SZKOŁA POLICJI

W PILE

Tomasz Kłys

Cyberprzestępczość

charakterystyka zjawiska

2023

SZKOŁA POLICJI w PILE

Zakład Kryminalny

Tomasz Kłys

Cyberprzestępczość

charakterystyka zjawiska

Skład komputerowy
Tomasz Kłys

Redakcja językowa
Waldemar Hałuja

Zatwierdzam i wprowadzam
do użytku jako materiał pomocniczy do zajęć

Zastępca Komendanta
Szkoły Policji w Pile

insp. Ryszard Jakubowski

Wydawnictwo Szkoły Policji w Pile
Wydanie I
Druk: Pracownia poligraficzna SP w Pile
Nakład ..... egz.
Piła 2023

Spis treści

Wstęp

Niniejsza publikacja została przygotowana jako materiał pomocniczy dla słuchaczy szkoleń zawodowego podoficerskiego oraz aspiranckiego, którzy realizują zajęcia z zakresu zagrożeń w cyberprzestrzeni. Z uwagi na rozwój nowoczesnych technologii teleinformatycznych może być ona jednak przydatna wszystkim funkcjonariuszom, którzy podczas wykonywania codziennych obowiązków służbowych spotykają się z przestępczością komputerową.

Głównym celem było opracowanie szczegółowej oceny problemu cyberprzestępczości, co pozwoliło na przedstawienie zjawiska zarówno w ujęciu statycznym, związanym z opisem zagrożeń, jak i dynamicznym - problematyką jego zwalczania. Charakter tego zjawiska sprawia, że problem ten w dalszym ciągu nie został w wystarczający sposób zbadany.

W publikacji skupiono się na przedstawieniu genezy cyberprzestępczości, historii rozwoju Internetu oraz kształtowania się regulacji prawnych, mających być odpowiedzią na pojawienie się nowych zagrożeń związanych z rozwojem technologicznym. Przedstawione zostały także aspekty techniczne związane z funkcjonowaniem sprzętu teleinformatycznego, sieci i nośników danych.

Dokonano także oceny rozmiaru i charakteru przestępstw komputerowych oraz przedstawiono najczęściej występujące oraz niosące największe niebezpieczeństwo zagrożenia, które wiążą się z funkcjonowaniem cyberprzestrzeni. Skupiono się na przestępstwach związanych z oszustwami komputerowymi, pornografii dziecięcej oraz nowych przestępstwach, do których zaliczyć można grooming, hacking, skimming lub cyberstalking.

Przedstawiono tu także problematykę związaną bezpośrednio ze zwalczaniem oraz zapobieganiem zjawisku cyberprzestępczości. Opisana została rola i znaczenie dowodu elektronicznego oraz czynności procesowych w cyberprzestrzeni wiążących się z jego zabezpieczeniem. Zwrócono uwagę na elementy, które w sposób negatywny wpływają na proces wykrywczy i możliwość ustalenia sprawców przestępczości komputerowej. Nie ulega wątpliwości, że rozwój cyberprzestępczości będzie postępował i ewoluował wraz z dalszym rozwojem technologicznym. Niezbędne więc okazuje się ciągłe poszukiwanie coraz nowszych i skutecznych metod zapobiegania temu zjawisku.

Rozdział I
Geneza i charakter cyberprzestępczości

1.1. Początki Internetu

W dzisiejszych czasach mamy do czynienia z niezwykle dynamicznym rozwojem technologii informacyjnych oraz coraz szerszym dostępem do Internetu. Elementy te w zasadniczy sposób wpływają na wzrost szybkości wymiany informacji. Niestety korzyści wynikające z rozwoju technologicznego wykorzystywane są także w celu popełniania przestępstw. Ich ściganie stało się poważnym problemem dla instytucji egzekwujących prawo, ale również dla samych ustawodawców.

Wiele osób definiuje pojęcie Internetu poprzez skojarzenie z jego najpowszechniejszym zastosowaniem, czyli stronami WWW. Należy zdawać sobie jednak sprawę z tego, iż narzędzie to oferuje zdecydowanie większe możliwości niż dostęp do ogólnoświatowego zbioru stron internetowych[1].

Internet stanowi więc globalny system wymiany danych, który może funkcjonować dzięki wzajemnie połączonym ze sobą sieciom lokalnym, rozmieszczonym w wielu fizycznych lokalizacjach. Dzięki temu możliwa staje się jednoczesna i wielopłaszczyznowa interakcja pomiędzy użytkownikami z całego świata[2].

Na rozwój technologiczny związany z rozwojem Internetu wpływ miało wiele czynników. Zimna wojna była nie tylko okresem rywalizacji na tle militarnym, ale również technologicznym. Wówczas to rząd Stanów Zjednoczonych powołał agencję rządową Advances Research Project Agency, która funkcjonowała w strukturach Departamentu Obrony. Jej celem było tworzenie nowych projektów związanych z technologią wojskową[3].

Rozpoczęły się prace nad budową sieci komputerowych, których zadaniem było podtrzymanie ciągłości dowodzenia w przypadku ataku nuklearnego. Powstała wówczas sieć ARPANET. Kolejnym krokiem było podjęcie próby połączenia ze sobą

[1] J. Kulesza, *Międzynarodowe Prawo Internetu*, Poznań 2010, s. 55
[2] Tamże s. 56
[3] I. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 1

różnych sieci ARPANET, co stało się możliwe dzięki stworzeniu w latach 70. protokołu TCP/IP. Stał on się w późniejszym okresie podstawą struktury współczesnego Internetu[4]. W pierwszej połowie lat 80. ubiegłego stulecia protokoły TCP/IP zaczęły być powszechnie wykorzystywane przez wojsko, zaś w międzyczasie do powszechnego obiegu weszło pojęcie Internet – był to skrót od słów "inter" i "network", czyli "międzysieć", co oznaczało niemal nieograniczone możliwości tworzenia kolejnych sieci służących do wymiany informacji – zmniejszając przy tym udziały ARPANET-u.

Lata 90. były okresem, w którym zainteresowanie usługami sieciowymi zaczęły przejawiać firmy telekomunikacyjne[5]. Dniem, w którym Polska została przyłączona do Internetu był 12 września 1991 roku[6]. Od tego dnia musiało jednak jeszcze upłynąć sporo czasu, zanim użytkownicy zaczęli dostrzegać nowe możliwości, które przyniosło to narzędzie.

Internet miał służyć głównie celom badawczym i edukacyjnym. Charakteryzowała go możliwość uzyskania łatwego dostępu do różnego rodzaju informacji. Dynamiczny wzrost liczby użytkowników Internetu pozwolił zwrócić uwagę na kwestie związane z bezpieczeństwem. Osoby korzystające z zasobów sieci wywodziły się bowiem z różnych środowisk i grup społecznych.

Społeczeństwo uprzemysłowione wraz z rozwojem technologicznym rozpoczęło proces przekształcania się w społeczeństwo informacyjne. Rozwój Internetu spowodował, że informacja zaczęła przybierać coraz doskonalsze formy przekazu. Internet dobrze sprawdzał się nie tylko do uzyskiwania informacji, ale również do przekazywania jej innym. Powiązanie ze sobą komputerów i środków łączności dało możliwość podniesienia efektywności pracy i znacząco zmieniło wiele aspektów dotychczasowego życia. Wzrost zainteresowania Internetem doprowadził do powstania nowego miejsca dla ludzkiej aktywności - cyberprzestrzeni.

[4] J. Hofmolk, *Internet jako nowe dobro wspólne*, Warszawa 2009, s. 66
[5] Tamże
[6] T. Bienias, *Internet*, Kraków 1998, s. 8.

1.2. Rozwój technologii informatycznych

Skala zagrożeń związanych z przestępczością internetową rośnie wraz z rozwojem technologicznym. Coraz łatwiejszy dostęp do usług, takich jak bankowość elektroniczna, pociąga za sobą wzrost liczby różnorodnych form przestępczej aktywności[7].

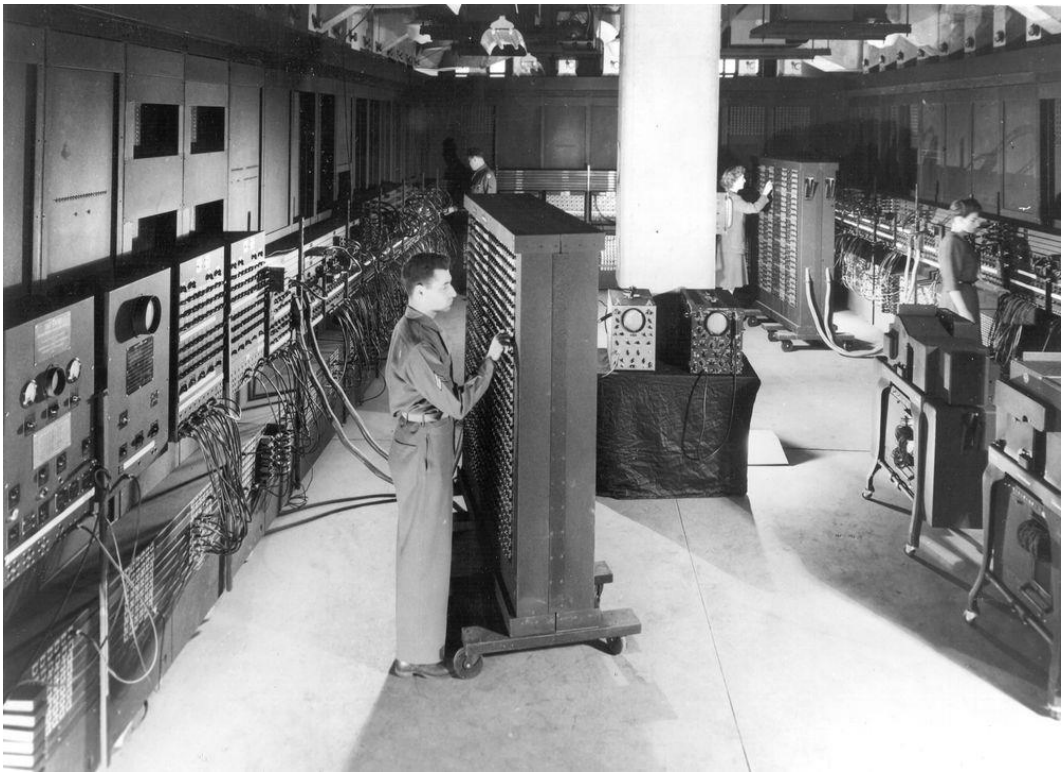
Podstawowy element cyberprzestrzeni stanowi tworząca ją technologia. Składają się na nią elementy infrastrukturalne poszczególnych sieci telekomunikacyjnych, czyli centrale i linie, urządzenia końcowe u użytkowników oraz warstwa programowa. Wszystkie te składniki są ze sobą fizycznie połączone. Kształt i funkcjonowanie cyberprzestrzeni uzależnione są właśnie od zastosowanych rozwiązań sprzętowych i programowych.

Większa dostępność nowoczesnych technologii przyczyniła się w konsekwencji do znacznego obniżenia kosztów produkcji takich elementów, jak układy scalone. To z kolei doprowadziło do tego, iż posiadanie komputera osobistego z dostępem do Internetu stało się rzeczą zupełnie oczywistą. Ogromna moc współczesnych komputerów pozostaje w korelacji z rosnącą ilością przetwarzanych przez nie danych. Dlatego też pojawiła się konieczność wykorzystania wydajnych nośników, które charakteryzować się będą nie tylko odpowiednią pojemnością, ale także szybkością odczytu i zapisu informacji.

Tak duża ilość przechowywanych informacji stanowi w wielu przypadkach trudność z punktu widzenia zwalczania nowych form przestępczości. Samo wyszukanie informacji jest niezwykle czasochłonnym i skomplikowanym procesem. Zastosowanie znajdują tu specjalistyczne narzędzia do informatyki śledczej, które pozwalają na filtrowanie danych w sposób automatyczny.

Za pierwszy i największy na świecie komputer stacjonarny uznaje się Eniac. Został zaprojektowany w 1945 roku przez J.P. Eckerta i J.W. Mauchly'ego z University of Pennsylvania's Moore School of Electrical Engineering. Publicznie zaprezentowano go jednak dopiero w lutym 1946 roku na Princeton University. Warto podkreślić, że był monstrualnym urządzeniem: zajmował 167 m^2 powierzchni, składał się z 42 szaf z blachy stalowej, sięgał ponad 2,4 metra wysokości i mierzył 24 metry długości. Jego łączna waga przekraczała 27 ton.

[7] R. Balkowski, *Bezpieczeństwo systemów teleinformatycznych - zmiany, trendy i zasady,* Warszawa 2018, s. 5

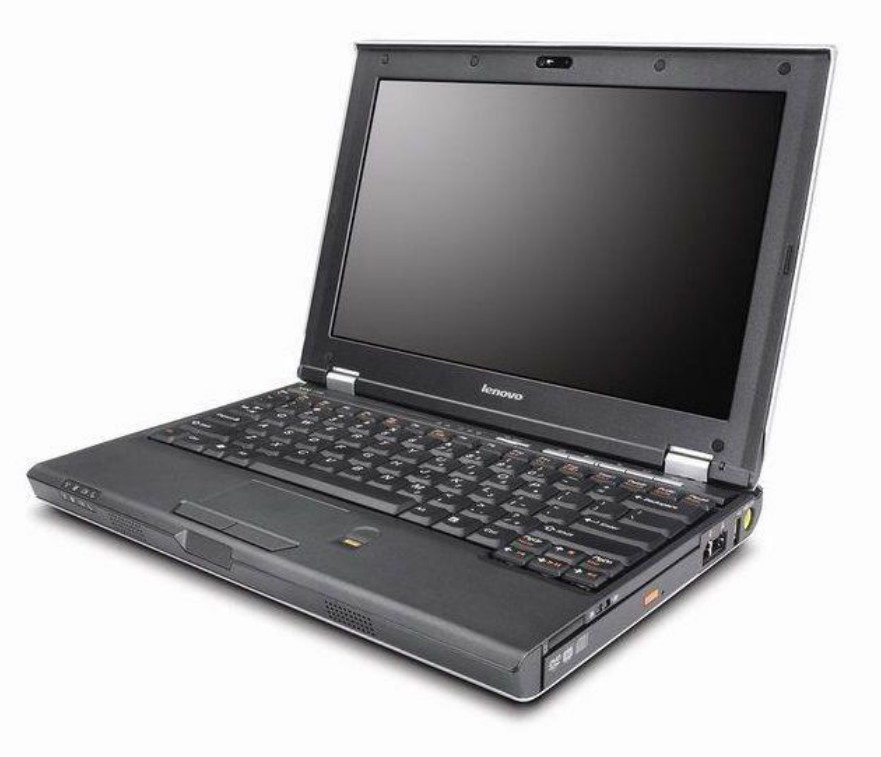


Ryc. 1. Eniac - pierwszy komputer na świecie.
Źródło: https://www.benchmark.pl/aktualnosci/historia-rozwoju-komputerow-i laptopow.html#noop [dostęp w dniu 05.09.2023 r.]

W późniejszym okresie jednym z najpopularniejszych komputerów był Commodore 64, który zadebiutował na rynku w 1982 roku i kosztował 595 dolarów.

Ryc. 2. Commodore 64.
Źródło: https://www.benchmark.pl/aktualnosci/historia-rozwoju-komputerow-i laptopow.html#noop [dostęp w dniu 05.09.2023 r.]

Lata 90. przyniosły rzeczywisty boom na komputery osobiste i laptopy oraz skokowy rozwój tej kategorii sprzętu. Wraz ze zwiększaniem się ich mocy obliczeniowej, zmniejszała się również masa, wskutek czego komputery osobiste stawały się stopniowo podstawowym wyposażeniem zwykłych użytkowników oraz firm. Przedsiębiorcy zaczęli z nich korzystać, a dobry komputer stał się synonimem prestiżu.



Ryc. 3. Lenovo A100.
Źródło: https://www.benchmark.pl/aktualnosci/historia-rozwoju-komputerow-i laptopow.html#noop [dostęp w dniu 05.09.2023 r.]

Obecnie szczytem osiągnięć techniki komputerowej są urządzenia typu 2-w-1, które mogą działać zarówno jak tablety (dotykowy ekran), ale też laptopy (dopinana do ekranu klawiatura). Ich głównymi zaletami są właśnie mobilność oraz wielofunkcyjność. Dzięki niewielkiej wadze i rozmiarom, można je ze sobą zabrać praktycznie wszędzie. Ogromną popularność zyskały także smartfony, które swoimi parametrami nie ustępują współczesnym komputerom. Stanowią one zwieńczenie procesu miniaturyzacji sprzętu komputerowego.

Ryc. 4. Microsoft Surface RT.

Źródło: https://www.benchmark.pl/aktualnosci/historia-rozwoju-komputerow-i laptopow.html#noop [dostęp w dniu 05.09.2023 r.]

1.3. Charakterystyka sieci komputerowych

Sieci komputerowe stanowią obecnie element, który nieodzownie łączy się z wykorzystaniem sprzętu komputerowego. To właśnie funkcjonalność sieciowa jest jedną z podstawowych i najważniejszych cech komputera. Sieci komputerowe znajdują swoje praktyczne zastosowanie właściwie we wszystkich obszarach związanych z ludzką aktywnością. Służą między innymi do zawierania umów na odległość, usprawniają przesyłanie różnego rodzaju informacji, wspomagają prowadzenie baz danych i wspierają procesy zarządzania pracą.

W najprostszym rozumieniu sieć komputerowa oznacza takie połączenie komputerów, które umożliwia im wzajemną wymianę oraz współdzielenie danych. W celu

zbudowania sieci niezbędne są przynajmniej dwa komputery. Muszą być one wyposażone w urządzenia sieciowe, protokół sieciowy oraz łącze[8].

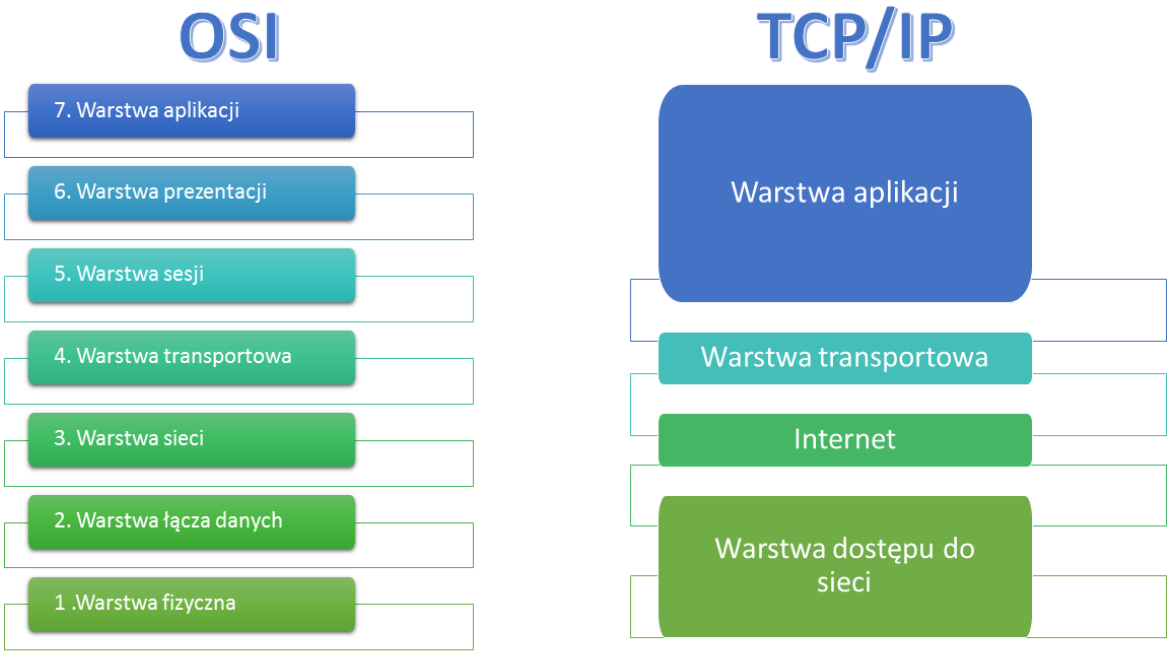
Wyróżnia się sieci lokalne, zwane Local Area Network, które buduje się w celu dzielenia jednego łącza internetowego na kilka komputerów. Z takim rozwiązaniem można się spotkać najczęściej w przypadku wewnętrznych sieci biurowych lub domowych. Istnieją także sieci rozległe, czyli Wide Area Network, czego prostym przykładem i nadrzędnym przedstawicielem jest właśnie Internet[9].

W celu opisu budowy i działania sieci komputerowych wykorzystywany jest model Open System Interconnection (OSI). Został on stworzony w celu ustandaryzowania rozwiązań sieciowych, które były dostarczane przez różnych producentów[10].

Model OSI zakłada, że sieć zbudowana została z siedmiu warstw, do których zalicza się: warstwa fizyczna, łącza danych, sieciowa, transportowa, sesji, prezentacji oraz aplikacji. Dzięki nim pojawia się możliwość szczegółowego określenia pełnej drogi, jaką przebywają dane. Cały proces rozpoczyna się w najwyższej warstwie, jaką jest warstwa aplikacji. Następnie przedostają się one kolejno w dół, aż do warstwy fizycznej. Przed wysłaniem dane wraz z przekazywaniem do niższych warstw sieci zmieniają swój format, co nosi nazwę procesu kapsułkowania. Kolejnym krokiem jest przechodzenie przez warstwy w odwrotnym kierunku, by w rezultacie dotrzeć do aplikacji komputera docelowego[11].

Zamiennie wykorzystywany jest także model TCP/IP, który stanowi implementację modelu OSI. Podobnie jak poprzednik, stworzony został w oparciu o logicznie wydzielone warstwy, które posiadają hierarchiczną budowę. Model TCP/IP posiada warstwę dostępu do sieci, Internetu, transportową i aplikacji. Uproszczona budowa miała na celu lepsze odzwierciedlenie etapów, podczas których wykonywane są procesy sieciowe[12].

[8] J. Wasilewski, *Cyberprzestępczość - wybrane aspekty prawnokarne i kryminalistyczne,* Białystok 2017, s. 136
[9] Tamże, s. 135
[10] Tamże s. 136
[11] Tamże
[12] Tamże s. 137



Ryc. 5. Warstwy sieci komputerowych – model OSI i TCP/IP.

Źródło: https://egzamin-e13.pl/projektowanie-lokalnych-sieci-komputerowych-2/warstwy-sieci-komputerowych-model-osi-i-tcpip/ [dostęp w dniu 05.09.2023 r.]

Podstawowe protokoły komunikacji, które zostały wykorzystane w tym modelu - TCP i IP, stanowią fundament dla całego ruchu sieciowego. Działając na poszczególnych warstwach, tworzą one podstawowe zasady oraz instrukcje wymiany danych. Protokół TCP odpowiada za nawiązywanie i obsługiwanie połączenia między dwoma zakończeniami sieci. Protokół działa w warstwie transportowej. Kolejnym zadaniem protokołu jest weryfikacja poprawności przesyłania danych. Dzięki temu można uniknąć przesłania niekompletnych danych lub też takich, których nie da się odczytać. Finalnie protokół TCP dokonuje zakończenia połączenia poprzez wymianę odpowiednich poleceń[13].

Protokół IP funkcjonuje w warstwie Internetu. Umożliwia on hostowi określenie dokładnej ścieżki prowadzącej przez elementy infrastrukturalne sieci, dzięki czemu możliwe staje się zestawienie logicznego połączenia pomiędzy stronami i dostarczenie plików do odbiorcy[14].

[13] M. Hassan, J. Raj, *Wysoko wydajne sieci TCP/IP*, Gliwice 2004 s. 22
[14] J. Wasilewski, *Cyberprzestępczość - wybrane aspekty prawnokarne i kryminalistyczne,* Białystok 2017, s. 139

Taki sposób działania pozwala na łączenie ze sobą dwóch dowolnych punktów sieci, nawet jeśli nie występują między nimi bezpośrednie łącza. Internet stanowi bowiem sieć powiązań, w której dwa punkty można ze sobą połączyć na setki różnych sposobów. Rozwiązanie wynika z faktu, iż w pierwotnym zamyśle Internet został zaprojektowany na potrzeby wojskowe. Cechować miała go zatem zdolność do zestawiania i utrzymywania połączeń na duże odległości, nawet jeśli część pośredniczących węzłów zostanie zniszczona.

Trasowanie ruchu sieciowego odbywa się za pomocą adresu IP. Stanowi on identyfikator zakończeń sieci Internet i pozwala na fizyczne lokalizowania punktów, między którymi dochodzi do wymiany informacji. Za jego pomocą możliwe staje się także ustalenie ścieżki, którą pakiety muszą przebyć w celu dotarcia do końcowego odbiorcy.

Z uwagi na fakt, iż adres IP wskazuje wyłącznie na wykorzystywane zakończenie sieci, nie można bezpośrednio utożsamiać go z konkretnym użytkownikiem, który generuje ruch sieciowy, a więc również ewentualnym sprawcą cyberprzestępstwa. Najczęściej jest on bowiem przypisywany przez dostawcę Internetu danemu zakończeniu sieci dynamicznie, czyli wyłącznie na czas trwania danej sesji.

Biorąc pod uwagę tego typu rozwiązanie w celu zwalczania przestępczości komputerowej konieczne staje się weryfikowanie informacji, do którego zakończenia przypisany był konkretny adres IP w ściśle określonym czasie, w którym doszło do popełnienia przestępstwa. Służą do tego logi operatora, które zawierają szczegółowe informacje dotyczące ruchu sieciowego. Analogiczną funkcję w sieciach telefonicznych pełnią billingi.

Kolejnym identyfikatorem służącym do określania ruchu sieciowego jest Media Access Control (MAC), który nie określa zakończenia sieci, a konkretny egzemplarz urządzenia zastosowanego do jej obsługi. MAC pełni podobną rolę jak numer IMEI w telefonie komórkowym. Zawarte są w nim informacje na temat producenta sprzętu oraz unikatowy numer konkretnego egzemplarza urządzenia sieciowego. Z punktu widzenia cyberprzestępczości należy jednak podkreślić, że zdecydowana większość producentów daje możliwość swobodnej zmiany adresu MAC[15]. Taki zabieg ma na celu przede wszystkim ułatwienie konfiguracji urządzeń sieciowych, jednak sytuacja

[15] J. Wasilewski, *Cyberprzestępczość - wybrane aspekty prawnokarne i kryminalistyczne,* Białystok 2017, s. 142

może być wykorzystywana przez przestępców do ukrycia identyfikujących ich danych albo nawet podszycia się pod inną osobę.

Ukrywanie faktycznego źródła ruchu sieciowego wiąże się z powstaniem sporych trudności z ustaleniem sprawcy. Kwestia ta w głównej mierze dotyka stosowania serwerów proxy, które służą do przekierowywania i ukrywania ruchu, a także korzystania z usług anonimizujących, łączenia się za pomocą niezabezpieczonych punktów bezprzewodowych lub przejmowania kontroli nad komputerami innych użytkowników.

Z sieciami komputerowymi wiąże się również pojęcie zabezpieczeń kryptograficznych, które wykorzystywane są w celu szyfrowania przekazywanych pomiędzy komputerami informacji. Kryptografia stosowana jest głównie do zabezpieczania haseł dostępowych. Rosnący poziom zagrożeń spowodował, że coraz częściej można się z nią spotkać także w przypadku ochrony danych korporacyjnych lub też prywatnych. Kontrola zaszyfrowanego ruchu wymaga stosowania specjalistycznego dekryptażu. Tego rodzaju czynności potrafią zabierać śledczym sporo czasu, a to właśnie czas bardzo często stanowi najistotniejszy czynnik warunkujący skuteczność postępowania.

1.4. Zjawisko cyberprzestępczości

W przypadku czynów popełnianych przy pomocy elektronicznych systemów przetwarzania informacji celem naruszania dóbr chronionych przez prawo, literatura korzysta z różnego rodzaju określeń. Zaliczają się do nich: cyberprzestępczość, przestępczość komputerowa, przestępczość przy użyciu zaawansowanych technologii lub też przestępczość związana z komputerami. Zastosowanie znajdują także takie określenia, jak przestępstwa związane z technologią cyfrową oraz przestępstwa internetowe[16].

Polskie przepisy nie definiują wprost wskazanych pojęć. Natomiast próby ich bardziej szczegółowego określenia podejmowane są przez kryminologów i dogmatyków prawa karnego. Przestępstwa komputerowe określane są zatem jako działania przestępcze, w których narzędzie lub przedmiot zamachu stanowi komputer. W zakres tego zjawiska wchodzą wszelkie zachowania przestępne, które wiążą się

[16]A. Adamski, *Prawo karne komputerowe,* Warszawa 2000, s. 33

z funkcjonowaniem elektronicznego przetwarzania danych i godzą bezpośrednio w przetwarzaną informację, jej nośnik i obieg w całym systemie komputerowym[17].

Przestępstwa komputerowe mogą być czynami, które skierowane zostały na dane, programy komputerowe oraz systemy, a także przestępstwami, w których to komputer stanowi narzędzie przestępstwa. O tego rodzaju czynach można więc mówić w znaczeniu wąskim i szerokim. Wąskie rozumienie przestępstwa komputerowego wskazuje, iż musi ono obejmować czyny popełnione z wykorzystaniem komputera. Zalicza się do nich między innymi nielegalne uzyskanie oprogramowania komputerowego, oszustwo komputerowe lub sabotaż komputerowy. Natomiast w szerokim rozumieniu przestępstwa komputerowe mogą obejmować wszystkie czyny, gdzie komputer był narzędziem przestępstwa albo stanowił przedmiot lub środowisko zamachu[18].

Rozwój technologiczny miał wpływ nie tylko na charakter przestępczości komputerowej, ale także doprowadził do pewnej ewolucji w stosowanej terminologii. Jeśli bowiem komputer zaczął być powszechnie wykorzystywany w praktycznie wszystkich obszarach życia, definiowanie przestępstw komputerowych jako czynów popełnianych przy użyciu tego narzędzia zaczęło tracić na analitycznej ostrości.

Zarówno systemy, jak i sieci teleinformatyczne mogą stać się przedmiotem lub środowiskiem zamachu. Jednocześnie mogą służyć do naruszania różnego rodzaju dóbr prawnie chronionych, w tym także do rozpowszechniania informacji prawnie zabronionych, takich jak na przykład pornografia z udziałem małoletnich. Może się również okazać, że pełnią one funkcję wyłącznie incydentalną, która polega na wymianie informacji lub wykonywaniu zadań dodatkowych związanych z określonym przestępstwem, na przykład w postaci przechowywania informacji na temat nielegalnego handlu bronią lub sprzedaży narkotyków.

Problematyka terminologiczna spowodowana była rozwojem nowych form popełniania cyberprzestępstw. Choć pierwsza generacja przestępstw komputerowych obejmowała głównie ataki skierowane na komputer, dane oraz sieci, obecnie mamy do czynienia z wysokim poziomem automatyzacji. W rezultacie czyny nie są popełniane bezpośrednio przez napastników, ale są następstwem wykorzystania do tego celu specjalistycznego oprogramowania.

[17] M. Siwicki, *Podział i definicja cyberprzestępstw,* Prokuratura i Prawo 7-8, s. 244
[18] Tamże

Duży wkład w wypracowanie odpowiednich norm w zakresie przeciwdziałania przestępstwom popełnianym przy pomocy komputerów oraz ujednolicenia stosowanej terminologii mają międzynarodowe inicjatywy, podejmowane między innymi przez Radę Europy lub Organizację Narodów Zjednoczonych.

Komisja Wspólnot Europejskich korzysta z definicji mówiącej o tym, że za cyberprzestępstwa należy uznać czyny przestępcze, które zostały dokonane przy użyciu sieci łączności elektronicznej lub systemów informatycznych albo są skierowane przeciwko tym sieciom i systemom[19]. Cyberprzestępstwa dzieli na trzy podstawowe grupy czynów. W pierwszej grupie znajdują się tradycyjne formy przestępstw, takie jak fałszerstwo lub oszustwo, które zostało popełnione za pomocą sieci i systemów informatycznych. W drugiej grupie znalazła się publikacja nielegalnych treści w postaci materiałów związanych z wykorzystaniem seksualnym dzieci lub też nawoływania do nienawiści na tle rasowym. W ostatniej grupie znalazły się natomiast przestępstwa typowe dla sieci elektronicznej. Zaliczają się do nich ataki na systemy informatyczne i sabotaż komputerowy.

Konwencja Rady Europy o cyberprzestępczości stanowi natomiast, że przestępstwa dzielą się na:

1) przestępstwa przeciwko poufności, integralności i dostępności danych oraz systemów,
2) przestępstwa komputerowe,
3) przestępstwa ze względu na charakter zawartych informacji,
4) przestępstwa związane z naruszeniem praw autorskich i pokrewnych[20].

Inny podział przyjęła Międzynarodowa Organizacja Policji Kryminalnych. Interpol dzieli cyberprzestępstwa na zamachy polegające na naruszaniu praw dostępu do zasobów, powielanie programów, sabotaż sprzętu oraz oprogramowania, oszustwa przy użyciu komputera, przechowywanie zabronionych zbiorów i przestępstwa popełnione w sieci[21].

[19] M. Siwicki, *Podział i definicja cyberprzestępstw,* Prokuratura i Prawo 7-8, s. 247
[20] Tamże, s. 247-248
[21] Tamże, s. 249

Natomiast polska doktryna cyberbezpieczeństwa mówi o czynach dokonywanych z potencjalnym lub rzeczywistym użyciem przemocy, a także o czynach dokonywanych bez użycia przemocy[22].

Głównym kryterium zaliczania poszczególnych czynów do kategorii cyberprzestępstw jest możliwość wystąpienia ich w obszarze cyberprzestrzeni. Jednocześnie żeby stwierdzić, że dany czyn został popełniony w obszarze cyberprzestrzeni wystarczy wykazać wystąpienie w domenie cyfrowej choćby jednego z elementów, którymi są przestępcze działanie, zaniechanie lub skutek. Tak szeroki zakres definicji wyznacza nowoczesny kierunek utożsamiania cyberprzestępczości z czynami popełnionymi w cyberprzestrzeni, niezależnie od formy i szczegółowych metod działania sprawcy.

1.5. Skala problemu

Cyberprzestępczość stanowi jeden z najpoważniejszych problemów, z którym zmierzyć muszą się gospodarki na całym świecie. Pomimo tego, że o zjawisku dyskutuje się już dość długo, w dalszym ciągu wykorzystywanie nowoczesnych technologii do celów niezgodnych z prawem jest poważnym problemem zarówno dla ustawodawców, jak i organów egzekwujących prawo. Jednocześnie do ataków dochodzi coraz częściej. Są one również bardziej wyrafinowane i kosztowne.

Określenie skali tego zjawiska nie jest prostym zadaniem. Polska oraz wiele innych państw nie dysponują bowiem odpowiednimi mechanizmami magazynowania danych. Z tego względu statystyki kryminalne dają wyłącznie przybliżony obraz[23]. Odpowiadają za to zarówno problemy definicyjne oraz fakt, iż funkcjonariusze często napotykają na trudności związane z określeniem właściwej kwalifikacji prawnej poszczególnych czynów, które popełnione zostały w cyberprzestrzeni[24].

Samo zjawisko cyberprzestępczości jest bardzo zmienne i dynamiczne. Wynika to w dużej mierze z różnorodności metod wykorzystywanych przez sprawców. Okazało się bowiem, że najistotniejszym elementem nie jest wcale samo naruszenie integralności oraz poufności danych, a fakt w jaki sposób sprawcy uzyskują do nich dostęp. Pozwoliło to wskazać na bardzo poważne braki w systemach bezpieczeń-

[22] M. Siwicki, *Podział i definicja cyberprzestępstw,* Prokuratura i Prawo 7-8, s. 249
[23] M. Siwicki, *Cyberprzestępczość,* Warszawa 2013, s.47-48
[24] A. Adamski, *Cyberprzestępczość - aspekty prawne i kryminologiczne*, „Studia Prawnicze", Zeszyt 4 (166) 2005, Warszawa 2006, s. 68-9

stwa. W rezultacie rozpoczął się proces poszukiwania wykorzystywanych przez sprawców luk w zabezpieczeniach[25].

Sprawcy przestępczości komputerowej często działają znacznie szybciej niż jednostki odpowiedzialne za zapewnienie bezpieczeństwa. Nieustannie doskonalą bowiem swoje umiejętności. Dlatego ofiarami cyberprzestępstw najczęściej padają małe oraz średnie przedsiębiorstwa, które nie posiadają rozbudowanych środków celem zapewnienia bezpieczeństwa sieciowego na wysokim poziomie[26].

Niepokoi także wzrost liczby ataków przy wykorzystaniu szkodliwego oprogramowania. Wiążą się one z przenikaniem do wnętrza zainfekowanego komputera oraz kodowania danych będących własnością użytkownika. Następnie program zamieszcza notatkę, w której zawarte zostały żądania wobec właściciela plików. Najczęściej dotyczą one przelania środków finansowych, po czym sprawca wysyła instrukcję pozwalającą na odzyskanie danych[27].

Przez oszustów wykorzystywane są również portale społecznościowe. Użytkownicy są bowiem bardziej skłonni do klikania w treści umieszczone przez znane im osoby. Dlatego strony phishingowe naśladują popularne platformy, takie jak Facebook[28].

Warto zdawać sobie sprawę z tego, że narażone są nie tylko komputery. Cyberprzestępcy wykazują także zainteresowanie bankomatami lub domowymi routerami. Dodatkowo wiele urządzeń może być w obecnych czasach obsługiwana za pomocą telefonu komórkowego. Podczas instalacji różnego rodzaju aplikacji użytkownik zobowiązany jest do wyrażenia zgody na dostęp do znajdujących się w pamięci urządzenia informacji. Nieustanny wzrost liczby użytkowników Internetu, obniżenie ich wieku oraz fakt większego uzależnienia wielu sfer życia od technologii doprowadzają do tego, że cyberprzestępczość może nieść ze sobą coraz poważniejsze konsekwencje[29].

[25] I. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 23
[26] Tamże
[27] Tamże, s. 24
[28] M. Siwicki, *Cyberprzestępczość,* Warszawa 2013, s. 52
[29] Tamże, s. 136

Rozdział II

Wybrane przestępstwa w cyberprzestrzeni

2.1. Oszustwa i fałszerstwa komputerowe

Przestępstwa popełniane z udziałem komputera to ataki skierowane przeciwko tradycyjnym dobrom prawnym. Nie są one w bezpośredni sposób skierowane przeciwko integralności, poufności i dostępności danych informatycznych. Dlatego też działania prewencyjne w tym przypadku nie są związane z potrzebą zapewnienia systemom informatycznym odpowiedniego stopnia ochrony[30]. Do tego rodzaju przestępstw zaliczyć można oszustwo oraz fałszerstwo komputerowe.

Oszustwo komputerowe wiąże się w bezpośredni sposób z postępem technologicznym i rozwojem komunikacji elektronicznej. Klasyczne oszustwo stało się dla przestępców narzędziem niewystarczającym, bowiem na skutek automatyzacji różnego rodzaju procesów związanych z wymianą dóbr i świadczeniem usług, relacje pomiędzy ludźmi zostały wyparte przez relacje człowiek-maszyna[31].

Oszustwa w Internecie można podzielić na dwie duże kategorie: przestępstwa, w których komputer jest celem i takie, w których jest narzędziem. Te pierwsze wymagają od sprawców znacznie większej wiedzy specjalistycznej i to właśnie na nie społeczeństwo jest bardziej nieprzygotowane. Przestępstwa te zwykle opierają się na zastosowaniu złośliwego oprogramowania, takiego jak: wirus, robak, malware, ransomware, spyware, koń trojański, exploit, keylogger.

Cyberprzestępstwa, w których komputer jest narzędziem, to przestępstwa o wiele mniej wyrafinowane technicznie, przez co o wiele bardziej powszechne. W przypadku tych zagrożeń oszuści wykorzystują ludzkie słabości lub strach. Najpopularniejszymi atakami bazującymi na emocjach są:

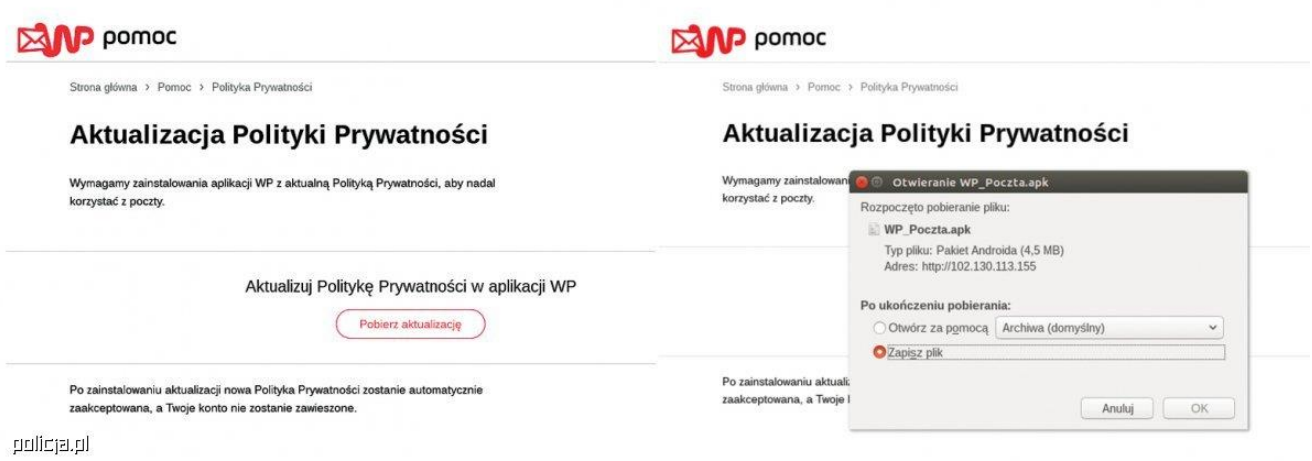
- Phishing – to metoda, w której przestępca podszywa się pod inną osobę lub instytucję. Skłania użytkownika w wiadomości e-mail lub SMS do odwiedzenia

[30] A. Suchorzewska, *Ochrona systemów informatycznych wobec zagrożeń cyberterroryzmem*, Warszawa 2010, s. 235-236
[31] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s.115

określonej strony internetowej. Nieświadomy odbiorca ujawnia tam często poufne informacje, takie jak loginy i hasła do bankowości elektronicznej czy numery kart kredytowych;

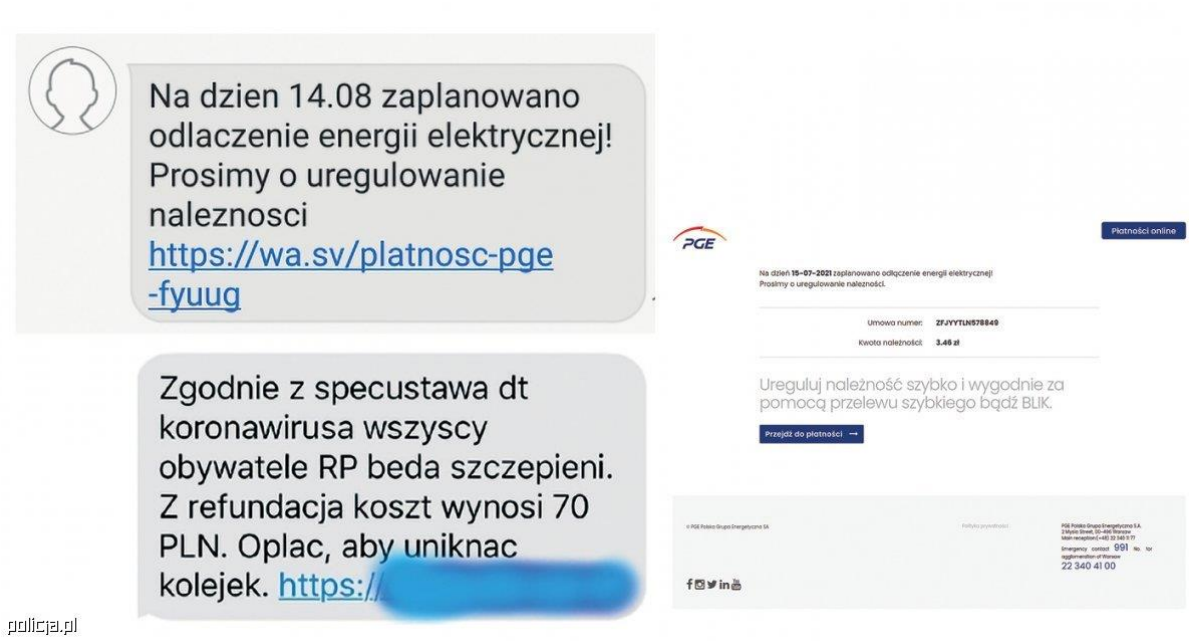
- Scam – to oszustwo wykorzystujące techniki inżynierii społecznej. Polega na wzbudzeniu zaufania drugiej osoby, dzięki czemu możliwe jest łatwe sterowanie jej wyborami i zmuszenie jej do powierzenia np. swoich pieniędzy czy danych osobowych;
- Oszustwo nigeryjskie – jest swego rodzaju typową odmianą scamu. To przestępstwo, które pierwotnie było rozpowszechniane za pośrednictwem faksu, telefonu i tradycyjnej poczty, ale Internet sprawił, że stało się o wiele bardziej powszechne. Polega ono na tym, że ofiara otrzymuje komunikat od kogoś, kto potrzebuje pomocy w transferze dużej sumy pieniędzy z obcego kraju. Często przestępcy wcześniej przez wiele tygodni starają się wzbudzić zaufanie u ofiary, aby na końcu poprosić o pomoc, która sprowadza się do przekazania pieniędzy[32].

Oszustwa phishingowe mogą przybierać formę fałszywych wiadomości SMS lub szkodliwego oprogramowania, które ukrywa się pod akceptacją regulaminu.



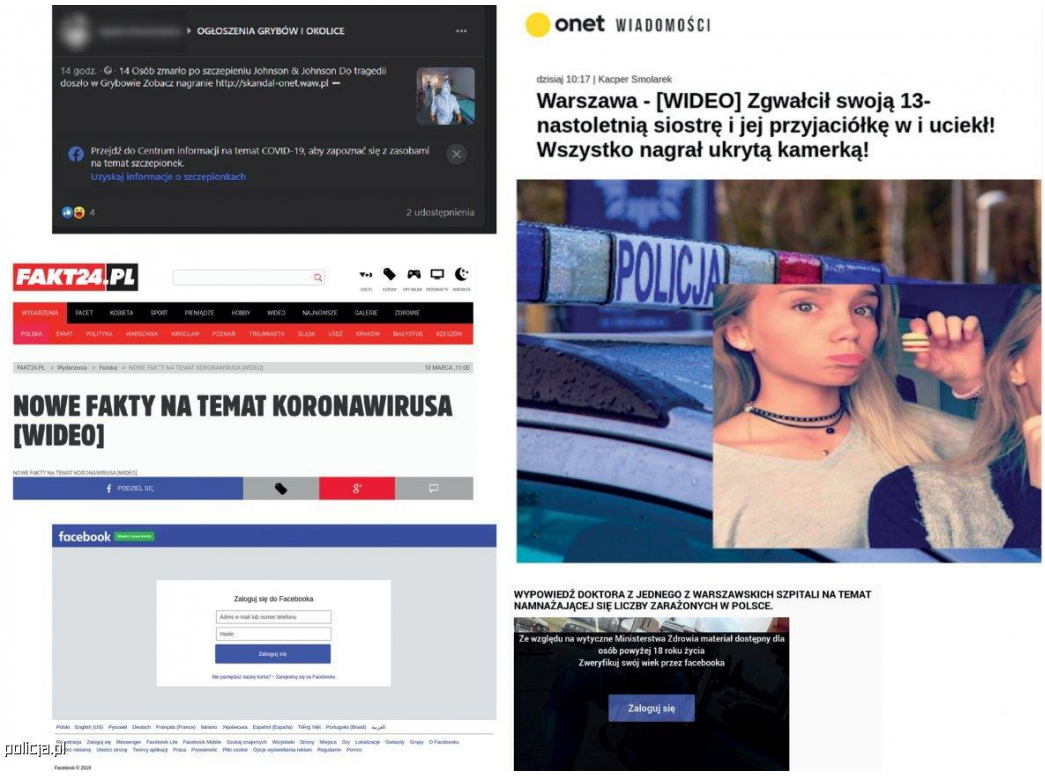
Ryc. 6. Szkodliwe oprogramowanie ukryte pod aktualizacją polityki prywatności.
Źródło: https://policja.pl/pol/aktualnosci/212455,Top-5-najczestszych-technik-phishingowych.html [dostęp w dniu 08.09.2023 r.]

[32] https://blik.com/oszustwa-internetowe-jakie-cyberataki-sa-dzis-najpopularniejsze [08.08.2023]



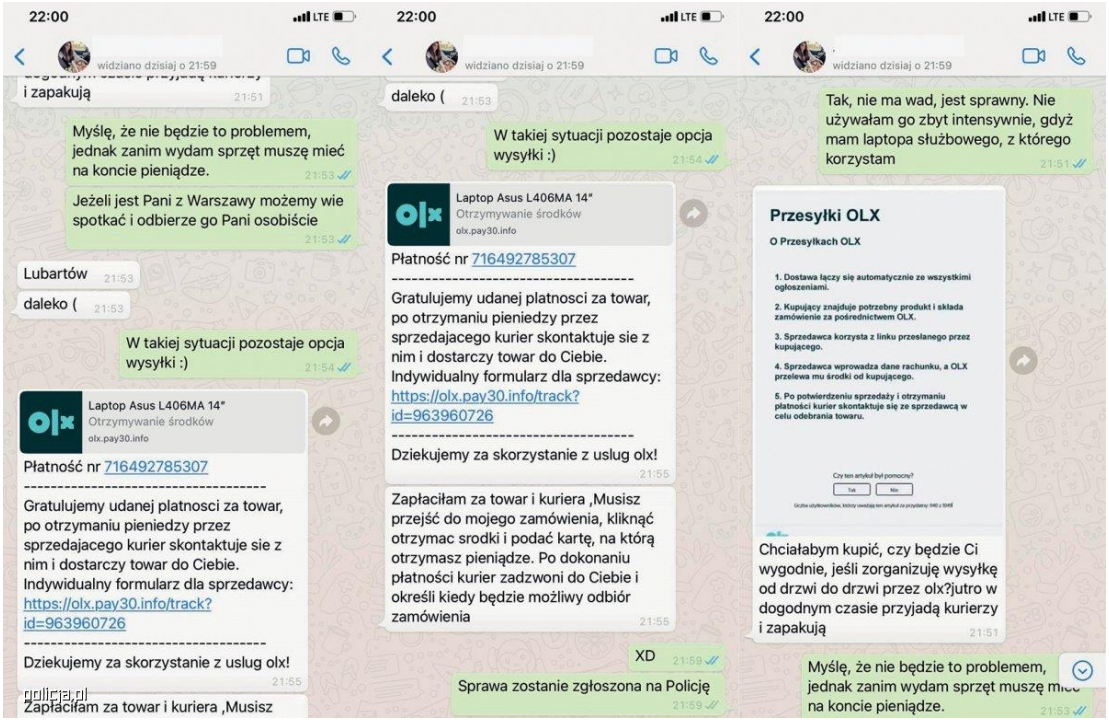
Ryc. 7. Fałszywy sms z przekierowaniem do płatności.

Źródło: https://policja.pl/pol/aktualnosci/212455,Top-5-najczestszych-technik-phishingowych.html [dostęp w dniu 08.09.2023 r.]



Ryc. 8. Fałszywe strony wyłudzające dane do logowania.

Źródło: https://policja.pl/pol/aktualnosci/212455,Top-5-najczestszych-technik-phishingowych.html [dostęp w dniu 08.09.2023 r.]



Ryc. 9. Oszustwo na przesyłkę i płatność OLX.
Źródło: https://policja.pl/pol/aktualnosci/212455,Top-5-najczestszych-technik-phishingowych.html [dostęp w dniu 08.09.2023 r.]

2.2. Pornografia dziecięca

Internet daje ogromne możliwości udostępniania i publicznego przekazywania różnego rodzaju informacji, dotyczących zarówno swojego życia, wydarzeń i opinii. Pomimo wielu zalet związanych z tym zjawiskiem, nie należy zapominać o konieczności przeciwdziałania prezentowaniu informacji, które są zakazane przez prawo.

Przez pojęcie pornografii należy rozumieć przedstawienie przejawów życia seksualnego ze szczególnym zwróceniem uwagi na uwidocznienie narządów płciowych i z wyłączeniem wszelkich aspektów psychicznych oraz społecznych związanych z seksualnością człowieka[33].

Pornografia dziecięca jest niezwykle istotnym problemem, który wymaga podjęcia stosownych działań na szczeblu międzynarodowym. Rozwój Internetu dopro-

[33] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawnokarne*, Warszawa 2011, s. 132

wadził do zwiększenia ilości pornografii dziecięcej oraz wzrostu liczby przestępstw seksualnych popełnianych przeciwko dzieciom i młodzieży[34].

Pornografia dziecięca to materiały pornograficzne, które w wyraźny sposób przedstawiają:

- osobę małoletnią w trakcie czynności seksualnej,
- osobę, która wydaje się być małoletnią, w trakcie czynności wyraźnie seksualnej,
- realistyczny obraz osoby małoletniej w trakcie czynności wyraźnie seksualnej[35].

Za czynność wyraźnie seksualną uznawany jest stosunek seksualny, sodomia, masturbacja, masochistyczne lub sadystyczne wykorzystanie w kontekście seksualnym oraz lubieżne obnażanie narządów płciowych lub miejsc intymnych ciała dziecka[36].

Szeroki dostęp do sieci sprawił, że niemal wszystkie formy pornografii stały się łatwo dostępne. Internet z jednej strony ułatwił sprawcom możliwość popełniania przestępstw kontaktowych przeciwko dzieciom, a z drugiej zapewnia zdecydowanie łatwiejszy dostęp do pornografii dziecięcej. Materiały znaleźć można za pośrednictwem grup dyskusyjnych lub aplikacji P2P.

W kontekście cyberprzestępczości warto wspomnieć także o pozorowanej i wirtualnej pornografii dziecięcej. Jest ona efektem manipulacji obrazem lub też specjalnej charakteryzacji osoby dorosłej, tak aby wyglądała na dziecko. Wirtualna pornografia pozwala na generowanie za pomocą systemów komputerowych realistycznych wizerunków osób małoletnich. Nie są to jednak prawdziwe osoby, a wyłącznie komputerowo wygenerowane fantomy. Dochodzi do sytuacji, w której odróżnienie prawdziwej pornografii dziecięcej od tej pozorowanej staje się zadaniem zdecydowanie trudniejszym[37].

W procesie produkcji wirtualnej pornografii dziecięcej stosowane jest specjalistyczne oprogramowanie. Materiały często powstają w wyniku nakładania fotografii małoletniego na twarz osoby dorosłej, biorącej udział w czynności seksualnej. Wyko-

[34] J. Carr, *Internet a wykorzystywanie seksualne dzieci i pornografia dziecięca, "*Dziecko krzywdzone" nr 13, Warszawa 2005, s. 2
[35]I. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 81
[36] Tamże, s. 81-82
[37] M. Siwicki, *Cyberprzestępczość,* Warszawa 2013, s.184

rzystana zostaje tak zwana technika morfingu, polegająca na wykorzystaniu jednego obrazu przy produkcji innego, za pomocą ich płynnej zmiany[38].

2.3. Grooming

Grooming jest pojęciem związanym z uwodzeniem, czyli procesem polegającym na zaprzyjaźnianiu się sprawcy z dzieckiem, celem jego późniejszego wykorzystania. To również zachęcanie dziecka do udziału w różnego rodzaju czynnościach seksualnych, dyskutowanie na temat intymnych zachowań lub prezentowanie treści o charakterze pornograficznym. Kontakt z dzieckiem nawiązywany jest w szczególności przy wykorzystaniu Internetu[39].

Choć zjawisko groomingu nie jest nowe, to właśnie dynamiczny rozwój nowoczesnych technologii wykorzystywanych w procesie komunikacji, przyczynił się do ułatwienia możliwości nawiązania przez sprawców kontaktu z osobami małoletnimi. Grooming nie jest pojedynczym działaniem, a całym procesem składającym się z szeregu zachowań sprawcy, którego efektem staje się zdobycie zaufania przy wykorzystaniu technik manipulacyjnych[40].

Upowszechnienie dostępu do sieci otworzyło przed sprawcami przestępstw nowe możliwości. Środowiska osób o skłonnościach pedofilskich stopniowo zaczęły przenosić swoją działalność w bezpieczniejsze dla nich miejsce, które dodatkowo dostarczało im również nowych możliwości. Rzeczywistość wirtualna pozwalała bowiem na budowanie relacji o charakterze seksualnym, które nie byłyby możliwe w świecie realnym[41].

Internet stał się doskonałym miejscem dla rozwoju różnego rodzaju patologii, przede wszystkim na anonimowość lub też złudne poczucie anonimowości oraz powszechność, przez co zapewniona została wręcz nieograniczona liczba potencjalnych ofiar. Dostępny jest także niezwykle szeroki dostęp do narzędzi i platform komunikacji. Oczywiście sam Internet jest wyłącznie technologią, która bez udziału

[38] Tamże, s. 185
[39] Tamże, s. 188
[40] M. Dąbrowska, *Grooming - wybrane aspekty prawnokarne i kryminologiczne,* Warszawa 2018, s. 12
[41] E. Martellozo, *Online Child SexualAbuse: Grooming, Policing and Child Protection in a Multi-Media World, Routledge*, New York 2012, s. 9

człowieka pozostaje nieaktywna. Wobec tego kluczowe znaczenie odgrywa w tym przypadku czynnik ludzki.

Za pierwsze stadium groomingu uznawane jest nawiązanie kontaktu z małoletnim. Sprawca wcześniej zbiera informacje na temat potencjalnych ofiar. Są one dostępne w przestrzeni publicznej, na przykład w pokojach czatów, na portalach społecznościowych lub blogach. Uzyskane w taki sposób dane podlegają selekcji, w celu dokonania wyboru najbardziej atrakcyjnej ofiary, którą łatwo będzie można poddać manipulacji. Na tym etapie dąży się do zdobycia jak największej liczby informacji na temat konkretnego małoletniego. Równolegle odbywają się także czynności przygotowawcze polegające między innymi na kreowaniu fałszywej tożsamości. Możliwość wglądu w spreparowane przez sprawcę informacje, które umieszczone zostały przez niego w Internecie, budują w oczach dziecka większą wiarygodność oraz skracają dystans pomiędzy sprawcą i ofiarą[42].

Początkowo kontakt opiera się na niegroźnej relacji, pozbawionej kontekstu seksualnego. Wybierane są głównie cieszące się popularnością portale społecznościowe, czaty, serwisy randkowe lub komunikatory internetowe. Następnie sprawca dąży do przeniesienia rozmowy na grunt prywatny, by móc kontynuować dalszą korespondencję sam na sam z dzieckiem.

Kolejnym stadium jest próba stworzenia silnej relacji. Dąży się do tego przed zintensyfikowanie kontaktu, coraz dłuższe oraz częstsze rozmowy. Dzięki poświęcaniu uwagi wytwarza się w dziecku poczucie akceptacji, staje się ono w swoim odczuciu ważne i wyjątkowe. Na tym etapie pojawić się może również rozmowa głosowa, której celem będzie skrócenie dystansu oraz nadanie bardziej realnego charakteru tej relacji[43].

Następnie sprawca przechodzi do kalkulowania ryzyka wykrycia internetowej znajomości przez rodziców dziecka lub bliskich z jego otoczenia. Zdobywa informacje na temat charakteru sprawowanej kontroli rodzicielskiej, rodzaju urządzeń, za pomocą których dziecko łączy się z Internetem lub też widoczności jego ekranu dla innych domowników. Dąży również do odizolowania dziecka od otoczenia. Wykorzystując wiedzę na temat problemów rodzinnych oraz techniki manipulacji, może stawiać w złym świetle rodziców małoletniego.

---

[42] M. Dąbrowska, *Grooming - wybrane aspekty prawnokarne i kryminologiczne,* Warszawa 2018, s. 81

[43] J. Carr, *Internet a wykorzystywanie seksualne dzieci i pornografia dziecięca, "*Dziecko krzywdzone" nr 13, Warszawa 2005, s. 15

Znajomość od tego momentu nabiera bardziej intymnego charakteru. Pozwala to na przekroczenie kolejnej granicy i poruszanie tematów związanych z seksualnością dziecka. Choć może ono odczuwać zażenowanie lub wstyd, silna więź ze sprawcą wywołuje również ciekawość i podekscytowanie. Dziecko godzi się na przekraczanie kolejnych granic, ponieważ nie chce stracić atrakcyjnego przyjaciela. Tego rodzaju rozmowy osłabiają zahamowania i doprowadzają do większej podatności na propozycje dotyczące życia seksualnego. W momencie, gdy sprawca uzna, że stworzona więź emocjonalna jest już wystarczająco silna, następuje propozycja spotkania[44].

Niektórzy sprawcy znacząco skracają czas poświęcany na uwodzenie dziecka, próbując jak najszybciej przejść do etapu z użyciem przemocy celem uzyskania pożądanego przez siebie efektu. Może być to spotkanie z ofiarą lub otrzymanie nagich fotografii. Z kolei inni z różnych względów nie doprowadzają do spotkań w świecie rzeczywistym, a swoje działania ograniczają do formy cyberseksu. Polega to na prowadzeniu wulgarnych rozmów o tematyce seksualnej, którym towarzyszyć może masturbacja przy zastosowaniu kamer internetowych, przesyłanie filmów pornograficznych lub zdjęć ze swoim udziałem. Choć nie dochodzi w tym przypadku do fizycznego spotkania, skutki takich działań mogą być bardzo poważne. Działa to bowiem na psychikę dziecka w sposób destrukcyjny[45].

2.4. Hacking

Hackerem określa się osobę, która dokonuje włamania do systemów komputerowych poprzez pokonanie zabezpieczeń broniących dostępu do zgromadzonych tam informacji. Samo uzyskanie dostępu do systemu komputerowego stanowi bezpośredni zamach na bezpieczeństwo elektronicznie przetwarzanej informacji. Z kolei skuteczne przeprowadzenie takiego zamachu, które skutkuje przejęciem kontroli nad komputerem, daje sprawcy możliwość popełniania innych przestępstw, skierowanym przeciwko różnym dobrom prawnym[46].

[44] M. Dąbrowska, *Grooming - wybrane aspekty prawnokarne i kryminologiczne,* Warszawa 2018, s. 88
[45] Tamże
[46] A. Adamski, *Przestępczość w cyberprzestrzeni*, *Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy, Toruń 2001* s.19

Dostęp do komputera lub systemu może zostać uzyskany zarówno poprzez zalogowanie się do cudzego komputera lub sieci przez fizyczną interakcję lub wykorzystanie połączenia zdalnego. Sprawcy dysponują szeregiem różnorodnych technik, za pomocą których mogą dokonywać infiltracji systemów oraz sieci teleinformatycznych. Sama procedura jest zwykle wielostopniowa i rozpoczyna się od przeszukania konkretnego systemu pod kątem znalezienia ewentualnych luk i elementów podatnych na atak. W dalszym etapie rozpoczyna się działania, których celem jest dokonanie paraliżu prawidłowego funkcjonowania systemu. Zwykle wykorzystywane jest do tego specjalistyczne oprogramowanie[47].

Złośliwe oprogramowanie daje sprawcy możliwość uzyskania poufnych danych, w postaci nazw użytkowników, haseł, numerów kont bankowych, numerów PESEL, imion, nazwisk lub adresów zamieszkania. Jednocześnie dzięki wykorzystaniu błędów programistycznych doprowadzić można do przejęcia kontroli nad działaniem procesu wykonywanego przez oprogramowanie. Do instalacji oprogramowania dochodzi zwykle w wyniku podstępu, w ramach którego użytkownik nakłaniany jest do wykonania tej czynności. Wykorzystywane są także wirusy komputerowe[48].

Najbardziej popularnym sposobem zabezpieczenia danych oraz dostępu do systemu jest wymóg potwierdzenia własnej tożsamości przy zastosowaniu loginu oraz hasła. Wykorzystywane są także karty chipowe lub dane biometryczne. Jeśli hasła są przesyłane siecią, wówczas sprawca uzyskuje możliwość jego przejęcia za pomocą tak zwanych snifferów, czyli programów lub urządzeń przeznaczonych do przechwytywania oraz lokalizowania danych przepływających w sieci[49].

Najprostszym sposobem pokonywania zabezpieczeń jest stosowanie metody siłowej, polegającej na próbie wprowadzania kolejnych kombinacji hasła w celu jego odgadnięcia. Znajduje on zastosowanie w sytuacji, jeśli hacker zna swoją ofiarę i jest w posiadaniu danych, które mogą być wykorzystane przy konstruowaniu hasła. Istnieją również dedykowane do tego celu rozwiązania programowe, które wyręczają sprawcę w procesie wpisywania kolejnych kombinacji znaków. Działanie nazywane jest atakiem słownikowym. W przypadku skomplikowanych systemów zabezpieczeń, wymagany jest bardziej złożony program do łamania haseł[50].

---

[47] M. Siwicki, *Cyberprzestępczość,* Warszawa 2013, s. 96
[48] Tamże
[49] F. Radoniewicz, *Hacking w kodeksie karnym - wybrane zagadnienia techniczne i karne, "*Przestępczość teleinformatyczna 2020", Gdynia 2021, s. 182
[50] Tamże, s. 183

Działalność hackerów nie ogranicza się wyłącznie do przełamywania zabezpieczeń, ale związana jest również z ich omijaniem. W tym celu oprócz środków technicznych, korzystają oni także między innymi z socjotechniki. Wiąże się to z uzyskiwaniem poufnych informacji poprzez wchodzenie w odpowiednie interakcje z innymi osobami. Kluczowym czynnikiem nie jest oprogramowanie lub sprzęt informatyczny, ale wykorzystanie ludzkich słabości, zdobycie zaufania, wykorzystanie beztroski, braku uwagi lub też skorzystanie z podstępu. Wszystkie te elementy służą wyłudzeniu haseł od uprawnionych osób[51].

Ryc. 10. Siedziba NASA.
Źródło: https://www.komputerswiat.pl/artykuly/redakcyjne/najwieksze-ataki-hakerskie-ostatnich-lat-o-tych-zdarzeniach-mowil-caly-swiat/khfnngd#slajd-7 [dostęp w dniu 26.09.2023 r.]

Na przestrzeni lat dochodziło do wielu ataków hackerskich, których ofiarami padały osoby prywatne, przedsiębiorstwa, ogromne korporacje oraz instytucje rządowe. W 1999 r. 16-letni wtedy haker o nicku cOmrade uzyskał dostęp do sieci komputerowej wykorzystywanej przez Agencję Redukcji Zagrożeń Obronnych (DTRA). Jego backdory pozwoliły na pobranie ponad 3 tys. wiadomości, a także przejęcie da-

[51] Tamże, s. 184

nych logowania co najmniej 19 pracowników. W podobnym okresie ten sam haker znalazł sposób na połączenie z 13 komputerami NASA w Marshall Space Flight Center w Huntsville w stanie Alabama. Dzięki temu był w stanie pobrać dokumenty i oprogramowanie do obsługi fizycznego środowiska Międzynarodowej Stacji Kosmicznej. Po tym wydarzeniu NASA musiała zawiesić całą działalność na 21 dni.

Ryc. 11. Hotel Marriot.
Źródło: https://www.komputerswiat.pl/artykuly/redakcyjne/najwieksze-ataki-hakerskie-ostatnich-lat-o-tych-zdarzeniach-mowil-caly-swiat/khfnngd#slajd-7 [dostęp w dniu 26.09.2023 r.]

W 2014 r. hakerzy dostali się do serwerów sieci Marriott, wykradając informacje o kartach kredytowych należących do siedmiu milionów brytyjskich klientów. Dane te zostały przez nich odszyfrowane ze względu na fakt, że klucze deszyfrujące były przechowywane na dokładnie tym samym serwerze, włącznie z numerami paszportów. Podobny problem pojawił się też w 2016 r. w przypadku sieci Starwood Hotels, przejętych przez Marriotta. Najgorsze jest w tym jednak to, że wiadomość o wycieku pojawiła się dopiero w 2018 r., więc aż przez cztery lata klienci hotelu byli narażeni na utratę środków.

W 2016 r. hakerzy przeprowadzili zmasowany atak na serwery Ubera, skąd wykradli dane aż 57 mln użytkowników platformy oraz samych kierowców. Sprawa wyszła na jaw dopiero w 2022 r., co sprowadziło na nią gigantyczną falę krytyki. Przedstawiciele Ubera przyznali równocześnie, że przekazali hakerom 100 tys. dol. okupu, by ci usunęli ransomware, a sprawa nie została upubliczniona[52].

2.5. Cyberstalking

Rozwój technologii informacyjno-komunikacyjnej przyczynił się do znaczącego rozszerzenia możliwości związanych z życiem we współczesnym społeczeństwie. Jednak aktywność odbiorców i swoboda działania doprowadziła również do powstania nowych form patologii. Sprzyja temu przede wszystkim poczucie anonimowości.

Stalking definiowany jest jako wrogie, złośliwe i powtarzalne śledzenie oraz prześladowanie innej osoby, które zagraża jej bezpieczeństwu lub życiu. Rozwój technologiczny doprowadził do pojawienia się nowego pojęcia - cyberstalkingu. Może ono przybierać różne formy przestępstw, które skierowane są zarówno przeciw człowiekowi, jak i jego sprzętowi komputerowemu[53].

Cyberprzemoc należy do jednego z poważniejszych oraz bardziej powszechnych zagrożeń, z którymi obecnie mogą zetknąć się osoby korzystające z Internetu. Może ona przybierać rozmaite formy, do których zaliczają się między innymi:

- wojna na obelgi - publiczna, agresywna i zwykle pełna wulgaryzmów wymiana zdań pomiędzy użytkownikami. Ze zjawiskiem często można spotkać się na forach dyskusyjnych,
- prześladowanie - regularne przesyłanie do ofiary agresywnych lub ośmieszających treści,
- oczernianie - przesyłanie przez sprawcę informacji, których celem jest zniszczenie reputacji ofiary lub jej dobrych relacji z innymi osobami,
- prowokowanie lub atakowanie osoby, a następnie zarejestrowanie jej reakcji za pomocą filmów lub zdjęć, celem późniejszego upublicznienia takiego materiału w Internecie,

[52] https://www.komputerswiat.pl/artykuly/redakcyjne/najwieksze-ataki-hakerskie-ostatnich-lat-o-tych-zdarzeniach-mowil-caly-swiat/khfnngd#slajd-7 [12.09.2023 r.]
[53] M. Cyrklaff-Gorczyca, *Cyberstalking jako forma przemocy z wykorzystaniem technologii informacyjno-komunikacyjnych. Ekologia informacji a zasoby informacyjne w bibliotekach i cyberprzestrzeni*, Słupsk 2017, s. 204

- wykluczenie - celowe usunięcie konkretnej osoby z listy kontaktów lub grup dyskusyjnych,
- agresja techniczna - skupiona przeciwko bezpieczeństwu sprzętu elektronicznego. Zaliczają się do niej ataki przy użyciu złośliwego oprogramowania lub też wysyłanie dużej liczby wiadomości e-mail,
- cyberstalking - inwigilacja ofiary drogą elektroniczną oraz nękanie jej niechcianymi komunikatami, szykanami lub groźbami o charakterze prześladowczym[54].

Na rozwój wirtualnych form stalkingu wpływa wiele elementów. To głównie anonimowość, możliwość ciągłego oddziaływania oraz łatwość atakowania ofiar. Pojawia się w tym przypadku także efekt niewidzialnej publiczności, czyli potencjalnie nieograniczonej liczby osób, która uzyskuje dostęp do udostępnionego przez sprawcę materiału, mogącego zawstydzić lub obrazić ofiarę[55].

Przejawem cyberstalkingu będzie:

- wysyłanie obraźliwych wiadomości e-mail,
- przesyłanie wyraźnych gróźb lub obraźliwych komentarzy lub umieszczanie ich na forach i grupach dyskusyjnych,
- zachęcanie innych użytkowników do prześladowania lub zniewagi określonej osoby,
- próby monitorowania czyiś działań za pomocą instalacji oprogramowania śledzącego,
- próba uzyskania dostępu do poufnych informacji, które zgromadzone zostały na czyimś komputerze,
- poszukiwanie w Internecie różnego rodzaju informacji o osobie, mogących zażenować lub publicznie ośmieszyć ofiarę, a także zepsuć jej kontakty rodzinne, zawodowe i towarzyskie[56].

[54] M. Cyrklaff-Gorczyca, *Cyberstalking jako forma przemocy z wykorzystaniem technologii informacyjno-komunikacyjnych. Ekologia informacji a zasoby informacyjne w bibliotekach i cyberprzestrzeni*, Słupsk 2017, s. 203
[55] Tamże
[56] Tamże, s. 205-206

Nie należy wychodzić z założenia, iż cyberstalking nie stanowi tak realnego zagrożenia jak tradycyjna forma uporczywego nękania. Choć prześladowanie rozpoczyna się w świecie wirtualnym, jego następstwa i skutki odczuwane są przez ofiarę w świecie rzeczywistym.

Cyberstalking należy do jednej z najbardziej eskalujących form przemocy, do której dochodzi przy wykorzystaniu nowoczesnych technologii. Narażona jest między innymi młodzież, która publikuje za pomocą mediów społecznościowych bardzo osobiste informacje na swój temat. Potencjalny cyberstalker wchodząc w ich posiadanie może rozpocząć proces prześladowania. Tak naprawdę narażona może być jednak każda osoba posiadająca dostęp do Internetu, tak samo jak każda z tych osób może stać się sprawcą. Dlatego warto przygotować się do krytycznego wykorzystania technologii informacyjno-komunikacyjnych. Oprócz niewątpliwych korzyści, które niesie ze sobą korzystanie z Internetu, trzeba także pamiętać o wielu zagrożeniach z tym związanych.

2.6. Skimming

Skimmingiem w ścisłym znaczeniu jest skopiowanie paska magnetycznego oryginalnej karty płatniczej. Całe działanie odbywa się poprzez odczytanie przez głowicę elektromagnetyczną danych z drugiej ścieżki paska magnetycznego w momencie, gdy karta zostanie przesunięta po głowicy skimmera. Następuje wzmocnienie i przetworzenie informacji z postaci analogicznej na cyfrową. Kolejnym krokiem będzie zakodowanie odczytanych danych do postaci właściwej użytkowanemu skimmerowi oraz zarchiwizowanie zapisów w pamięci elektronicznej urządzenia[57].

Celem i ostatecznym efektem tego rodzaju działania jest uzyskanie fałszywej karty płatniczej. Bezprawne skopiowanie informacji z paska magnetycznego oraz przechwycenie przypisanego karcie kodu PIN, pozwala w konsekwencji na wykonanie duplikatu służącego do obciążenia rachunku bankowego jego posiadacza[58]. W najszerszym ujęciu skimming nie ogranicza się do skopiowania paska magnetycznego i przechwycenia PIN-u, ale wiąże się także z przetwarzaniem tych informacji.

[57] K. Mikołajczyk, *Przestępstwa związane z wykorzystaniem bankowości elektronicznej - skimming,* Przegląd Bezpieczeństwa Wewnętrznego 2014, nr 10, s. 104
[58] P. Opitek, *Skimming - aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej,* Warszawa 2017, s. 64

Biorąc pod uwagę zakres uzyskanych danych wyróżnić można:

- skimming pośredni - skimming paska magnetyczne,
- skimming pełny[59].

W pierwszym przypadku skimming dostarczy wyłącznie danych, które zapisane zostały na nośniku magnetycznym. Najczęściej dochodzi do tego w przypadku dokonywania płatności w sklepie. Sprzedawca, oprócz przeciągnięcia karty przez czytnik, przesuwa ją również przez skimmer, dzięki czemu w pamięci urządzenia zapisane zostają zgromadzone na pasku informacje.

W przypadku skimmingu pełnego, drugie urządzenie w postaci kamery lub spreparowanej klawiatury rejestruje przypisane do karty PIN-y. Doprowadza to do bardzo niebezpiecznej sytuacji, bowiem sprawca wchodzi w posiadanie danych zgromadzonych na pasku oraz kodów autoryzacyjnych pozwalających na przykład pobrać pieniądze z bankomatu[60].

Do zdarzenia może dojść w rozmaitych sytuacjach, biorąc pod uwagę chociażby miejsce zamontowania nakładki do kopiowania danych. Mamy więc do czynienia ze skimmingiem:

- bankomatowym,
- w terminalach POS na terenie punktów handlowo-usługowych,
- w innych terminalach płatniczych, na przykład służących do zapłaty za miejsce parkingowe lub do zakupu biletu kolejowego,
- w sytuacjach, w których sprawca skanuje kartę pozostawioną przez właściciela w miejscu uznanym przez niego za bezpieczne[61].

Najbardziej typowy i najczęściej spotykany jest jednak skimming bankomatowy, który oparty jest na montażu czytnika oraz układu filmującego w celu przejęcia kodu PIN oraz danych zgromadzonych na ścieżce magnetycznej[62]. Urządzenia potrafią być bardzo dobrze zakamuflowane. Tradycyjny skimmer dostępny jest w formie nakładki, która montowana jest na slot służący do wkładania karty bankomatowej.

---

[59] Tamże

[60] P. Opitek, *Skimming - aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej,* Warszawa 2017,, s. 65

[61] Tamże

[62] K. Mikołajczyk, *Przestępstwa związane z wykorzystaniem bankowości elektronicznej - skimming, "*Przegląd Bezpieczeństwa Wewnętrznego", nr 10, 2014, s. 108

Celem przestępstwa jest wykorzystanie faktu użycia karty w maszynie dla zdobycia wrażliwych informacji. Dla sprawcy najważniejsze jest, aby karta została przeciągnięcia przez czytnik oraz został wpisany kod PIN. Dane zostają skopiowane przez skimmer, natomiast PIN uzyskany zostanie za pomocą zastosowania fałszywej nakładki na klawiaturę lub zakamuflowanej kamery. Przestępcy muszą również dokonać montażu wszystkich spreparowanych części, które swym wyglądem wpisują się w konkretne urządzenie, dokonywać cyklicznej kontroli ich prawidłowego funkcjonowania oraz finalnie zdemontować całe oprzyrządowanie[63].

Rozwój skimmingu wiąże się z kilkoma aspektami, do których zaliczyć można:

- łatwość w obsłudze,
- zaawansowana technologia wykorzystywana przez sprawców,
- anonimowość sprawcy,
- nieświadomość ofiary,
- krótki czas potrzebny do popełnienia przestępstwa,
- stosunkowo niskie koszty finansowe ponoszone przez sprawców,
- międzynarodowy zasięg[64].

Ryc. 12. Nakładka na klawiaturę bankomatową.

Źródło: https://praga-polnoc.policja.gov.pl/r6/aktualnosci/56954,Skimming-bankomatowy-czym-jest-i-jak-sie-przed-nim-chronic.html [dostęp w dniu 12.09.2023 r.]

[63] P. Opitek, *Skimming - aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej,* Warszawa 2017, s. 66
[64] Tamże, s. 77

Ryc. 13. Skimmer w postaci nakładki na slot bankomatu.
Źródło: https://sekurak.pl/wp-content/uploads/2013/03/skimmer01.jpg [dostęp w dniu 12.09.2023 r.]

Rola wykorzystania kart płatniczych w dzisiejszym świecie jest nie do przecenienia. Bankowość elektroniczna i system obsługi płatności bezgotówkowych zwiększył zasięg i dostępność pieniądza na rynku. To jeden z najprężniej rozwijających się sektorów usług finansowych. Ta rewolucja technologiczna niesie jednak ze sobą pewne zagrożenia. Funkcjonowanie płatności bezstykowych jest dla przestępców okazją do nieuprawnionego przechwycenia danych[65].

[65] P. Opitek, *Skimming - aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej,* Warszawa 2017, s. 9-10

Rozdział III

Zapobieganie i zwalczanie cyberprzestępczości

3.1. Zapobieganie cyberprzestępczości

Zapobieganie zjawisku cyberprzestępczości nie ogranicza się wyłącznie do wprowadzania odpowiednich przepisów prawa. Do eliminacji tego rodzaju zachowań przestępczych konieczne staje się redukowanie ryzyka popełniania nadużyć. Dużą rolę odgrywa w tym przypadku właściwa współpraca z dostawcami usług internetowych oraz z samymi użytkownikami[66].

Ochrona systemów komputerowych oraz przetwarzanych za ich pomocą informacji to specjalność zabezpieczeń techniczno-organizacyjnych. Doskonalenie stosowanych metod i procedur technicznych, których celem jest ochrona przetwarzanych informacji, sprowadza się głównie do tworzenia zabezpieczeń wykorzystywanych w systemach operacyjnych. Działają one na zasadzie kontroli dostępu. Dodatkowo wykorzystuje się rozwiązania programowe, do których zaliczyć można między innymi oprogramowanie antywirusowe, antyspamowe, antyszpiegowskie lub też związane z identyfikacją i uwierzytelnianiem podmiotu uprawnionego[67].

Za skuteczny środek ochrony treści umieszczonych w Internecie uznawane są również metody kryptograficzne. To dzięki nim możliwa staje się ochrona poufności i autentyczności informacji. Podejmuje się także inicjatywy, które dążą do blokowania lub ograniczenia dostępu do nielegalnych treści za pomocą wykorzystywania technologii filtrujących. Polega to na skanowaniu stron internetowych pod kątem występowania odpowiednich słów kluczowych, albo też określonych elementów ich budowy. Oprogramowanie filtrujące może zablokować dostęp do niepożądanych treści[68].

Ważnym aspektem wiążącym się z ochroną systemów komputerowych jest dobrowolny charakter. Wyłącznie w przypadku komputerów, na których przetwarzane są dane osobowe osób trzecich, administrator ma obowiązek ochrony poufności i integralności. Wynika to z międzynarodowych standardów dotyczących ochrony danych osobowych.

---

[66] I. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 35

[67] Tamże, s. 36

[68] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawnokarne*, Warszawa 2011, s. 279

Zapobieganie i zwalczanie zjawiska cyberprzestępczości musi opierać się na rozwijaniu współpracy pomiędzy organami ścigania, sektorem prywatnym, a także samymi użytkownikami.

Przepisy nie będą skuteczne, jeżeli użytkownicy nie będą świadomi zagrożeń, z którymi mogą się zetknąć. Należy więc przywiązywać dużą wagę do propagowania świadomego korzystania z sieci. W wielu krajach takie programy dedykowane są już dla najmłodszych użytkowników. Największą aktywnością w tym zakresie mogą pochwalić się różnego rodzaju organizacje pozarządowe, które organizują szkolenia dla dzieci oraz młodzieży. Wiele informacji znaleźć można między innymi na dedykowanych portalach, na których umieszczone zostają materiały o nowych rodzajach zagrożeń[69].

Należy podejmować działania o charakterze ponadnarodowym, które muszą przyjąć formę stałej kooperacji. Tylko w taki sposób będzie można tworzyć nowe rozwiązania, przynoszące oczekiwane efekty. Rolą państwa jest zagwarantowanie bezpieczeństwa wszystkich podmiotów również w cyberprzestrzeni. Pojawia się konieczność nieustannego rozwijania potencjału ochronnego w zakresie działań, które mają na celu ochronę bezpieczeństwa cybernetycznego. Działania te są niezwykle ważne oraz powinny być prowadzone na liczniejszą skalę z powodu coraz większego upowszechnienia się Internetu i nowoczesnych rozwiązań technologicznych. Pojawiają się bowiem zupełnie nowe zagrożenia, które obok cyberprzestępczości przybierają także formy cyberterroryzmu, cyberszpiegostwa lub cyberkonfliktów. Każde z tych zagrożeń może przyczynić się do destabilizacji społeczeństwa[70].

Model walki z cyberprzestępczością powinien być oparty na trzech fazach:

1. Prowadzenie śledztwa sieciowego - pozwalającego określić czy doszło do popełnienia przestępstwa. W ramach czynności należy określić motywy działania sprawcy, zabezpieczyć dowody oraz zidentyfikować miejsce przestępstwa i samą osobę, która jest podejrzewana o jego popełnienie,
2. Tradycyjne działania w fizycznym miejscu - zebranie śladów cyfrowych oraz jeśli istnieje tak możliwość, zatrzymanie osoby podejrzanej,

[69] I. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 39

[70] K. Bakalarczyk-Burakowska, Z. Ciekanowski, *Cyberprzestępczość jako współczesne zagrożenie*, [w:] *Edukacja dla bezpieczeństwa,* Poznań 2019, s. 164

3. Analiza dowodów - odtworzenie przebiegu przestępstwa, a także wskazanie wykorzystanych do jego popełnienia narzędzi i współsprawców[71].

Prezentowany schemat znajdzie jednak zastosowanie w przypadku prostych zdarzeń o niskim stopniu złożoności, bowiem często ataków dokonują sprawcy posiadający dużą wiedzę i dostęp do zaawansowanych technologii. W efekcie doskonale potrafią ochronić i zabezpieczyć swoją tożsamość, co w wielu przypadkach utrudnia przeprowadzenie śledztwa[72].

3.2. Rola i podział dowodów elektronicznych

Zrozumienie znaczenia dowodu elektronicznego pozwala uzupełnić obraz zjawiska cyberprzestępczości, a także wskazać, z jakimi wyzwaniami wiąże się podejmowanie czynności procesowych, które nakierowane są na wykrycie czynu bezprawnego popełnionego w cyberprzestrzeni[73].

Dowód elektroniczny rozumiany jest jako informacja w formie elektronicznej o znaczeniu dowodowym[74] lub też dane stanowiące materiał dowodowy w sprawach o przestępstwa, które popełnione zostały z wykorzystaniem technologii informacyjnych[75].

Dane w szerokim ujęciu pojmowane są jako wszelkie przejawy rzeczywistości, które mogą być przetwarzane maszynowo lub umysłowo[76]. Mogą być to także zbiory liczb oraz tekstów, wykonanych w różnych formach. Dane po poddaniu ich odpowiedniemu przetworzeniu, mogą stanowić materiał do budowy informacji. Jednocześnie zarówno w języku informatycznym, jak i prawnym, można spotkać się z definicją danych komputerowych. Oznaczają one przedstawienie informacji, pojęć lub faktów w taki sposób, by były one możliwe do przetwarzania za pomocą systemów informa-

[71] K. Bakalarczyk-Burakowska, Z. Ciekanowski, *Cyberprzestępczość jako współczesne zagrożenie*, [w:] *Edukacja dla bezpieczeństwa,* Poznań 2019, s. 166
[72] J. Kosiński, *Paradygmaty Cyberprzestępczości*, Warszawa, 2015, s. 214
[73] B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Kraków 2000, s. 113.
[74] A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 28
[75] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s.192
[76] J. Wasilewski, *Cyberprzestępczość - wybrane aspekty prawnokarne i kryminalistyczne,* Białystok 2017, s. 297

tycznych, włącznie z programem umożliwiającym wykonanie odpowiedniej funkcji przez system informatyczny[77].

Dowód elektroniczny funkcjonuje z pojęciami, które określić można jako szeroko rozumiane ślady popełniania cyberprzestępstw. Ślady te (dowód elektroniczny) to wszelkie materiały, które występują w formie elektronicznej. W swym najprostszym ujęciu elektroniczne ślady popełniania cyberprzestępstw opierają się zatem na ruchu impulsów elektrycznych w układzie elektronicznym zawierającym elementy aktywne i pasywne[78].

Z kolei dowód cyfrowy zawęża się wyłącznie do dowodów elektronicznych, które występują w postaci cyfrowej. W praktyce występuje w formie liczb binarnych. Zabezpieczona kopia pliku komputerowego mieści się zatem w obydwu wskazanych kategoriach. Natomiast nagranie z kamer analogowych, pomimo faktu, iż zaliczane jest do materiałów cyfrowych, przyjmuje postać analogową, a nie cyfrową[79].

Dowód komputerowy łączy się natomiast nie tyle z formą potencjalnego dowodu, a określonym rodzajem urządzenia źródłowego, którym w tym przypadku jest komputer. Urządzenie to jednak zaliczane jest do kategorii sprzętu elektronicznego oraz cyfrowego. Z tego też powodu dowód komputerowy musi być jednocześnie dowodem elektronicznym i cyfrowym. Trudno zatem za dowód komputerowy uznać materiał zabezpieczony z telefonu komórkowego, pomimo tego, że funkcjonalność współczesnych smartfonów wcale nie odbiega od możliwości oferowanych przez nowoczesne komputery[80].

Pomimo różnic w pojęciach określających ślady popełniania cyberprzestępstw, to właśnie dowód elektroniczny w doktrynie prawnej stosowany jest najczęściej. Swym zakresem obejmuje bowiem bardzo szerokie spektrum materiałów.

Rola i znaczenie dowodów cyfrowych uzależnione są od ich właściwego zabezpieczenia. Praca systemów teleinformatycznych opiera się na przetwarzaniu danych. Żeby jednak mogło do tego dojść, konieczne staje się wykorzystanie odpowiednich nośników pamięci elektronicznej, które pozwalają na chwilowe lub trwałe przechowywanie wszystkich operacji przeprowadzanych na konkretnych danych. Do zapisu stosowana jest między innymi pamięć podręczna procesora (cache), pa-

[77] J. Wasilewski, *Cyberprzestępczość - wybrane aspekty prawnokarne i kryminalistyczne,* Białystok 2017, s. 297
[78] Tamże s. 303
[79] Tamże
[80] Tamże s. 304

mięć operacyjna systemu (RAM), pamięć wykorzystywana w układach graficznych, pamięć dysków twardych, pamięci półprzewodnikowych lub nośników optycznych.

Poszczególne rodzaje pamięci, z uwagi na budowę oraz charakterystykę działania, zaliczają się do ulotnych lub nieulotnych. W pamięci ulotnej dane przechowywane są tymczasowo i znikają wraz z wyłączeniem komputera. Na nośnikach wyposażonych w pamięć nieulotną, dane usuwane są z woli użytkownika systemu. Uzyskuje się także możliwość tymczasowego odczytu nawet wcześniej usuniętych danych, co może stanowić podstawę uzyskania potencjalnego materiału dowodowego[81].

Sytuacja prezentuje się zupełnie odmiennie w przypadku danych przekazywanych podczas transmisji poprzez sieci teleinformatyczne. Przekazywane są one bowiem pomiędzy poszczególnymi węzłami nie w postaci zapisu na nośniku, a w formie impulsów lub fal elektromagnetycznych w ramach zestawionego połączenia sieciowego. Nośnikiem jest więc łącze sieciowe, które może przybrać formę infrastruktury kablowej lub radiowej. Nie dają one jednak możliwości przechowywania danych, a wyłącznie stanowią drogę do ich transmisji. Łączą kolejne węzły sieci, czyli serwery, które są zaopatrzone w rozmaite rodzaje pamięci elektronicznych umożliwiających przetwarzanie i dalsze przekazywanie danych. Finalnie zatem wszystkie przetwarzane w systemach dane, muszą być transmitowane przy wykorzystaniu różnego rodzaju nośników pamięci[82].

Dowody elektroniczne mogą się składać z materiałów różniących się od siebie z uwagi na prezentowane treści. Zaliczają się do nich:

1) dowody zawierające tekst - dokumenty elektroniczne sporządzone w formie pisemnej, które najczęściej zapisane zostały w plikach z rozszerzeniem .doc, .pdf lub .txt,
2) dowody zawierające obrazy - mogą one składać się z zapisów zdjęć, filmów lub nagrań z kamer. Do najczęściej wykorzystywanych formatów zaliczyć można rozszerzenie .jpg, .gif, .avi, .mpg,
3) dowody zawierające zapis dźwięku - nagrania audialne, które mogą być zapisane jako dane cyfrowe lub analogowe. W szczególności mogą być to pliki o rozszerzeniu .wav lub .mp3,

[81] J. Wasilewski, *Cyberprzestępczość - wybrane aspekty prawnokarne i kryminalistyczne,* Białystok 2017, s. 306
[82] Tamże, s. 307

4) dowody zawierające dane o pracy systemu - są to logi lub zapisy audytowe, które umożliwiają odtworzenie historii pracy systemu. W rezultacie pozwala to na odtworzenie *modus operandi* sprawcy ataku. Wiele informacji na temat aktywności użytkownika w ramach korzystania z różnych usług sieciowych dają również pliki cookies,
5) dowody zawierające dane tworzące kod maszynowy oprogramowania – to skomplikowane pliki programów, które są całkowicie nieczytelne dla człowieka. Wykonywane są one wyłącznie przez przystosowane do tego urządzenia, czyli na przykład komputer z odpowiednim systemem operacyjnym[83].

Biorąc pod uwagę kryterium powstania zapisu, dowody elektroniczne można podzielić na:

1) dowody elektroniczne pierwotne,
2) dowody zdigitalizowane[84].

Dowody elektroniczne pierwotne oznaczają materiały, które oryginalnie zostały wytworzone w wersji elektronicznej. Są to więc w szczególności dane zapisane w plikach komputerowych lub nagrania audiowizualne. Z kolei dowody zdigitalizowane swoją elektroniczną formę uzyskały wtórnie. Do tej kategorii zaliczyć można zeskanowany dokument[85].

Ostatni podział dowodów elektronicznych uwzględnia kryterium źródła, z którego materiał dowodowy został pozyskany. Wyodrębnione zostały:

1) dowody elektroniczne przechwycone w czasie transmisji, zebrane w ramach kontroli operacyjnej lub podsłuchu procesowego,
2) dowody elektroniczne tworzone przez dane zapisane lokalnie na informatycznych nośnikach danych[86].

Wszystkie dane pojawiające się w obszarze cyberprzestrzeni w początkowej fazie wytwarzane są lokalnie. Przedstawione kryterium zwraca wobec tego uwagę na miejsce, z którego mogąca stanowić dowód porcja danych została pobrana.

---

[83] J. Wasilewski, *Cyberprzestępczość - wybrane aspekty prawnokarne i kryminalistyczne,* Białystok 2017, s. 311-312
[84] A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 37
[85] J. Wasilewski, *Cyberprzestępczość...*, s. 317
[86] Tamże, s. 318

Materiał dowodowy w postaci elektronicznej można spotkać właściwie w każdym miejscu, w którym odbywa się ludzka aktywność[87]. Wszystko za sprawą nieustannie postępującego procesu cyfryzacji. Coraz trudniej wykonywać codzienne zadania bez wykorzystania urządzeń elektronicznych, zestawiania połączeń głosowych, obsługi poczty elektronicznej, dokonywania transakcji z wykorzystaniem kart płatniczych lub korzystania z najróżniejszych aplikacji. Charakteryzując dowody elektroniczne nie można zatem ograniczać się wyłącznie do materiałów, które zapisane zostały na nośnikach danych lub komputerach.

Dane komputerowe mogą być przetwarzane lokalnie lub w szeroko rozumianej cyberprzestrzeni o potencjalnie globalnym zasięgu. Źródła odseparowane od cyberprzestrzeni wiążą się bezpośrednio z wszelkiego rodzaju pamięcią przenośną, która nie została podłączona do sieci lub też do urządzenia posiadającego czynne połączenie sieciowe. Z kolei szeroko rozumiane zasoby cyberprzestrzeni oznaczają materiały, które mogą być zlokalizowane w dowolnym typie pamięci systemów teleinformatycznych, funkcjonujących w sieci urządzeń cyfrowych, a przede wszystkim w sieci Internet. W tej kategorii źródeł dowodowych mieszczą się również urządzenia wykorzystywane do budowy infrastruktury sieciowej, takie jak routery, przełączniki lub centrale[88].

Istotą dowodu elektronicznego jest jego szczególna forma, która wyraża się w elektronicznym zapisie, przez co odczyt treści materiału nie jest możliwy bez zastosowania odpowiedniego urządzenia do przetwarzania informacji. Mogą one przybierać rozmaite formy w postaci zapisu plików tekstowych, multimedialnych, wiadomości pocztowych, historii ruchu sieciowego lub wpisów na forach i portalach społecznościowych. W celu ich pozyskania istnieje możliwość fizycznego zabezpieczenia danego nośnika wykorzystanego w systemie pracującym lokalnie lub w sieci, albo też w ramach zabezpieczenia materiałów przetwarzanych online[89].

[87] K. J. Pawelec, *Proces dowodzenia w postępowaniu karnym*, Warszawa 2010, s. 24
[88] J. Wasilewski, *Cyberprzestępczość...*, s. 326
[89] Tamże, s. 331

3.3. Zabezpieczanie dowodów elektronicznych

We współczesnym świecie coraz większego znaczenia w postępowaniach sądowych nabierają materiały pochodzące z urządzeń elektronicznych - komputerów osobistych, telefonów komórkowych, tabletów i innych. Może zaistnieć konieczność przedstawienia danych cyfrowych w charakterze dowodu rzeczowego. Procedura karna nie posługuje się osobną kategorią „dowodów elektronicznych" - są to więc również dowody rzeczowe, ale ze względu na swoją formę, mają one cechy szczególne. Dowodem cyfrowym nazwiemy każdą informację, występującą pod postacią danych w formie cyfrowej, która ma znaczenie dla postępowania karnego[90].

Do specyficznych cech danych w formie cyfrowej należy zaliczyć przede wszystkim:

- Łatwość dokonania zmiany danych (przypadkowo lub celowo); dane cyfrowe są łatwe do zmodyfikowania, niekiedy można tego dokonać w sposób niemożliwy do wykrycia. Wymagają więc szczególnej ostrożności przy ich zabezpieczaniu i analizie.
- Brak rzeczywistych różnic pomiędzy „kopią" a „oryginałem" danych; ponieważ dane cyfrowe zapisywane są za pomocą wartości binarnych (0 lub 1), to nie mają one indywidualnych cech identyfikacyjnych. Możliwe jest więc wykonanie wiernej i wiarygodnej kopii danych, która będzie identyczna z oryginałem[91].

Chcąc zabezpieczyć dane cyfrowe do ich wykorzystania w postępowaniu karnym, należy co do zasady wykonać ich wierną i uwierzytelnioną kopię. Obecne rozwiązania techniczne umożliwiają wykonanie tzw. kopii binarnej danych i jej uwierzytelnienie za pomocą tzw. sumy kontrolnej. Zabezpieczenia danych można dokonać na przykład w toku oględzin. Ze względu na łatwość modyfikacji danych cyfrowych, pod żadnym pozorem nie wolno korzystać ze sprzętu, na którym się znajdują. Należy bowiem zadbać o niezmienność materiału cyfrowego od momentu rozpoczęcia jego zabezpieczania (jeżeli bowiem dojdzie do zmiany w treści danych po tym, jak w ich posiadanie wejdą organy ścigania, a zmiany tej nie będzie się dało uzasadnić prawidłowymi i koniecznymi czynnościami, to możliwe będzie podważenie takiego dowodu). Z tego powodu najbezpieczniejszym sposobem zabezpieczenia np. danych

[90] http://dowody.karne.pl/cyfrowe.html [14.09.2023]
[91] Tamże

z dysku komputera jest wykonanie kopii binarnej całej jego zawartości, po wymontowaniu dysku z komputera i podłączeniu go do stacji roboczej z wykorzystaniem urządzenia blokującego zapis na tym dysku[92].

Z technicznego punktu widzenia nie ma potrzeby zabezpieczania sprzętu. Wykonanie uwiarygodnionej kopii binarnej danych gwarantuje, że dane znajdujące się na „kopii" będą w stu procentach odpowiadały zawartości oryginalnego nośnika. Nośnik danych (dysk twardy, pamięć przenośna, karty pamięci, płyty itp.) służy jedynie do przechowywania danych - a to one stanowią dowód. Z tej perspektywy, organy ścigania mają możliwość wykonania kopii dowodów „dla siebie" bez potrzeby fizycznego zabezpieczenia sprzętu użytkownika (co wiąże się z dużą uciążliwością dla niego). Praktyka postępowań karnych wskazuje jednak, że stosunkowo często zabezpieczany jest sprzęt w całości - organy ścigania są do tego uprawnione, pomimo iż teoretycznie nie jest to konieczne. Należy jednak podkreślić, że zdarzają się sytuacje, kiedy zabezpieczenie samego sprzętu jest jednak uzasadnione. Ma to miejsce szczególnie wtedy, gdy istnieje podejrzenie przechowywania materiałów, których posiadanie jest zabronione, a także gdy istnieje np. podejrzenie, że sprzęt pochodzi z kradzieży[93].

Wartość i moc dowodowa danych cyfrowych zależeć będzie od kilku elementów. Po pierwsze, istotna jest oczywiście treść danych - po bliższej analizie danych może okazać się, że po prostu nie zawierają one poszukiwanych informacji, lub że ich treść jest inna od oczekiwań. Po drugie, dowód cyfrowy musi być wiarygodnie zabezpieczony - koniecznie możliwe musi być wykazanie, że dane prezentowane w sądzie stanowią takie same dane, jak te, które posiadał użytkownik (np. podejrzany). Wiarygodność dowodu zapewnia się przez prawidłowe wykonanie kopii binarnej i jej uwierzytelnienie za pomocą sumy kontrolnej. Po trzecie, dowód cyfrowy musi być autentyczny - jego źródło pochodzenia musi być bezsporne. Odpowiednia dokumentacja w treści protokołów może umożliwić wykazanie, iż prezentowane w sądzie dane są w istocie tymi samymi, które zabezpieczono[94].

Dowody cyfrowe, co do zasady, wymagać będą sporządzenia opinii przez biegłego informatyka. Biegły musi zachować wszelkie zasady prawidłowego obchodzenia się z takim materiałem. Wszelkie analizy powinien przeprowadzać na osobnej

[92] http://dowody.karne.pl/cyfrowe.html [14.09.2023]
[93] Tamże
[94] Tamże

kopii danych (tak, by nie zmodyfikować danych wzorcowych). Każdorazowo kopię należy uwierzytelniać poprzez sumę kontrolną. Biegły powinien oczywiście prowadzić ścisłą dokumentację swoich czynności, wraz ze wskazaniem wykorzystanych do tego programów komputerowych itp. Prezentując swoją opinię powinien to zaś uczynić w sposób zrozumiały. Powinien unikać nadmiaru sformułowań technicznych, hermetycznego języka. Jego rolą jest przecież przedstawienie informacji, które odnalazł w przekazanych mu danych cyfrowych w taki sposób, aby możliwa była świadoma ocena tego dowodu przez sąd[95].

Dowody cyfrowe występują zwłaszcza w zdarzeniach, które można nazwać „przestępstwami komputerowymi". Istnieje wiele przestępstw, które można popełnić wyłącznie z użyciem komputera lub innego sprzętu elektronicznego. Wówczas zawsze konieczne będzie przedstawienie dowodów cyfrowych (np. w razie włamania do systemu informatycznego, uszkodzenia danych itp.). Istnieje też grupa przestępstw, których intuicyjnie nie można nazwać „komputerowymi", a jednak z punktu widzenia procesu karnego i kryminalistyki mogą one zawierać taki element. Na przykład gdy sprawa dotyczy wynoszenia dokumentów z miejsca pracy - może okazać się konieczna analiza danych w komputerze służbowym i prywatnym u podejrzanego[96].

3.4. Czynniki utrudniające ściganie przestępstw komputerowych

Przestępstwa komputerowa w bardzo dużym stopniu wpływają na życie i bezpieczeństwo społeczeństwa. Okazuje się, że tradycyjne metody śledcze nie zawsze są w pełni wystarczające do skutecznego ścigania oraz wykrywania sprawców cyberprzestępstw. Wymaga to bowiem aktywnej współpracy na szczeblu międzynarodowym, a także partnerstwa publiczno-prywatnego[97].

Wzrost zagrożenia cyberprzestępczością wiąże się między innymi z brakiem wystarczającej wiedzy na temat tego zjawiska oraz skutecznego oprogramowania pomocnego w jego wykryciu. Niewielkie szanse na ujawnienie sprawcy wywołują niechęć podmiotów pokrzywdzonych, które nie chcą informować Policji o zaistniałych

[95] http://dowody.karne.pl/cyfrowe.html [14.09.2023]
[96] Tamże
[97] I. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 31

zamachach. Ofiary przestępstw komputerowych lekceważą także środki bezpieczeństwa[98].

Ściganie utrudnione jest także przez niedopracowanie przepisów prawnych. Organy ścigania nie posiadają właściwego przygotowania do realizacji tego rodzaju spraw. Pojawiają się problemy z oceną dowodów, które posiadają formę elektroniczną. Z takim materiałem należy obchodzić się wyjątkowo ostrożnie, bowiem sprawca może go uszkodzić lub usunąć[99].

Przestępstwa popełniane przy wykorzystaniu Internetu cechuje ich transgraniczny charakter. Transfer danych może przebiegać przez terytorium różnych państw, co stawia ustawodawców przed wyjątkowo trudnym zadaniem.

Niezadowalająca jest również działalność prokuratury oraz sądów. Przekłada się na to zaawansowana technologicznie natura zjawiska cyberprzestępczości, niewystarczająca wiedza osób, które reprezentują wymiar sprawiedliwości na temat postępowania dowodowego z zakresu cyberprzestępczości. Trzeba jednak pamiętać o tym, że Internet nieustannie się rozwija, a zatem stwarza coraz to nowe możliwości podejmowania działań o charakterze przestępczym. Brak próby podejmowania działań zapobiegawczych, mających na celu ochronę sieci i systemów komputerowych, w konsekwencji przynieść może fatalne skutki[100].

Jednym z najistotniejszych problemów związanym z cyberprzestępczością jest automatyzacja. Choć niewątpliwie zwiększa ona w znaczący sposób szybkość funkcjonowania poszczególnych usług internetowych i zwalnia z konieczności stosowania dużej ilości kosztownej siły roboczej, wpływa również na zwiększenie skali działalności przestępnej. Cyberprzestępcy wpływają bowiem na automatyczne procesy korzystając z narzędzi hackerskich.

Problemem jest również:

1) brak lub zbyt mała liczba odpowiednich instrumentów i narzędzi, które pozwalają na skuteczne ściganie cyberprzestępców,
2) korzystanie z technologii kryptograficznych w celu ukrycia przestępczej działalności.
3) nieskuteczna ochrona systemów teleinformatycznych z uwagi na ich dużą liczbę oraz poddawanie nieustannym modyfikacjom,

[98] M. Siwicki, *Cyberprzestępczość,* Warszawa 2013, s. 77
[99] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 22-23
[100] M. Siwicki, *Cyberprzestępczość...*, s. 80

4) nieodpowiedni nadzór ze strony podmiotów odpowiedzialnych za świadczenie usług internetowych,
5) zwiększająca się liczba usług świadczonych za pomocą drogi elektronicznej[101].

Taki rodzaj przestępczości może przynosić sprawcom spore zyski, przy relatywnie niskim ryzyku pociągnięcia do odpowiedzialności karnej. Fakt ten dodatkowo zachęca do popełniania czynów karalnych. Wiele spółek oraz podmiotów gospodarczych nie zawiadamia również o przestępstwach w obawie o pogorszenie własnego wizerunku w wyniku upublicznienia stopnia ich narażenia na tego typu zagrożenia[102].

[101] Tamże, s. 79
[102] Tamże

Zakończenie

Cyberprzestępczość jest stosunkowo nową, jednak niezwykle dynamicznie rozwijającą się formą przestępczości. Praktycznie na terytorium większości państw znajdują się wyspecjalizowane komórki, których zadaniem stało się zapobieganie oraz ściganie tego zjawiska. Niestety rozwój technologiczny sprawia, że stosowane metody nie zawsze okazują się w pełni skuteczne. Główną przeszkodą okazuje się transgraniczny charakter cyberprzestępczości oraz losowość w wyborze ofiar.

Brak podjęcia odpowiednich działań, które będą miały na celu ochronę sieci i systemów komputerowych może okazać się katastrofalne w skutkach. Kluczową kwestią wydaje się być ścisła współpraca międzynarodowa w zakresie zwalczania cyberprzestępczości. Do realizacji tego celu pojawia się potrzeba przyjęcia jednorodnych środków karnych w przepisach prawa. Polskie przepisy, pomimo świadomości tego faktu, również nie są w pełni zgodne ze standardami opracowanymi przez organizacje podejmujące inicjatywy dotyczące zwalczania cyberprzestępczości. Pojawia się więc konieczność wprowadzenia kolejnych zmian do polskiego ustawodawstwa, aby mogły one w pełni odpowiadać standardom międzynarodowym.

Cyberprzestrzeń wymusza konieczność wypracowania zupełnie innych metod badawczych w odniesieniu do przestępstw popełnianych za pośrednictwem sieci teleinformatycznej. Rozwój technologiczny w znaczący sposób przyczynił się bowiem do powstania całkowicie nowych i wcześniej nieznanych metod i form działań bezprawnych. Systemy komputerowe mogą być wykorzystywane zarówno jako narzędzie służące do popełniania ataku, jak i cel ataku. Realizacja czynności procesowych zgodnie z obowiązującymi przepisami, skupia się na podejmowaniu działań konwencjonalnych, które wykonywane są fizycznie w otaczającej rzeczywistości. Nie znajduje to jednak przełożenia w przypadku pracy z zasobami cyberprzestrzeni. Dowody cyfrowe w postaci danych komputerowych nie posiadają swojej materialnej postaci. Pojawia się także potrzeba uregulowania kwestii związanych z określeniem zasad i metod prowadzenia czynności procesowych w obszarze domeny cyfrowej, takich jak przeszukanie systemu oraz zatrzymanie danych.

Ocena zjawiska pozwala również stwierdzić, że do skutecznej walki z problemem cyberprzestępczości wykorzystane muszą zostać także środki pozaprawne. Chodzi między innymi o określone standardy bezpieczeństwa, system samokontroli

oraz uświadamianie użytkowników Internetu na temat grożących im niebezpieczeństwom, które wiążą się z korzystaniem z sieci. Stworzenie określonych zasad postępowania jest procesem znacznie szybszym od wdrażania nowego ustawodawstwa, a jednocześnie wydaje się także rozwiązaniem zdecydowanie łatwiejszym i bardziej elastycznym. Profilaktyka i edukacja powinny być więc uzupełnieniem strategii podejmowanej przez państwo.

Problem związany z cyberprzestępczością staje się coraz bardziej powszechny. Same ataki charakteryzują się wysokim poziomem profesjonalizmu i coraz częściej dopuszczają się ich nie tylko pojedyncze osoby, a wyspecjalizowane grupy. Coraz większa liczba użytkowników Internetu bazuje na środowiskach opartych na chmurze, które posiadają ogromny potencjał, ale jednocześnie stanowią doskonałe miejsce do działań o charakterze przestępczym. Należy więc nieustannie poszukiwać nowych metod pozwalających na ograniczanie oraz zwalczanie tego zjawiska.

Nowym wyzwaniem może okazać się także sztuczna inteligencja, która odgrywa coraz większą rolę w rozwoju społecznym, poprawiając jednocześnie wydajność pracy oraz redukując jej koszty. Nie ulega jednak wątpliwości, że wspomniana technologia stwarza również pewne zagrożenie oraz stawia organy ścigania przed nowymi wyzwaniami. Wykorzystanie sztucznej inteligencji pozwala między innymi na generowanie treści cyfrowych, które tworzą fałszywą rzeczywistość. Wszystko to w konsekwencji wymusza konieczność wypracowania zupełnie nowych metod wykrywania i przeciwdziałania tego typu zdarzeniom.

Bibliografia

Publikacje zwarte, artykuły

- Adamski A., *Prawo karne komputerowe*, Warszawa 2000.
- Adamski A., *Cyberprzestępczość - aspekty prawne i kryminologiczne*, „Studia Prawnicze", Zeszyt 4 (166) 2005, Warszawa 2006.
- Bakalarczyk-Burakowska K., Ciekanowski Z., *Cyberprzestępczość jako współczesne zagrożenie*, [w:] *Edukacja dla bezpieczeństwa,* Poznań 2019.
- Balkowski R., *Bezpieczeństwo systemów teleinformatycznych - zmiany, trendy i zasady,* Warszawa 2018.
- Bienias T., *Internet*, Kraków 1998.
- Carr J., *Internet a wykorzystywanie seksualne dzieci i pornografia dziecięca,* „Dziecko krzywdzone" nr 13, Warszawa 2005.
- Cyrklaff-Gorczyca M., *Cyberstalking jako forma przemocy z wykorzystaniem technologii informacyjno-komunikacyjnych. Ekologia informacji a zasoby informacyjne w bibliotekach i cyberprzestrzeni*, Słupsk 2017.
- Dąbrowska M., *Grooming - wybrane aspekty prawnokarne i kryminologiczne,* Warszawa 2018.
- Fischer B., *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Kraków 2000.
- Hassan M., Raj J., *Wysoko wydajne sieci TCP/IP*, Gliwice 2004.
- Hofmolk J., *Internet jako nowe dobro wspólne*, Warszawa 2009.
- Jaroszewska I., *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017.
- Kosiński J., *Paradygmaty Cyberprzestępczości*, Warszawa, 2015.
- Kulesza J., *Międzynarodowe Prawo Internetu*, Poznań 2010.
- Lach A., *Dowody elektroniczne w procesie karnym*, Toruń 2004.
- Martellozo E., *Online Child SexualAbuse: Grooming, Policing and Child Protection in a Multi-Media World, Routledge*, New York 2012.
- Mikołajczyk K., *Przestępstwa związane z wykorzystaniem bankowości elektronicznej - skimming,* Przegląd Bezpieczeństwa Wewnętrznego 2014, nr 10.

- Opitek P., *Skimming - aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej,* Warszawa 2017.
- Pawelec K. J., *Proces dowodzenia w postępowaniu karnym*, Warszawa 2010.
- Radoniewicz F., *Hacking w kodeksie karnym - wybrane zagadnienia techniczne i karne, „*Przestępczość teleinformatyczna 2020", Gdynia 2021
- Siwicki M., *Cyberprzestępczość,* Warszawa 2013.
- Siwicki M., *Podział i definicja cyberprzestępstw,* Prokuratura i Prawo 7-8.
- Siwicki M, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawnokarne*, Warszawa 2011.
- Suchorzewska A., *Ochrona systemów informatycznych wobec zagrożeń cyberterroryzmem*, Warszawa 2010.
- Wasilewski J., *Cyberprzestępczość - wybrane aspekty prawnokarne i kryminalistyczne,* Białystok 2017.

Źródła internetowe

- https://www.benchmark.pl/aktualnosci/historia-rozwoju-komputerow-i laptopow .html#noop
- https://egzamin-e13.pl/projektowanie-lokalnych-sieci-komputerowych-2/warstwy-sieci-komputerowych-model-osi-i-tcpip/
- https://policja.pl/pol/aktualnosci/212455,Top-5-najczestszych-technik-phishingowych.html
- https://www.komputerswiat.pl/artykuly/redakcyjne/najwieksze-ataki-hakerskie-ostatnich-lat-o-tych-zdarzeniach-mowil-caly-swiat/khfnngd#slajd-7
- https://praga-polnoc.policja.gov.pl/r6/aktualnosci/56954,Skimming-bankomatowy-czym-jest-i-jak-sie-przed-nim-chronic.html
- https://sekurak.pl/wp-content/uploads/2013/03/skimmer01.jpg
- http://dowody.karne.pl/cyfrowe.html