działaniami jak wysuwanie żądań zapłaty okupu, czy istnieje prawdopodobieństwo podjęcia działań na zlecenie w drodze inspiracji pochodzącej przykładowo od nieuczciwej konkurencji, czy atak można powiązać z aktualnymi wydarzeniami geopolitycznymi, komu i w jakim rozmiarze zablokowanie usługi przyniosłoby korzyść);

10) poczynienie ustaleń w kwestii, jakie działania zostały podjęte by zapobiec atakom DoS;

11) uzyskanie danych co do wcześniejszych ataków DoS wymierzonych w daną instytucję;

12) zgromadzenie informacji odnoszących się do kwestii, kto odpowiada za projektowanie, wykonanie oraz obsługę platformy/aplikacji/strony, która stała

się celem ataku, skorelowane z zabezpieczeniem dokumentacji technicznej odnoszącej się do tych zagadnień;

13) uzyskanie informacji, czy, a jeśli tak, to kiedy były prowadzone testy obciążeniowe, a także zabezpieczenie ich wyników[65].

Czyny zabronione stypizowane w rozdziale XXXIII k.k. są zagrożone karami pozbawienia wolności w stosunkowo niskim wymiarze, co sprawia iż na ogół są one prowadzone w formie dochodzenia, co w pewnym zakresie ogranicza możliwości nadzoru przez prokuratora. Do wszczęcia śledztwa na podstawie art. 309 pkt 5 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego[66] uprawnia natomiast stwierdzenie, że atak miał poważny charakter i przykładowo wiązał się ze sprowadzeniem zagrożenia powstania szkody w wielkim rozmiarze, czy też naruszył interesy instytucji ważnej dla funkcjonowania państwa[67].

„Wszczynając postępowanie, należy precyzyjnie określić zakres postępowania oraz kwalifikację prawną. Czynność ta jest o tyle istotna, że będzie determinować szereg elementów późniejszego postępowania, takich jak powierzenie postępowania jednostce Policji odpowiedniego szczebla, czy kolejność realizowania wniosków o międzynarodową pomoc prawną przez organy wezwane (co do zasady nadając priorytety w realizacji, uwzględniają one zagrożenie karą za czyny stanowiące przedmiot postępowania)”[68].

Niezbędnym elementem prowadzenia postępowania obejmującego swoimi ramami zachowania określane jako cyberprzestępstwa winno być sporządzenie planu śledztwa lub planu czynności śledczych, zawierającego analizę dotychczas zgromadzonego materiału dowodowego, określenie wersji śledczych, a także wskazanie dowodów oraz czynności koniecznych do wykonania podczas śledztwa, a ukierunkowanych na weryfikację postawionych hipotez śledczych[69].

Proces gromadzenia materiału dowodowego w toku prowadzenia postępowań o cyberprzestępstwa obejmuje w znacznej mierze pozyskiwanie rzeczowego materiału dowodowego w drodze wydania oraz realizacji postanowień o przeszukaniu/zatrzymaniu rzeczy/żądaniu wydania danych informatycznych, względnie w drodze podejmowania dalszych działań procesowych o charakterze bardziej restrykcyjnym, które wkraczają w obszar prawa do poszanowania prywatności[70].

---

65 Zob. *ibidem*, s. 248-250.

66 Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 1997 r. Nr 89, poz. 555, ze zm.).

67 C. Fiertek, K. Frąckowiak, T. Iwanowski, J. Motawski, P. Pawłowski, T. Piekarski, S. Stojak, W. Szelągowski, *Metodyki postępowań…*, s. 250.

68 *Ibidem*, s. 251.

69 Zob. *ibidem*, s. 252.

70 Zob. *ibidem*.

Nierzadko w tego typu postępowaniach zachodzi potrzeba posiłkowania się międzynarodową pomocą prawną, co w szczególności odnosi się do informacji podlegających przetwarzaniu przez zagranicznych oraz ponadnarodowych dostawców usług internetowych (ISP – ang. *International Service Providers*)[71].

„Trzeba podkreślić, że w zakresie tzw. cyberprzestępstw duża cześć z globalnych dostawców (*Google, Facebook, Microsoft*) udziela niezbędnych informacji także w sposób odformalizowany, szczególnie danych o ruchu sieciowym (uzyskanie informacji dotyczących treści przekazu może wymagać wydania postanowienia – w kwestii szczegółów uzyskania informacji w tej drodze należy skontaktować się odpowiednimi Wydziałami do Walki z Cyberprzestępczością KWP lub koordynatorami do spraw cyberprzestępczości w Prokuraturach Regionalnych)"[72]. Współpraca międzynarodowa obejmuje formułowanie Europejskich Nakazów Dochodzeniowych (END), jak też system umów bilateralnych MLAT (ang. *Mutual Legal Assistance Treaties*)[73].

Wzrost ilości sprzętu elektronicznego w powiązaniu z łatwością w jego dostępie oraz w efekcie częstości korzystania z nowoczesnej technologii generuje zwiększenie liczby funkcjonujących śladów cyfrowych[74]. Kluczowe zatem miejsce w procesie koncentracji materiału dowodowego w tej kategorii przestępstw zajmuje opinia biegłego z zakresu informatyki śledczej, o czym będzie mowa szerzej w dalszej części publikacji poświęconej roli współczesnej informatyki śledczej wobec nasilenia zjawiska cyberprzestępczości w ramach procesu gromadzenia dowodów elektronicznych zawierających ślady cyfrowe. W tym miejscu należy natomiast zasygnalizować, że zabezpieczając sprzęt, z którego mógł być przeprowadzony atak w cyberprzestrzeni, należy dążyć do ustalenia:

– czy dane urządzenie zostało zainfekowane, a jeśli tak to, jaki to rodzaj infekcji;

– czy stwierdzono ruch sieciowy wychodzący z komputera, a jeśli tak, to z jakimi adresami IP badane urządzenie podejmuje próby połączenia (serwer);

– czy na badanym nośniku danych/urządzeniu znajdują się narzędzia, które mogły posłużyć do dokonania określonego typu ataku;

– czy dane urządzenie modyfikowano względem pierwotnego, oryginalnego oprogramowania, jaki był to rodzaj modyfikacji oraz kiedy go dokonano;

---

71 Zob. *ibidem*.

72 Zob. *ibidem*.

73 P. Opitek, *Wybrane aspekty pozyskiwania dowodów cyfrowych*, „Prokuratura i Prawo" 7-8, 2018, s. 69.

74 A. Hyła, *Analiza śladów cyfrowych*, „Prokuratura i Prawo" 2018, nr 5, s. 159.

– czy aplikacje znajdujące się na badanym urządzeniu generują ruch sieciowy, a w przypadku odpowiedzi pozytywnej, z jakim adresami IP[75].

W toku zaś gromadzenia osobowego materiału dowodowego kluczowe z kolei staje się przesłuchanie w charakterze świadka administratora sieci komputerowej, od którego należy odebrać depozycje na okoliczność:

– charakterystyki danych technicznych dotyczących konfiguracji administrowanej sieci teleinformatycznej;

– oprogramowania operacyjnego oraz rodzaju sprzętu komputerowego wykorzystywanego podczas pracy w sieci;

– sposobu zabezpieczania i przekazywania danych teleinformatycznych przetwarzanych w sieci;

– udostępnienia/podania haseł dostępu użytkowników sieci, jak też ustalenia ich numerów IP;

– czy informacje o każdej sesji w sieci są na tyle odpowiednio zabezpieczone, by na podstawie zgromadzonych danych możliwe było dokonanie identyfikacji grupowej sprawcy;

– czy możliwe jest ustalenie, jakim loginem oraz hasłem posługiwał się sprawca, jakich transakcji dokonał, jakim systemem roboczym się posługiwał;

– kiedy doszło do wykrycia nielegalnych działań;

– czy ustalono, kto może być sprawcą, czy działał on sam, czy współpracował z innymi osobami w sieci, a jeśli tak, to gdzie oraz z kim;

– z jakich programów oraz usług sieciowych sprawca korzystał podczas sesji;

– czy w oparciu o analizę aktywności sprawcy podczas trwania sesji możliwe jest ustalenie, gdzie oraz kiedy nastąpił skutek inkryminowanego działania sprawcy[76].

Odnosząc się do zagadnień metodologicznych związanych z prowadzeniem śledztw w sprawach dotyczących cyberprzestępstw, autor niniejszej publikacji dostrzega zdecydowaną potrzebę usprawnienia procedur z płaszczyzny dotyczącej międzynarodowego obrotu prawnego. Jeśli chodzi o kwestie związane z obrotem prawnym, a wynikające z uczestnictwa w strukturach Unii Europejskiej, zasadne byłoby wprowadzenie zmian w regulaminie prokuratorskim, które umożliwiałyby formułowanie END-ów już z poziomu prokuratur rejonowych, nie zaś za pośrednictwem właściwych miejscowo prokuratur okręgowych, co przyspieszyłoby obieg zapytań oraz odpowiedzi na nie. Spore nadzieje należy wiązać z takimi instytucjami procesowymi jak europejski nakaz wydania materiału dowodowego (EPO) oraz

---

[75] C. Fiertek, K. Frąckowiak, T. Iwanowski, J. Motawski, P. Pawłowski, T. Piekarski, S. Stojak, W. Szelągowski, *Metodyki postępowań…*, s. 254.

[76] Zob. M. Białkowski, *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Warszawa 2020, s. 206.

europejski nakaz zabezpieczenia danych (EPrO). Postulować także należy skrócenie czasu wykonania END-u w sprawach cyberprzestępstw: z 30 do 5 dni w zakresie wydania postanowienia o wykonaniu END-u przez państwo wykonujące, jak też z 90 do 30 dni przy zabezpieczaniu dowodów elektronicznych. Odnosząc się natomiast do współpracy międzynarodowej z państwami spoza UE – z uwagi na brak funkcjonalnego i w miarę wydolnego systemu pozyskiwania materiału dowodowego w sprawach cyberprzestępstw – postulować należy skrócenie łańcucha podmiotów biorących udział w wymianie informacji do niezbędnego minimum (idealnym modelem były taki zakładający bezpośredni kontakt organów ścigania danego państwa z podmiotem dysponującym danymi retencyjnymi innego państwa). Ważnym elementem usprawniającym obrót międzynarodowy byłoby także wprowadzenie uniwersalnych procedur dowodowych o charakterze globalnym oraz skorelowane z nim ujednolicenie wzorów formularzy o pomoc międzynarodową.

Końcowo w tym zakresie nadmienić należy, że jak wynika z policyjnych statystyk, w 2020 r. odnotowano ponad 55 tys. przestępstw mających związek z naruszeniem bezpieczeństwa informacji w sieci, w sytuacji gdy ponad 4 lata wcześniej było ich o połowę mniej. Jednocześnie drastycznie spadła wykrywalność tej kategorii przestępstw[77]. Usprawnienie sposobu prowadzenia postępowań przygotowawczych obejmujących swoimi ramami cyberprzestępstwa poprzez stałe udoskonalanie metodyki prowadzenia tej kategorii śledztw winno odwrócić ten niekorzystny dla organów ścigania trend.

ZADANIA WSPÓŁCZESNEJ INFORMATYKI ŚLEDCZEJ (W RAMACH PROCESU POZYSKIWANIA DOWODÓW ELEKTRONICZNYCH) WOBEC NASILENIA ZJAWISKA CYBERPRZESTĘPCZOŚCI

Śledztwa prowadzone w sprawach cyberprzestępstw sprowadzają się w znacznej mierze do gromadzenia oraz badania śladów cyfrowych, gdyż każde działanie potencjalnego sprawcy w systemie teleinformatycznym generuje powstanie śladu po tej formie aktywności[78].

Ślad cyfrowy można natomiast zdefiniować jako „zmianę w kodzie binarnym systemu teleinformatycznego, a także narzędzia cyfrowego zdolnego

---

[77] Zob. Przegląd Prasy PAP, *Hakerzy mają się w Polsce dobrze. Problem Policji*, dostępny na stronie: https:/bussinesinsider.co.pl/technologie/cyberprzestepstwa- w Polsce –statystyki/zm 11/7 (dostęp: 31.12.2021 r.).

[78] W.A. Kasprzak, *Ślady cyfrowe…*, s. 25.

do przetwarzania, wysyłania, gromadzenia pakietów danych, będącą wynikiem ingerencji zewnętrznej (fizycznej) lub wewnętrznej (zdalnej)"[79].

Dowód, który zostaje uzyskany ze śladu cyfrowego, przyporządkowuje się do kategorii dowodów rzeczowych, jako że pochodzi z nośnika danych (bezpośrednio) oraz stanowi jego właściwość[80].

Jak słusznie zauważa P. Opitek, „procesowe i kryminalistyczne przeszukanie systemu komputerowego oraz ujawnienie i zabezpieczenie śladów cyfrowych są czynnościami skomplikowanymi z uwagi na specyfikę wspomnianych śladów: chodzi o ulotność artefaktów i łatwość manipulowania nimi na odległość, metody kryptograficzne blokowania dostępu do danych, obowiązek respektowania jurysdykcji obcych państw przy ich uzyskiwaniu czy powinność szczegółowego ewidencjonowania czynności związanych z zabezpieczonym sprzętem"[81].

Ślady cyfrowe stanowią przedmiot badań informatyki śledczej, którą należy uznać za naukę, gdyż istnieją w niej przyjęte praktyki zbierania oraz analizy dowodów, a także zasady ich dopuszczalności w sądzie[82]. Podczas pierwszych warsztatów *Digital Forensic Research Workshop* (DFRWS) w 2001 r. informatyka śledcza została zdefiniowana jako „zastosowanie naukowo opracowanych i sprawdzonych metod zabezpieczenia, zbierania, weryfikacji i identyfikacji, analizy, interpretacji, dokumentowania oraz prezentowania cyfrowego materiału dowodowego pozyskanego z różnorodnych cyfrowych źródeł danych w celu ujawnienia i rekonstrukcji zdarzeń mających charakter kryminalny, prowadzących do nadużyć lub mających charakter nieautoryzowanych czynności zmierzających do zakłócenia innych, legalnych działań"[83]. Z kolei W. Filipkowski i G. Dobrowolski proponują ujęcie informatyki kryminalistycznej jako „całokształtu zastosowań wiedzy informatycznej do celów analizy technik i taktyk: popełniania przestępstw, ich dochodzenia oraz profilaktyki, a także wykorzystania jej w strategii kryminalistycznej zarówno przez podmioty sektora publicznego oraz prywatnego, jak też przez organizacje pozarządowe"[84]. Dla odróżnienia, informatyka sądowa (często mylnie rozumiana jako informatyka śledcza) ma znacznie szerszy kontekst niż informatyka śledcza

---

79 Zob. *ibidem*, s. 25.

80 *Ibidem*.

81 P. Opitek, *Cyberprzestępczość w pracy prokuratora*, „Prokuratura i Prawo" (wydanie specjalne) 2018, s. 79-80.

82 Zob. D.R. Hayes, *Informatyka w kryminalistyce. Praktyczny przewodnik*, Gliwice 2021, s. 33.

83 C. Altheide, H. Carrey, *Informatyka śledcza. Przewodnik po narzędziach open source*, Gliwice 2014, s. 18.

84 G. Dobrowolski, W. Filipkowski, *Charakterystyka informatyki kryminalistycznej w Polsce w ujęciu teoretycznym*, [w:] *Kryminalistyka, a nowoczesne technologie*, V. Kwiatkowska-Wójcikiewicz, D. Wilk, J. Wójcikiewicz (red.), Kraków 2019, s. 320.

oraz badanie informatycznych nośników danych. Zdaniem A. Chojnowskiego stanowi ona jedną z gałęzi nauk sądowych, której celem jest dostarczenie wiedzy specjalnej z zakresu informatyki organom przygotowawczym i sądom w sprawach karnych, jak też zgodnie z kodeksem postępowania cywilnego także komornikom sądowym[85].

Opinia eksperta z zakresu informatyki śledczej, rozumiana jako zespół czynności badawczych, które wymagają wiadomości specjalnych, wykonywanych przez biegłego na zlecenie organu procesowego, stanowi samoistny dowód w procesie[86].

Jak wskazuje W.A. Kasprzak, metody badań śladów cyfrowych, z uwagi na różne obszary działania urządzeń elektronicznych, można podzielić na pięć zasadniczych kategorii. Są to badania: 1) cyfrowej zawartości komputera; 2) zawartości nośników danych; 3) strumienia danych informatycznych; 5) treści zabezpieczanych plików; 6) wybranych serwerów[87].

Badanie w ramach ekspertyzy śladów cyfrowych komputera jako nośnika informacji pozwala na poczynienie miarodajnych ustaleń takich jak:

– typ, numer seryjny, numer IP komputera wykorzystywanego w celu łączenia się z siecią Internet (na podstawie analizy systemu operacyjnego);

– stan techniczny danych znajdujących się w pamięci komputera;

– jakiego typu pliki znajdują się w pamięci komputera;

– historia procesów oraz czynności wykonywanych w danym systemie (na podstawie sprawdzenia logów systemowych);

– historia korzystania z sieci internetowej (poprzez analizę danych pochodzących z programów przeglądarkowych);

– historia pobieranych i wysyłanych plików z danego komputera;

– wyekstrahowanie wykasowanych plików zawartych w „koszu" systemu (można ja przywrócić w niezmienionej formie cyfrowej);

– zlokalizowanie w poddawanym badaniom komputerze wszelkich programów oraz danych wykorzystywanych do działań ukierunkowanych na łamanie prawa (chodzi tu o materiały pochodzenia pirackiego: nielegalne programy, treści nielicencjonowane naruszające prawa autorskie czy też programy hackerskie);

– historia konwersacji prowadzonych za pośrednictwem sieci internetowej poprzez sprawdzenie komunikatorów wykorzystywanych przez poszczególnych użytkowników sieci;

---

85 Zob. A. Chojnowski, *Informatyka sądowa w praktyce*, Gliwice 2020, s. 7.

86 Zob. M. Białkowski, *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Warszawa 2016, s. 216.

87 Zob. W.A. Kasprzak, *Ślady cyfrowe...*, s. 184.

– historia połączeń internetowych, w tym przede wszystkim numerów IP oraz adresów stron, z jakimi najczęściej dokonywano połączeń;

– stwierdzenie, kto w danym czasie korzystał z komputera poprzez analizę danych w systemie uwierzytelniania lub logowania osoby;

– określenie, jaką funkcję pełnił danych komputer (nierzadko komputery stacjonarne pełnią funkcję serwerów, czyli urządzeń przeznaczonych do świadczenia usług dla innych komputerów, a serwer jako miejsce łączenia się wielu komputerów z bazą źródłową może być zasobem wielu cennych informacji dla organów ścigania;

– kopie bezpieczeństwa danych cyfrowych ujawniane na przypisanych do komputera zewnętrznych nośnikach danych[88].

M. Białkowski w kontekście zagadnień odnoszących się do kwestii ekspertyzy kryminalistycznej koncentrującej się na badaniu śladów cyfrowych wyróżnił katalog zagadnień podlegających wyjaśnieniu na polecenie organów procesowych lub dochodzeniowo-śledczych pod postacią następujących pytań:

– czy zajęte przedmioty (sprzęt komputerowy) mogły posłużyć do popełnienia przestępstwa skorelowanego z nielegalnym wykorzystaniem narzędzi informatycznych;

– czy ujawnione na zabezpieczonym sprzęcie elektronicznym programy komputerowe mogły zostać wykorzystane do popełnienia przestępstwa, jakiego rodzaju to były programy oraz do czego mogły służyć;

– jakiego rodzaju ślady udało się ujawnić na przedmiotach poddanych badaniom (czy są to ślady mające postać danych teleinformatycznych oraz jakiego rodzaju są to dane, czy programy znajdujące się na badanym dysku twardym mają charakter produktów licencjonowanych, na które użytkownik posiada licencję, czy też ujawnione na dysku twardym programy zostały stworzone specjalnie w zamiarze popełnienia przestępstwa przybierającego postać jednej z form *hackingu*, a także do jakiego celu mogły zostać wykorzystane, czy zabezpieczony sprzęt lub programy mogły zostać użyte do podrabiania lub przerabiania dokumentów, czy na powierzchni przedmiotów poddawanych badaniom znajdują się ślady mechanicznych uszkodzeń uniemożliwiających poczynienie ustaleń co do autentyczności zapisanych na nich danych teleinformatycznych);

– czy po dokonaniu czynu zabronionego wykasowano z zabezpieczonych dysków twardych komputerów programy komputerowe lub dane;

– czy na podstawie zabezpieczonych protokołów internetowych możliwe jest ustalenie, który komputer posłużył do dokonania ataków, nielegalnych transakcji, względnie użyto go do działań hakerskich o takim podłożu;

---

[88] Zob. *ibidem*, s. 167-169.

– czy sprawca podczas popełnienia czynu zabronionego użył zabezpieczonych narzędzi informatycznych, względnie czy w toku podejmowania inkryminowanych działań posługiwał się w sposób „zdalny" innym komputerem;

– jakie inne metody mogły zostać wykorzystane przez sprawcę zdarzenia do popełnienia czynu zabronionego;

– czy na podstawie ustalonych „metod postępowania sprawcy" możliwe jest dokonanie jego identyfikacji grupowej;

– przy wykorzystaniu jakich środków/metod/technik możliwym jest dokonanie identyfikacji indywidualnej sprawcy inkryminowanego zdarzenia[89].

Z uwagi na coraz popularniejsze korzystanie z usług typu *cloud computing* istotne dla finalnego rezultatu śledztwa staje się podjęcie działań ukierunkowanych na zabezpieczenie znajdujących się na dysku loginów, jak też haseł autoryzujących dostęp do zasobów z wirtualnego obszaru. Spora część użytkowników laptopów korzysta z funkcji automatycznego łączenia się systemu operacyjnego komputera z serwerem oraz przesyłania pomiędzy nimi informacji. Pośród zbioru danych przechowywanych na dysku twardym komputera może znajdować się zapisany klucz API (interfejs programowania aplikacji) stanowiący ściśle określone reguły umożliwiające komunikowanie się programów pomiędzy sobą, a niektóre usługi chmur obliczeniowych z niego korzystają. Kluczowym zadaniem biegłego z zakresu informatyki śledczej będzie zatem dokonanie gruntownej analizy dysku, skoncentrowanej na ujawnieniu oraz zabezpieczeniu danych służących do autoryzowania akcesu do zasobów wirtualnych[90].

Z kolei badanie pamięci operacyjnej komputera (RAM) może posłużyć do odzyskania kluczy kryptograficznych przeznaczonych do szyfrowania dysku, haseł dostępu do aplikacji, danych o działających programach szpiegujących, oprogramowania typu *malware*, a także innego związanego z działaniami hackerskimi. W pamięci RAM może także znajdować się szyfrowany systemowo zbiór kodów z własnym szyfrowanym kodem dostępu, czyli „skarbiec haseł", który może okazać się szczególnie pomocny w procesie odzyskiwania śladów cyfrowych z komputera będącego obiektem badań z wykorzystaniem narzędzi informatyki śledczej[91].

Bardzo wielu cennych danych dla prowadzących śledztwo może także dostarczyć badanie zasobów cyfrowych telefonów komórkowych, sprowadzające się do analizy trzech zasobów pamięci w postaci: karty SIM, pamięci właściwej telefonu oraz karty typu *flash*, w tym w drodze ekspertyzy rozszerzonej poprzez

---

89 Zob. M. Białkowski, *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Warszawa 2016, s. 218.

90 Zob. P. Opitek, *Cyberprzestępczość…*, s. 88.

91 Zob. *ibidem*, s. 89.

rutowanie telefonu polegające na wgraniu do systemu operacyjnego badanego urządzenia specjalistycznego oprogramowania umożliwiającego dostęp do jego pełnych zasobów w postaci plików systemowych oraz aplikacji[92].

Ślad cyfrowy będący przedmiotem szczególnego zainteresowania informatyki śledczej – jako że realizuje wszystkie funkcje śladu kryminalistycznego – jest pełnowartościowym śladem kryminalistycznym[93]. W.A. Kasprzak zauważa, że „problematyka, jaką jest badanie śladów cyfrowych jako pozostałości po dokonaniu przestępstwa i znajomość metodyki pracy biegłego z zakresu informatyki śledczej, są stosunkowo słabo znane przez prawników i pracowników organów ścigania. Do skutecznego współdziałania kryminalistyki i procesu karnego wymagane jest poznanie podstaw funkcjonowania systemów komputerowych i praw nimi rządzących, a także lepsze zaznajomienie się z przepisami i terminologią przez biegłych informatyków"[94].

Wprawdzie ślad cyfrowy jest śladem bardzo trwałym, niemniej jednak wiele nośników wymaga różnych procedur ich zabezpieczenia, a ich nieznajomość może prowadzić do zniekształcenia śladu cyfrowego lub wręcz do jego zniszczenia, dlatego też dużą wagę należy przykładać do popularyzowania wiedzy w tym zakresie[95]. Same zaś wydane w oparciu o badanie śladów cyfrowych opinie z zakresu informatyki śledczej – zdaniem przedstawicieli organów ścigania – charakteryzują się zbytnią hermetycznością, małą zrozumiałością lub wręcz niezrozumiałością, co również wymaga zmiany w kierunku wzrostu przejrzystości wniosków końcowych wywiedzionych w toku opiniowania[96]. W.A. Kasprzak, zauważając, że postęp technologiczny we współczesnym świecie jest nie do zahamowania, celnie puentuje, iż „skuteczna walka ze współczesną przestępczością powinna zakładać szerokie wykorzystanie śladów cyfrowych i prowadzenie szerokich badań kryminalistycznych w tym zakresie – to nowy kierunek zmian paradygmatu współczesnej kryminalistyki"[97].

Jako że ekspertyzy z zakresu informatyki śledczej swoimi ramami zakresowymi obejmują nierzadko rozbudowane wolumeny danych traktowanych jako *big data*, toteż autor niniejszej publikacji jako konieczność traktuje posiłkowanie się dodatkowo w pracy śledczej przez organy ścigania narzędziami analizy kryminalnej niezwykle pomocnymi przy porządkowaniu materiału dowodowego. Trzeba też

---

92 Zob. *ibidem*, s. 92-93.
93 W.A. Kasprzak, *Ślady cyfrowe...*, s. 227.
94 *Ibidem*.
95 Zob. *ibidem*, s. 228.
96 *Ibidem*, s. 229.
97 Zob. *ibidem*.

mieć na względnie okoliczność, że nie każdy ślad cyfrowy może finalnie okazać się dowodem cyfrowym. Z pewnością także do wzrostu rangi informatyka śledczego, a tym samym profesjonalizacji tej dziedziny wiedzy przysłuży się popularyzacja standardów, takich jak choćby „najlepsze praktyki w informatyce śledczej" opracowane przez A. Lacha ze Stowarzyszenia Instytut Informatyki Śledczej.

KRYPTOWALUTY A CYBERPRZESTĘPCZOŚĆ

Nierzadko w praktyce organów ścigania pojawia się schemat przestępczego działania, w ramach którego dochodzi do prania pieniędzy z wykorzystaniem kryptowalut, a czynem bazowym jest cyberprzestępstwo. Dochodzi także do finansowania terroryzmu z wykorzystaniem kryptowalut. Rozwój technologiczny sprzyja nadto oszustwom z wykorzystaniem kryptowalut na fałszywych giełdach, jak też z użyciem klasycznych technik *phishingowych*.

Przyjęta przez Europejski Bank Centralny definicja kryptowaluty przyjmuje, że jest to „cyfrowo prezentowana wartość, która nie została wyemitowana przez bank centralny, instytucję kredytowa, jak i instytucję pieniądza elektronicznego, która w pewnych okolicznościach może być wykorzystana jako alternatywa wobec pieniądza"[98].

W świecie przestępczym funkcjonują liczne zorganizowane grupy hackerskie oraz organizacje brokerów zajmujące się w sposób profesjonalny nielegalną działalnością wartą setki milionów dolarów[99].

P. Opitek oraz K. Góral na gruncie literatury przedmiotu opisują przypadek obywatela Niemiec, który w ciągu kilku miesięcy, posługując się internetowymi platformami do transferów *bitcoinów*, dokonał malwersacji setek tysięcy EURO, które pochodziły z oszustw dokonanych na aukcjach internetowych oraz z ataków *phishingu*. Sam zaś model popełnienia czynu zabronionego cechował się znamionami wskazującymi ewidentnie na pranie pieniędzy, gdyż sprawca wykorzystał spółkę formalnie zarejestrowaną w Wielkiej Brytanii, posługiwał się rachunkami bankowymi przypisanymi do „słupów" z terenu: Niemiec, Rumunii, Bułgarii, Polski. Dodatkowo sprawca korzystał z bezpiecznych serwerów ulokowanych na terenie obcych jurysdykcji, które hostowały jego platformę tradingową zawierającą oprogramowanie umożliwiające korzystanie z rożnych kontraktów. Nadto sprawca przeprowadził wymianę bitmonet na pieniądze fiducjarne z wykorzystaniem

[98] A.I. Piotrowska, *BITCOIN. Płatnicze i inwestycyjne zastosowanie kryptowaluty*, Warszawa 2018, s. 15.

[99] Zob. P. Opitek, K. Góral, *Analiza kryminalna transferów kryptowalutowych w pracy prokuratora (cz. II),* „Prokuratura i Prawo" 2020, nr 6, s. 114.

jednej z największych giełd kryptowalutowych[100]. Jak zauważają P. Opitek i K. Góral, „pranie pieniędzy jest bowiem wspólnym mianownikiem przestępstw „kryptograficznych", ponieważ każdy przestępca, który uzyskał nielegalnie bitmonety, zmierza najpierw do ukrycia ich pochodzenia, a potem zamiany środków krypto na gotówkę"[101].

Według szacunków pochodzących za rok 2020 sumaryczne uszczuplenie wywołane przestępczością powiązaną z walutami wirtualnymi wyniosło 4,5 bln dolarów. Z kolei zestawienie lat 2019 i 2018 wskazuje na wzrost malwersacji z pokrzywdzeniem użytkowników oraz inwestorów tokenów cyfrowych rzędu 533%[102].

Nie sposób jest bowiem stracić z pola widzenia okoliczności, że rynek kryptowalut stanowi obszar do nadużyć w tym obejmujących pranie brudnych pieniędzy, gdyż daje osobom zaangażowanym w jego funkcjonowanie poczucie anonimowości, przy czym zakres tej anonimowości jest uzależniony od rodzaju kryptowaluty podlegającej obrotowi. Jest to spowodowane posługiwaniem się specjalistycznymi urządzeniami anonimizującymi w postaci mikserów pozwalających na ukrycie historii transakcji, których użycie może udaremnić lub utrudnić proces odtworzenia migracji kryptowaluty[103]. Wciąż jeszcze zasadą jest, że przestępstwo prania pieniędzy jest popełniane z wykorzystaniem tradycyjnych walut fiducjarnych, niemniej jednak rozwój walut wirtualnych rzutuje także na skalę prania pieniędzy na płaszczyźnie zjawiska cyberprzestępczości. Sprzyja temu wzrost popularności różnych modeli biznesowych bazujących na tokenach, a jako przykład wskazać należy ekonomię współdziałania (ang. *sharing economy*) opierającą się na technologii *blockchain*[104].

P. Opitek zwraca uwagę, że sprawcy zajmujący się praniem pieniędzy z wykorzystaniem kryptowalut stale udoskonalają metody działań przestępczych w obrębie sieci teleinformatycznej. Tego typu działania sprowadzają się do tworzenia fikcyjnych kont użytkowników kryptowalut, posługiwania się siecią TOR czy też VPN-ami, generowania dużej liczby nowych adresów przypisanych do każdego nowego przychodzącego przelewu, używania specjalnych serwisów sieciowych wykorzystywanych do zaburzania historii obrotu kryptowalutami, tak aby na kolejnym już

---

100 Zob. P. Opitek, K. Góral, *Analiza kryminalna transferów kryptowalutowych w pracy prokuratora (cz. I)*, „Prokuratura i Prawo" 2020, nr 4-5, s. 75.

101 *Ibidem*, s. 76.

102 Zob. Intelligence January 2020 Cryptocurrency Anti-Money Loundering Report, 2019 Q4 Cipher Trace. Cryptocurrency Intelligence January 2020, tekst dostępny na stronie: https:ciphertace.com/wp-content/uploads/2020/02/cipherTrace-CAML-2019-Q4.pdf (dostęp: 31.12.2021 r.).

103 Zob. P. Wójcik T. Kabarowski, *Kryptowaluty od zera*, Gdynia 2020, s. 148-150.

104 Zob. P. Opitek, *Pranie pieniędzy i finansowanie terroryzmu z wykorzystaniem walut wirtualnych*, Instytut Kościuszki, styczeń 2020, s. 1, https//ik.org.pl (dostęp: 31.12.2021 r.).

etapie przeprowadzać operacje z użyciem aplikacji pozwalających na łączenie wielu bitcoinowych adresów w obrębie jednego portfela przeznaczonego do zarządzania nimi przy użyciu każdego urządzenia[105].

Pojęcie kryptowalut pozostaje także w pewnej korelacji ze zjawiskiem cyberterroryzmu stanowiącego poważny problem na płaszczyźnie cyberprzestrzeni rozumianej jako „system nerwowy" nowoczesnego państwa[106]. K. Liedel definiuje cyberterroryzm jako motywowany kwestiami politycznymi zamach lub jego groźbę na systemy informatyczne, komputery, sieci, zmierzający do zniszczenia tej wyspecjalizowanej infrastruktury, względnie do zastraszenia czy też wymuszenia na obywatelach danego państwa bądź państw oraz rządzie lub rządach daleko idących celów o charakterze politycznym lub społecznym[107]. Cyberterroryzm wykorzystuje rozwój technologii informatycznych także do zdobywania i pomnażania funduszy[108]. Na łamach raportu *Terrorist Use of Cryptocurrencies* sporządzonego przez ekspertów z RAND Corporation dokonano szczegółowej analizy zjawiska finansowania grup terrorystycznych z wykorzystaniem kryptowalut, a sformułowane w jej następstwie wnioski wskazują na wzrost zagrożenia dla państw. Sygnalizowane obawy są tym bardziej uzasadnione, jeśli zważy się na okoliczność, że w ciągu ostatnich kilku lat pojawiło się wiele nowych kryptowalut, takich jak przykładowo: *BlackCoin, MasterCoin, Altcoiny, Monero* czy też *Zcash*, a ostatnia z przytoczonych walut cyfrowych zapewnia wyższy poziom prywatności, a nawet umożliwia korzystanie z waluty w trybie *offline*[109].

Rozwój kryptowalut – według opinii ekspertów z Kaspersky Lab (którzy dokonali identyfikacji stosunkowo nowego trendu odnoszącego się do oszustw *online*) – przyciąga nie tylko rzesze inwestorów, lecz także cyberprzestępców podejmujących działania ukierunkowane na generowanie swoich zysków. Cyberprzestępcy, dążąc do realizacji swoich zamierzeń, posługują się klasycznymi technikami *phishingowymi*, niemniej jednak nierzadko wykraczają one poza dobrze znane scenariuszem typowe dla tego typu inkryminowanych działań. W ramach najbardziej skutecznych ataków wykorzystywano znane projekty ICO (emisja cyfrowych monet),

---

105 Zob. *ibidem*, s. 3.

106 Zob. T.R. Aleksandrowicz, K. Jałoszyński, *Wpływ rozpadu dwubiegunowego świata na obraz terroryzmu po 1989 roku*, [w:] *Bezpieczeństwo państwa, a zagrożenie terroryzmem. Terroryzm na przełomie XX i XXI wieku*, t. 1, K. Jałoszyński, T.R. Aleksandrowicz, K. Wiciak, Szczytno 2016, s. 34.

107 Zob. K. Liedel, *Bezpieczeństwo informatyczne w dobie terrorystycznych innych zagrożeń bezpieczeństwa narodowego*, Toruń 2006, s. 36.

108 Zob. M. Smarzewski, *Cyberterrozym, a cyberprzestępstwo o charakterze terrorystycznym*, „Ius Novum" 2017, nr 1, s. 67.

109 Zob. Sz. Palczewski, *Kryptowaluty w rękach terrorystów. Rośnie zagrożenie dla państw*, tekst dostępny na stronie: cyberdefence24.pl/polityka-i-prawo/krypto waluty-w –rekach-terrorystów-rosnie-zagrozenie-dla-panstw (dostęp: 31.12.2021 r.).

tworzenie stron *phishingowych* dla projektu ICO OmaseGo czy też w drodze dokonywania oszustw na „świetną okazję" uzyskania kryptowalut. Tylko w pierwszej połowie 2018 r. produkty firmy Kaspersky Lab dokonały blokady ponad 100 tys. incydentów powiązanych z kryptowalutami na fałszywych giełdach oraz w innych źródłach, co świadczy o niepokojącej skali tego procederu[110].

Wprawdzie obrót kryptowalutowy gwarantuje nieskrępowany granicami zasięg, ale niesie też ze sobą wiele zagrożeń. Wzrost popularności tych nowych instrumentów finansowych wśród inwestorów idzie w parze ze zwiększeniem się skali ich wykorzystania w ramach działalności przestępczej. W mojej ocenie w ciągu kilku najbliższych lat dojdzie do gwałtownego wzrostu zaangażowania kryptowalut w działania noszące znamiona poważnych przestępstw, nierzadko o charakterze transgranicznym. Posługiwanie się przez sprawców cyberprzestępstw siecią TOR, anonimowymi kryptowalutami (np. Monero), tzw. mikserami, czy też korzystanie z usług anonimowych giełd kryptowalutowych jest w stanie uniemożliwić opracowywanie analiz przepływów kryptowalutowych, stanowiących podstawę wszelkich istotnych działań w tym zakresie przez śledczych. Wzrostowi cyberprzestępstw z wykorzystaniem kryptowalut skorelowanemu ze zmniejszeniem ich wykrywalności winna towarzyszyć zdecydowana odpowiedź organów ścigania oparta na nowoczesnych narzędziach informatyki śledczej.

ZAKOŃCZENIE

Postępujący rozwój technologiczny spowodował przeniesienie wielu form aktywności ludzkiej na płaszczyznę cyberprzestrzeni, która stała się normalnym miejscem bytowania oraz załatwiania podstawowych potrzeb społecznych[111]. Opisana prawidłowość objęła także zachowania inkryminowane określane mianem cyberprzestępczości. Wzrastająca lawinowo liczba przestępstw popełnianych w cyberprzestrzeni przy jednoczesnym spadku jej wykrywalności wymaga podjęcia zdecydowanych działań ukierunkowanych na odwrócenie tego niekorzystnego z punktu widzenia interesów całego systemu prawnego trendu. Bardzo pozytywnie należy ocenić zatem powstanie Centralnego Biura Zwalczania Cyberprzestępczości. Skorelowane z tymi posunięciami kadrowymi na gruncie instytucji Policji zmiany organizacyjne w prokuraturze mogą stać się skutecznym orężem do walki z inkryminowanymi zachowaniami w cyberprzestrzeni. Dodatkowo organy te należy wyposażyć w najnowsze (na bieżąco aktualizowane zgodnie z trendami

---

[110] Zob. *Rozwój kryptowalut rodzi nowe cyberprzestępstwa*, tekst dostępny na stronie: Rozwój%kryptowalut%20rodzinowe%20cyberprzestępstwa%20_%Business%20Journal%20Polska.html (dostęp: 31.12.2021 r.).

[111] Zob. J. Bednarek, *Człowiek w obliczu szans cyberprzestrzeni i świata wirtualnego*, Warszawa 2014, s. 22.

technologicznymi) narzędzia, jakimi dysponuje informatyka śledcza, pozwalające na poszukiwanie, zabezpieczenia oraz właściwe interpretowanie śladów cyfrowych. Zmianom w strukturze organów ścigania ukierunkowanym na wyspecjalizowanie poszczególnych jej ogniw winny także towarzyszyć intensywny proces szkoleniowy obejmujący stale udoskonalaną metodykę prowadzenia postępowań przygotowawczych w sprawach cyberprzestępstw, prawidłowe zabezpieczanie śladów cyfrowych, jak też jak najściślejsza współpraca z ekspertami z zakresu informatyki śledczej, tak by formułowane przez organy ścigania postanowienia o powołaniu biegłego odnosiły się do wszystkich istotnych zagadnień wymagających ustalenia w procesie dochodzenia do prawdy materialnej. Ważną rolę w procesie zwalczania cyberprzestępczości upatrywać także należy w działaniach profilaktycznych przybierających postać kampanii medialnych ostrzegających odwiedzających cyberprzestrzeń przez mechanizmami towarzyszącymi inkryminowanym zachowaniom, mogącym finalnie doprowadzić do pokrzywdzenia. Jako wniosek *de lege ferenda* należy zgłosić potrzebę usprawnienia współpracy międzynarodowej w zakresie wymiany informacji w sprawach dotyczących cyberprzestępczości, co jest tym bardziej uprawnione w kontekście obecnych unormowań odnoszących się do okresu przechowywania danych retencyjnych. Końcowo nadmienić należy, że kompleksowo przeprowadzone zmiany w polityce walki z cyberprzestępczością z czasem z pewnością zaowocują pozytywnymi rezultatami na tym polu.

BIBLIOGRAFIA

Literatura

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Aleksandrowicz T.R., Jałoszyński K., *Wpływ rozpadu dwubiegunowego świata na obraz terroryzmu po 1989 roku*, [w:] K. Jałoszyński, T.R. Aleksandrowicz, K. Wiciak, *Bezpieczeństwo państwa, a zagrożenie terroryzmem. Terroryzm na przełomie XX i XXI wieku*, t. 1, Szczytno 2016.

Altheide C., Carrey H., *Informatyka śledcza. Przewodnik po narzędziach open source*, Gliwice 2014.

Bednarek J., *Człowiek w obliczu szans cyberprzestrzeni i świata wirtualnego*, Warszawa 2014.

Białkowski M., *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Warszawa 2016.

Białkowski M., *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Warszawa 2020.

Białkowski M., *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Warszawa 2021.

Bubeła M., *Informatyka śledcza i techniki anti-forensic w świetle polskiego prawa*, [w:] *Przestępstwa rzadko podejmowane przez organy ścigania. Aspekty kryminalistyczne, prawnomaterialne i procesowe*, Rzeszów 2013.

Chojnowski A., *Informatyka sądowa w praktyce*, Gliwice 2020.

Communication in the European Parliament, the Council. The European Economic and Social Committee and the Committee of The Regions: Cybersecurity Strategy on the European Union: An Open, Safe and Secure Cyberspace (JOIN/2013/0001).

Dobrowolski G., Filipkowski W., *Charakterystyka informatyki kryminalistycznej w Polsce w ujęciu teoretycznym*, [w:] *Kryminalistyka, a nowoczesne technologie*, V. Kwiatkowska-Wójcikiewicz, D. Wilk, J. Wójcikiewicz (red.), Kraków 2019.

Fiertek C., Frąckowiak K., Iwanowski T., Motawski J., Pawłowski P., Piekarski T., Stojak S., Szeląg owski W., *Metodyki postępowań w sprawach o poszczególne rodzaje przestępstw*, Warszawa 2018.
Fischer B., *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Kraków 2000.
Formicki T., *Wywiad i kontrwywiad jako kluczowe komponenty walki informacyjnej*, Warszawa 2020.
Gruza E., Goc M., Moszczyński J., *Kryminalistyka, czyli rzecz o metodach śledczych*, Warszawa 2008.
Hayes D.R., *Informatyka w kryminalistyce. Praktyczny przewodnik*, Gliwice 2021.
Hołyst B., K*ryminalistyka*, Warszawa 2007.
Hołyst B., Pomykała J., *Cyberprzestępczość, ochrona informacji i kryptologia*, „Prokuratura i Prawo" 2011, nr 1.
Hyła A., *Analiza śladów cyfrowych*, „Prokuratura i Prawo" 2018, nr 5.
Jaroszewska J.A., *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017.
Język polski. Kieszonkowy słownik wyrazów obcych, D. Samek (red. koordynujący), Warszawa 2007.
Kasprzak W.A., *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Warszawa 2015.
Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.
Lewulis P., *O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych*, „Prokuratura i Prawo" 2021, nr 3.
Liedel K., *Bezpieczeństwo informatyczne w dobie terrorystycznych innych zagrożeń bezpieczeństwa narodowego*, Toruń 2006.
Mitnick K., Vamosi R., *Niewidzialny w sieci. Sztuka zacierania śladów*, Bielsko-Biała 2017.
Omsby E., *Darknet*, Kraków 2019.
Opitek P., *Cyberprzestępczość w pracy prokuratora*, „Prokuratura i Prawo" (wydanie specjalne) 2018.
Opitek P., Góral K., *Analiza kryminalna transferów kryptowalutowych w pracy prokuratora (cz. I)*, „Prokuratura i Prawo" 2020, nr 4-5.
Opitek P., Góral K., *Analiza kryminalna transferów kryptowalutowych w pracy prokuratora (cz. II),* „Prokuratura i Prawo" 2020, nr 6.
Opitek P., *Przestępczość w pracy prokuratora*, „Prokuratura i Prawo" (wydanie specjalne) 2018.
Opitek P., *Wybrane aspekty pozyskiwania dowodów cyfrowych*, „Prokuratura i Prawo" 7-8, 2018.
Oręziak B., *Cyberprzestępczość w aspektach proceduralnych. Dowody elektroniczne a nowoczesne formy przestępczości*, Warszawa 2019.
Piotrowska A.I., *BITCOIN. Płatnicze i inwestycyjne zastosowanie kryptowaluty*, Warszawa 2018.
R. Jedlińska, *Problem przestępczości elektronicznej*, „Ekonomiczne Problemy Usług" 2017, nr 1 (126), t. 2.
Radoniewicz F., *Odpowiedzialność karna za przestępstwa hackingu*, „Prawo w działaniu. Sprawy karne" 2013, nr 13.
Siebert U., *Informationrecht und Recht der Informationstechnik*, „Neue Juridische Wochenchrift" 1989, Heft 41.
Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7-8.
Smarzewski M., *Cyberterrozym a cyberprzestępstwo o charakterze terrorystycznym*, „Ius Novum" 2017, nr 1.
Snowden E., *Pamięć ulotna*, Kraków 2019.
Stefanowicz M., *Cyberprzestępczość – próba diagnozy zjawiska*, „Kwartalnik Policyjny" 2017, nr 4.
Trejderowski T., Kradzież *tożsamości. Terroryzm informatyczny. Cyberprzestępstwa. Internet, telefon, Facebook*, Warszawa 2013.
Wasilewski J., *Cyberprzestrzeń – wybrane aspekty prawnokarne i kryminalistyczne*, Białystok 2017.
Wasilewski J., *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15/16.

Witek K., *Przestępczość komputerowa – aspekty prawne*, „Edukacja – Technika – Informatyka" 2018, nr 2 (24).
Wójcik P., Kabarowski T., *Kryptowaluty od zera*, Gdynia 2020.
Zbrojewska M., Morozov V., Biedron S., Panskyi T., *Jak definiujemy cyberprzestępstwo?*, „Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska" 2016, nr 2.

Źródła internetowe

Intelligence January 2020 Cryptocurrency Anti-Money Loundering Report, 2019 Q4 Cipher Trace. Cryptocurrency Intelligence January 2020, https:ciphertace.com/wp-content/uploads/2020/02/cipherTrace-CAML-2019-Q4.pdf.
Kodeks karny. Komentarz zaktualizowany, P. Kozłowska-Kalisz, M. Mozgawa (red.), LEX/el. 2021.
Mazur M., *Przestępstwa komputerowe – zarys problematyki*, www.kryminalistyka.org.pl.
Opitek P., *Pranie pieniędzy i finansowanie terroryzmu z wykorzystaniem walut wirtualnych*, Instytut Kościuszki, styczeń 2020, s. 1, https//ik.org.pl.
Palczewski S., *Kryptowaluty w rękach terrorystów. Rośnie zagrożenie dla państw*, cyberdefence24.pl/polityka-i-prawo/krypto waluty-w –rekach-terrorystów-rosnie-zagrozenie-dla-panstw.
Przegląd Prasy PAP, *Hakerzy mają się w Polsce dobrze. Problem Policji*, https:/bussinesinsider.co.pl/technologie/cyberprzestepstwa-wPolsce–statystyki/zm11/7.
Rozwój kryptowalut rodzi nowe cyberprzestępstwa, Rozwój%kryptowalut%20rodzinowe%20 cyberprzestępstwa%20_%Business%20Journal%20Polska.html.

Źródła prawa

Konwencja Rady Europy o cyberprzestępczości sporządzona w Budapeszcie w dniu 23 listopada 2001 r., Dz. U. 2015, poz. 728.
Ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości, Dz. U. z 2021 r. poz. 2447.
Ustawa z dnia 17 maja 2005 r. o informatyzacji podmiotów realizujących zadania publiczne Dz. U. z 2017 r. poz. 570, ze zm.
Ustawa z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, Dz. U. z 2017 r. poz. 768.
Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, Dz. U. z 1997 r. Nr 89, poz. 555.
Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. z 2021 r. poz. 2345.

Selected criminal law, forensic and criminological aspects of cybercrime

SUMMARY

Constituting to exist of a Central Bureau Against Cybercrime should be treated as a increase – as a part of criminal politics – efforts directed to fight with escalating cybercrime in last years. By the way this event it is justified to concern in this publication for a number of aspects criminal law, criminalistic and criminology nature corelated with this specialized type of a crime. In this publication waggled issue linked with define of cybercrime, computer crimes, synonymousness those phrases, cybercrime and computer crimes divisions and techniques their

commiting. There was mentioned too abaut problems methodological nature in matters of preparatory cases concerning phishing attacks, access denied Dos type. It was stressed also role of a contemporary computer forensics in studying digital trace treated as a competent criminal trace. In the end mentioned abaut crypto-currency in cyberspace in the context of a criminality commited on this plain.

Keywords: Cybercrime, cyberspace, information, kryptowaluta, haker, Ddos atack