Received: 8.01.2023
Accepted: 23.02.2023
Published: 31.03.2023

Roczniki Administracji i Prawa
Annuals of The Administration and Law
2023, XXIII, z. 1: s. 29-50
ISSN: 1644-9126
DOI: 10.5604/01.3001.0016.3776
https://rocznikiadministracjiiprawa.publisherspanel.com

Marcin Konieczny*
Nr ORCID: 0000-0002-1798-1509

CYBERPRZESTĘPCZOŚĆ – KRÓTKA HISTORIA, WSPÓŁCZESNE OBLICZA I TRUDNA DO PRZEWIDZENIA PRZYSZŁOŚĆ

CYBERCRIME – A SHORT HISTORY, CONTEMPORARY FACES AND AN UNPREDICTABLE FUTURE

Streszczenie: Celem opracowania jest analiza zjawiska nowej i szybko rozwijającej się przestępczości o transgranicznym charakterze: cyberprzestępczości, czyli przestępstw popełnianych przy użyciu komputerów oraz tej, której celem są komputery. Rolą niniejszego artykułu jest także zwrócenie uwagi na skalę zjawiska cyberprzestępczości, przywołanie rodzajów cyberprzestępczości oraz przybliżenie dostępnych narzędzi i strategii zabezpieczeń przed nią. W opracowaniu podjęto zagadnienie historii i rozwoju przestępczości komputerowej oraz związanych z nią zagrożeń. Zagadnienie omawiane jest w kontekście kluczowych zjawisk współczesnego świata, jakimi są cyberprzestrzeń i społeczeństwo informacyjne. W oparciu o dostępną literaturę przedmiotu autor omawia rodzaje cyberprzestępstw w kontekście czterech obszarów: zachowań społecznych i porządku prawnego, technologii oraz gospodarki. Artykuł opisuje najbardziej popularne narzędzia i metody stosowane przez cyberprzestępców, m.in. phishing, malware, hacking, cyberterroryzm i cyberstalking. Opracowanie dowodzi, że cyberprzestępczość obejmuje swoim zakresem szeroką gamę czynów zabronionych, poczynając od „typowych" przestępstw, jakie są popełniane z wykorzystaniem sieci informatycznych (na przykład włamania na konta bankowe lub kradzież tożsamości), poprzez przestępstwa przeciwko ochronie informacji (na przykład sabotaż komputerowy), aż po przestępstwa wieloaspektowe, jakimi są przede wszystkim złożone przestępstwa gospodarcze.

Słowa kluczowe: cyberprzestępczość, przestępstwa komputerowe, społeczeństwo informacyjne, cyberprzestrzeń, cyberbezpieczeństwo

* dr ppor; Wyższa Szkoła Policji w Szczytnie. Źródła finansowania publikacji: środki własne autora; e-mail: markon7788@gmail.com

Summary: The aim of the study is to analyze the phenomenon of new and rapidly growing cross-border crime: cybercrime, i.e. crimes committed with the use of computers and those aimed at computers. The role of this article is also to draw attention to the scale of the cybercrime phenomenon, to recall the types of cybercrime and to present the available tools and strategies for protecting against it. The study deals with the history and development of computer crime and related threats. The issue is discussed in the context of the key phenomena of the modern world, which are cyberspace and the information society. Based on the available literature on the subject, the author discusses the types of cybercrimes in the context of four areas: social behavior and the legal order, technology and economy. The article describes the most popular tools and methods used by cybercriminals, incl. phishing, malware, hacking, cyberterrorism, and cyberstalking. The study proves that cybercrime covers a wide range of offenses, ranging from "typical" crimes that are committed using IT networks (for example, hacking into bank accounts or identity theft), to crimes against information protection (for example computer sabotage) , to multi-faceted crepes, sucha as, above all, complex economic crimes.

Keywords: cybercrime, computer crime, information society, cyberspace, cybersecurity

WSTĘP

Gwałtowny rozwój techniki oraz nowoczesnej technologii, do którego doszło na przełomie XX i XXI wieku, doprowadził do powstania całkowicie nowych zjawisk, które ze względu na swoją społeczną szkodliwość i nierzadko również niebezpieczeństwo są ścigane jako wykroczenia lub przestępstwa. Jednym z tego typu zjawisk, całkowicie związanych z postępem technicznym w obszarze przetwarzania oraz przechowywania informacji, jest przestępczość popełniana przy pomocy nowoczesnych technologii teleinformatycznych, określana mianem cyberprzestępczości (przestępstwa komputerowego)[1]. Zanim jednak zostanie ona omówiona, konieczne jest jeszcze wskazanie, że od początku swojego istnienia Internet w bardzo dużym stopniu zmienił sposób postrzegania otaczającego nas świata, a jedną z ważniejszych zmian było zatarcie się granic pomiędzy poszczególnymi państwami, a także zniwelowanie barier językowych. W ten sposób świat stał się niejako mniejszy i bardziej dostępny dla każdego użytkownika Internetu. Warto podkreślić, że w sieci tego typu każdy jej użytkownik posiada jednakowe prawa, a także może stać się zarówno odbiorcą istotnych informacji, jak i ich twórcą dla innych osób[2].

Niniejszy artykuł analizuje zjawisko cyberprzestępczości z perspektywy jego stopniowej ewolucji. Opracowanie dowodzi, że wraz ze zjawiskiem rozwoju sieci internetowej, łatwości dostępu do niej i zwiększania się liczby internautów, zwiększać się będą skala i rodzaje przestępczości, a sposoby dokonywania przestępstw

[1] R. Jedlińska, *Problem przestępczości elektronicznej*, „Ekonomiczne Problemy Usług" 2017, nr 1, s. 185.
[2] M. Stefanowicz, *Cyberprzestępczość – próba diagnozy zjawiska*, „Kwartalnik Policyjny" 2017, s. 19.

w cyberprzestrzeni będą coraz bardziej kreatywne. Dlatego niezmiernie istotne jest podjęcie działań zmierzających do redukcji tego zjawiska przez organy ścigania, administrację publiczną i powszechną edukację.

SPOŁECZEŃSTWO INFORMACYJNE I CYBERPRZESTRZEŃ – PRÓBA ZDEFINIOWANIA POJĘCIA

Zanim jednak zostaną omówione podstawowe pojęcia związane z tematem niniejszego opracowania, niezbędne jest odniesienie się do istotnego z punktu widzenia rozwoju współczesnego świata pojęcia społeczeństwa informacyjnego oraz cyberprzestrzeni.

Odnosząc się do społeczeństwa informacyjnego, warto podkreślić, że również to pojęcie posiada w literaturze przedmiotu wiele definicji oraz znaczeń, przez co trudne jest jednoznaczne określenie tego terminu. Problem ten poruszał między innymi E. Bendyk: „Co to jest społeczeństwo informacyjne? Ideologiczny twór państwowych biurokratów czy precyzyjna etykieta opisująca stan społeczeństwa wskutek rozwoju zaawansowanych technologii? Ani jedno, ani drugie. Społeczeństwo informacyjne to puste stwierdzenie, które w warstwie ideologicznej się wyczerpało, jego wartość opisowa zaś jest równie mała”[3]. Natomiast B. Ney, analizując pojęcie społeczeństwa informacyjnego, zwrócił uwagę na dwie cechy, które mają podstawowe znaczenie w procesie definiowania tego pojęcia: „pierwsza to powszechny dostęp do informacji wypełniający zapis Konstytucji RP, że każdemu zapewnia się wolność pozyskiwania i rozpowszechniania informacji. Drugą cechą społeczeństwa informacyjnego jest taki poziom infrastruktury, który zapewnia racjonalne zaspokajanie potrzeb informacyjnych obywateli, podmiotów gospodarczych oraz instytucji, organizacji i władz publicznych. Ta cecha pełni służebną rolę wobec cechy pierwszej, a jednocześnie wskazuje na konieczność dysponowania technologiami informacyjnymi tak rozwiniętymi, aby można było zaspokajać potrzeby w zakresie informacji specjalistycznych”[4].

Pomijając kwestie wątpliwości, jakie towarzyszą procesowi wypracowania najbardziej szerokiego znaczenia idei społeczeństwa informacyjnego, nie sposób wręcz zaprzeczyć, że pojęcie to weszło na trwale do społecznej świadomości, a także jest opisywane i wykorzystywane przez wiele dziedzin naukowych – na przykład socjologii, psychologii i ekonomii. Z całą pewnością cechą wspólną wszystkich definicji, jakie opisują ten stan rozwoju ludzkiej społeczności, jest ich związek z przemianami, które dotyczą czterech obszarów – zachowań i świadomości ludzkiej, edukacji, technologii oraz gospodarki. W pierwszym z nich społeczeństwo informacyjne ma

[3] J.S. Nowak, *Społeczeństwo informacyjne – geneza i definicje*, [w:] P. Sienkiewicz, J.S. Nowak (red.), *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*, Katowice 2008, s. 34-35.

[4] B. Ney, *Geoinformacja w społeczeństwie informacyjnym*, „Roczniki Geomatyki” 2005, tom III, zeszyt 3, s. 13-14.

związek z przeobrażeniem postrzegania jednostki ludzkiej przez pryzmat informacji oraz zmian odnoszących się do samego charakteru relacji interpersonalnych. W odniesieniu do drugiego ze wskazanych obszarów dotyczy on poziomu wykształcenia oraz nasycenia różnych sfer życia pojedynczego człowieka i całych społeczeństw urządzeniami informacyjnymi oraz telekomunikacyjnymi. Natomiast trzeci z obszarów wskazuje na zorientowanie obrotu gospodarczego na elektroniczne media, które z kolei prowadzą do wypracowania e-gospodarki. Zagrożenie cyberprzestępczością w oczywisty sposób wpływa na wymienione obszary przemian[5].

Aby jak najlepiej zobrazować ideę społeczeństwa informacyjnego, warto przytoczyć niektóre ze wskaźników, które mają za zadanie zobrazować tę ideę. Wśród nich funkcjonują te wypracowane przez Międzynarodowy Związek Telekomunikacyjny – Digital Access Index (DAI) oraz Information Society Index (ISI). Pierwszy z nich swoim zakresem obejmuje takie elementy, jak[6]:

- kosztochłonność, rozumiana jako koszt dostępu do Internetu w porównaniu do poziomu produktu krajowego brutto na jednego mieszkańca,
- infrastruktura, rozumiana jako liczba abonentów telefonii na 100 mieszkańców,
- jakość, mierzona między innymi liczbą abonentów Internetu szerokopasmowego na 100 mieszkańców,
- wykorzystanie, mierzone liczbą użytkowników Internetu na 100 mieszkańców,
- wiedza, rozumiana jako liczba uczniów oraz studentów, a także wykształcenie osób dorosłych.

Z kolei wskaźniki wypracowane przez Information Society Index dotyczą czterech obszarów społecznych[7]:

– aspektów społecznych – poziom korupcji w administracji, odsetek osób, które pobierają naukę w szkolnictwie wyższym i średnim, a także wolności obywatelskie,

– komputerów – poziom wydatków w sektorze IT względem produktu krajowego brutto, poziom usług sektora IT względem produktu krajowego brutto, liczba gospodarstw domowych z komputerem osobistym oraz poziom wydatków na oprogramowanie,

– Internetu – ogólna liczba użytkowników Internetu, Internetu mobilnego, Internetu w domu oraz poziom wydatków w e-handlu,

– telekomunikacji – liczba sprzedanych urządzeń mobilnych, liczba gospodarstw domowych z Internetem szerokopasmowym oraz liczba abonentów Internetu szerokopasmowego.

W trakcie World Summit of Information Society w 2013 roku zdefiniowane zostały natomiast aż czterdzieści dwa wskaźniki, które odnosiły się przede wszystkim do poziomu rozwoju infrastruktury telekomunikacyjnej oraz jej dostępności, po-

[5] M. Czyżak, *Cyberprzestępczość a rozwój społeczeństwa informacyjnego*, „Ekonomiczne Problemy Usług" 2015, nr 117, s. 666.
[6] M. Luterek, *e-Government. Systemy informacji publicznej*, Warszawa 2010, s. 19.
[7] Ibidem, s. 22-24.

ziomu rozwoju sektora technologii informacyjnych i komunikacyjnych, poziomu dostępności technologii informacyjnych i komunikacyjnych wraz z ich wykorzystaniem przez przedsiębiorstwa, poziomu dostępności technologii informacyjnych i komunikacyjnych wraz z ich wykorzystaniem przez gospodarstwa domowe oraz użytkowników indywidualnych[8].

Odnosząc się natomiast do cyberprzestrzeni, konieczne jest podkreślenie, że temu słowu przypisuje się szczególnie wiele znaczeń. Zgodnie z definicją opracowaną przez Departament Obrony Stanów Zjednoczonych cyberprzestrzeń to „globalna domena środowiska informacyjnego składająca się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery"[9]. Z kolei, w myśl definicji opracowanej przez Francuską Agencję Bezpieczeństwa Sieci oraz Informacji, cyberprzestrzeń jest przestrzenią komunikacyjną, jaka została utworzona przez globalne połączenie sprzętu, jaki służy do przetwarzania danych cyfrowych w sposób automatyczny[10]. W oparciu o definicję jeszcze innej instytucji, Komisji Europejskiej, cyberprzestrzeń to przestrzeń wirtualna, w jakiej krążą elektroniczne dane, jakie są przetwarzane przez komputery na całym świecie[11].

NOWE OBLICZA PRZESTĘPCZOŚCI

Wskazany na wstępie przełom XX i XXI wieku jest okresem, w którym zarówno na świecie, jak i w Polsce doszło do gwałtownego rozwoju komputerów, Internetu oraz dostępu do niego z użyciem mobilnych technologii. Internet obecnie jest wykorzystywany w tak ważnych aspektach ludzkiego życia jak zakupy, e-urzędy, operacje bankowe oraz, najpowszechniejszy z nich, poczta elektroniczna. Trudno wyobrazić sobie, że nie zostaną przez nas sprawdzone najnowsze informacje, odwiedzone popularne portale społecznościowe albo że ktoś dobrowolnie zrezygnuje z oglądania telewizji lub słuchania radia za pośrednictwem Internetu[12]. Jednak korzystanie z Internetu ma swoje ciemne strony i może powodować liczne zagrożenia.

Cyberprzestępczość to nowa i jedna z najszybciej rozwijających się przestępczości o transgranicznym charakterze. Ma to przede wszystkim związek z tym, że Internet stał się praktycznie niezbędnym elementem ludzkiego życia, dzięki któremu możliwe jest przekazywanie informacji oraz komunikowanie się z całym światem. Nie powinno zatem dziwić, że przestępcy zdecydowali się na wykorzystanie związanych z nim możliwości. Jak można się domyślać, obecnie z cyberprzestrzeni korzy-

[8] M. Czyżak, *Cyberprzestępczość a rozwój społeczeństwa informacyjnego…*, s. 667.
[9] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 227.
[10] Ibidem, s. 230.
[11] M. Czyżak, *Cyberprzestępczość a rozwój społeczeństwa informacyjnego…*, s. 665.
[12] Ibidem.

sta wiele miliardów użytkowników, przez co Internet stanowi wręcz idealną przestrzeń dla przestępców, którzy w swoich działaniach (dzięki podjęciu odpowiednich kroków) mogą zostać całkowicie anonimowi i jednocześnie pozyskać dostęp do informacji i danych osobowych[13].

Przestępczość komputerowa pojawiła się w momencie, gdy komputery przestały być ściśle strzeżonym przedmiotem zamówień rządowych, przez co stały się dostępne dla szeregu instytucji gospodarczych. Już na początku lat pięćdziesiątych XX wieku komputeryzacja była wykorzystywana do sterowania prostymi i rutynowymi czynnościami w administracji i gospodarce – jednocześnie dopiero dwie dekady później ujawnione zostały poważniejsze przypadki oszustw, sabotażu oraz szpiegostwa gospodarczego, w jakich wykorzystane zostały komputery[14].

W latach sześćdziesiątych XX wieku rozpoczęto pozyskiwanie i przetwarzanie informacji na masową skalę, a także danych osobowych, do czego wykorzystywane były utworzone wtedy banki danych. Praktycznie od samego początku problemem był brak ograniczeń w dostępie do tych danych, co postrzegane było jako realne zagrożenie dla praw obywatelskich. Praktycznie równocześnie z pojawieniem się w latach siedemdziesiątych otwartych systemów sieciowych doszło do ich rozpowszechnienia – wtedy też nadużycia te zaczęto określać jako *hawking*. Z kolei poprzez upowszechnienie komputerów osobistych w latach osiemdziesiątych ubiegłego wieku doszło do wręcz masowego zjawiska nazywanego piractwem. Proceder ten polegał na tworzeniu i sprzedawaniu nielegalnych kopii gier, filmów, utworów muzycznych i programów komputerowych.

Z kolei rozwój sieci bankomatów prawie natychmiast wiązał się z nadużyciami mającymi ścisły związek z ich wykorzystywaniem do celów przestępczych. Zorganizowane grupy przestępcze zaczęły również wykorzystywać powszechność poczty elektronicznej oraz powiązania pomiędzy telekomunikacją a systemami przetwarzania danych – w tym przypadku wykorzystywana jest ona nie tylko do kryminalnych i gospodarczych celów przestępczych, ale również do całkowicie perfekcyjnego zacierania śladów przestępstwa.

W kolejnej dekadzie, w latach dziewięćdziesiątych XX wieku, komputery stały się wręcz nieodłącznym elementem praktycznie każdej dziedziny życia – poprzez rozwój światowych sieci komputerowych, powstanie programów przyjaznych dla użytkowników, którzy nie posiadają specjalistycznej wiedzy na temat technologii oraz stałej obniżki cen sprzętu, doszło do coraz szerszego wykorzystywania tych urządzeń. Stąd też naturalnie stały się one również przedmiotem tej działalności, jaka jest prowadzona niezgodnie z prawem[15]. W tym miejscu konieczne jest wskazanie, że w literaturze przedmiotu istnieją właściwie dwa terminy określające przestępstwa popełniane

[13] R. Jedlińska, *Problem przestępczości elektronicznej*…, s. 185-186.
[14] J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 33-35.
[15] M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 162.

przy pomocy komputerów oraz sieci Internet. Jednym z nich jest pojęcie przestępstwa komputerowego, a drugim – pojęcie cyberprzestępstwa.

Nie istnieje jedna, w pełni wyczerpująca definicja zjawiska przestępstwa komputerowego, co oznacza, że każdy z ekspertów wypracował sobie jego własne określenie. Przykładowo, Międzynarodowa Organizacja Policji Kryminalnych Interpol zdefiniowała przestępczość elektroniczną jako przestępczość w zakresie technik komputerowych. Przestępstwami, które są objęte zbiorczą nazwą przestępstw komputerowych, są zarówno czyny skierowane przeciwko samemu systemowi komputerowemu (czyli celem ataku jest komputer), jak i czyny, które są dokonywane przy użyciu komputera[16].

W opinii K. Jakubowskiego pojęcie przestępczości elektronicznej jest wieloznaczne i nieprecyzyjne: „W szerokim rozumieniu, przestępczość ta obejmuje wszelkie zachowania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, polegające zarówno na naruszaniu uprawnień do programu komputerowego, jak i godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz cały system połączeń komputerowych, a także w sam komputer. Należy tu zaznaczyć, iż będą to zarówno czyny popełniane przy użyciu elektronicznych systemów przetwarzania danych (komputer jako narzędzie do popełnienia przestępstwa), jak i skierowane przeciwko takiemu systemowi"[17].

Komputery oraz sieci komputerowe mogą „uczestniczyć" w przestępstwie na kilka sposobów, wśród których powinno się wymienić przede wszystkim[18]:

– komputer albo sieć komputerowa są narzędziem przestępstwa, czyli zostają użyte do jego popełnienia,
– komputer albo sieć są celem przestępstwa (czyli są niejako jego „ofiarą"),
– komputer albo sieć są użyte do zadań dodatkowych, jakie są związane z popełnieniem przestępstwa (przykładowo – do przechowania danych o nielegalnych działaniach).

Przestępczość elektroniczna jest również często określana mianem cyberprzestępczości.

Współczesna literatura na określenie przestępstw dokonywanych za pomocą komputera zwykła używać przede wszystkim pojęcia cyberprzestępczości. W praktyce jego określenie może wiązać się z pewnego rodzaju trudnościami, co ma związek przede wszystkim z tym, że niemal każda organizacja oraz poszczególne państwa postrzegają je nieco inaczej. Część z nich cyberprzestępczość traktuje jako swoistą „podkategorię" przestępczości komputerowej, uznając, że termin ten mieści w sobie wszystkie te przestępstwa (oraz mechanizmy służące do ich popełniania), jakie wymagają użycia Internetu albo też innych sieci komputerowych, które – jak się powszechnie przyjmuje – stają się bądź to narzędziem służącym do popełnienia przestępstwa

[16] R. Jedlińska, *Problem przestępczości elektronicznej…*, s. 187.
[17] J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 126.
[18] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, Kraków 2014, s. 134.

(lub też jego celem), albo też zostają wykorzystane do dodatkowych zadań związanych z popełnieniem konkretnego rodzaju przestępstwa (przykładowo do przechowywania danych o nielegalnej sprzedaży produktów bez akcyzy). Inni z kolei w cyberprzestępczości dostrzegają całkowicie nowe źródło zagrożeń, których elementem wspólnym jest specyficzny i nowy obszar, w jakim są one popełniane – cyberprzestrzeń[19].

Najogólniej jednak cyberprzestępczość jest rozumiana jako „przestępstwa cybernetyczne", czyli takie, jakie są popełniane w przestrzeni cybernetycznej. W efekcie cyberprzestępczość *sensu largo* obejmuje wszelkiego rodzaju typy czynów zabronionych, w popełnianiu których wykorzystuje się właśnie technologie informatyczne, a także czyny skierowane przeciwko samym danym oraz systemom informatycznym. W tego typu ujęciu pojęcie cyberprzestępczości będzie można odnosić do przestępstw, jakie są popełniane przy użyciu nowoczesnych technologii[20]. W ujęciu wąskim terminowi cyberprzestępczości powinno się jednak dać o wiele bardziej dokładane wyjaśnienie – z jednoczesnym zastrzeżeniem, że równocześnie powinno się zgodzić z tymi stwierdzeniami, które podkreślają jego zmienność i dynamikę. Dlatego też przyjmuje się, że cyberprzestępczość *sensu stricto* obejmuje przestępstwa komputerowe, przez które należy rozumieć ataki na systemy komputerowe wraz z przetwarzanymi przez nie danymi, co prowadzi do ich uszkodzenia albo też całkowitego zniszczenia. Przedrostek „cyber-" w każdym przypadku wskazuje na ścisłe powiązanie pewnych rodzajów czynów zabronionych z nowymi technologiami, jakie służą do kreowania cyberprzestrzeni przez system powiązań komputerowych[21].

Podsumowując problematykę wątpliwości etymologicznych i semantycznych dotyczących samego pojęcia cyberprzestępczości, można przyjąć, że pojęcie to obejmuje swoim zakresem szeroką gamę czynów zabronionych, poczynając od „typowych" przestępstw, jakie są popełniane z wykorzystaniem sieci informatycznych (na przykład włamania na konta bankowe lub kradzież tożsamości), przez przestępstwa przeciwko ochronie informacji (na przykład sabotaż komputerowy), aż po przestępstwa wieloaspektowe, jakimi są przede wszystkim złożone przestępstwa gospodarcze. Co ważne, w polskim prawie zostały zdefiniowane przestępstwa popełnianie przy użyciu komputerów, ale nie ma w nim jeszcze oficjalnej definicji cyberprzestępczości. W naszym kraju wypracowana została legalna definicja tego pojęcia, wynikająca z przepisów odnoszących się do stanów nadzwyczajnych, w tym między innymi ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[22] – w ustawie tej

[19] R. Łukasiewicz, *Rozwój informatyczny a cyberterroryzm*, [w:] B. Hołyst, K. Jałoszyński, A. Letkiewicz (red.), *Wojna z terroryzmem w XXI w.*, Szczytno 2009, s. 110.

[20] M. Siwicki, *Cyberprzestępczość…*, s. 11.

[21] Ibidem, s. 15-17.

[22] Ustawa z dnia 29 sierpnia 2002 roku o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (tekst jedn. Dz.U. z 2017 r., poz. 1932).

cyberprzestrzeń została określona jako „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (...), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami".

RODZAJE CYBERPRZESTĘPSTW I NARZĘDZIA WYKORZYSTYWANE W CYBERPRZESTĘPCZOŚCI

Sama natura cyberprzestrzeni, niezależnie od jej definicji, pozwala na stwierdzenie, że stanowi ona nieodłączny element współczesnego rozwoju, do czego przyczynia się to, że jest ona nie tylko środowiskiem obrotu gospodarczego lub wymiany informacji, ale stanowi również wymiar, w jakim może zostać naruszony obowiązujący porządek prawny.

Istnieje wiele rodzajów cyberprzestępstw. W niniejszym miejscu zostaną scharakteryzowane wybrane z nich.

Phishing

Poczta e-mail jest jednym z najpowszechniejszych współczesnych sposobów komunikacji. Wykorzystywana jest nie tylko w pracy zawodowej, ale służy również utrzymywaniu kontaktu z najbliższymi i rodziną. Większość współczesnych społeczeństw swoją komunikację opiera właśnie na poczcie elektronicznej, przez co nie powinno dziwić, że stała się ona jednym z narzędzi służących przeprowadzeniu cyberataku[23].

W oparciu o podstawową definicję przyjmuje się, że *phishing* polega na wysyłaniu do przypadkowych osób wiadomości e-mail, których odbiorcy pod wymyślonym pretekstem są namawiani do tego, by zalogować się pod fałszywym adresem. Przeważnie takim adresem jest niby-strona logowania banku, urzędu albo popularnego portalu. Zadaniem osoby atakowanej jest kliknięcie w załączony w wiadomości link – wtedy dochodzi do przekierowania na stronę internetową sfałszowaną przez przestępców. Nieświadomy odbiorca podaje swój link oraz hasło. W ten sposób przestępcy pozyskują dostęp do konta atakowanego na wybranym portalu internetowym albo mogą kontrolować jego konto bankowe[24]. Z kolei zgodnie z definicją, jaka została zamieszczona w art. 190a kodeksu karnego[25], *phishing* to wykorzystanie wizerunku albo też innych danych osobowych w celu wyrządzenia szkody osobistej lub majątkowej. Co istotne, istnieje również specjalna forma *phishingu*, tak zwany *spearphising*, który jest ukierunkowany na konkretną osobę lub instytucję. W tym przypadku przestępcy poświęcają bardzo dużo czasu na poznanie swojego celu i stworzenie w pełni spersonalizowanych wiadomości, jakie odnoszą się do sy-

[23] P. Danhieux, *Phishing i oszustwa w e-mailach*, „OUCH! Biuletyn Bezpieczeństwa Komputerowego" 2011, grudzień, s. 1.
[24] T. Pączkowski, *Słownik cyberbezpieczeństwa*, Katowice 2017, s. 43.
[25] Ustawa z dnia 6 czerwca 1997 roku – Kodeks karny (tekst jedn. Dz.U. z 2020 r., poz. 1517, ze zm.).

tuacji konkretnej jednostki. Tego typu wiadomości są o wiele trudniejsze do wykrycia, przez co trudniej jest się przed nimi bronić.

Omawiane przestępstwo łączy w sobie umiejętność wykorzystania przez przestępców socjotechniki oraz sztuczek technologicznych.

Do podstawowych celów ataków *phishingu* zalicza się przede wszystkim[26]:

– wyłudzenie istotnych i wrażliwych informacji, pozwalających na pozyskanie przez przestępców dostępu do ważnego dla nich profilu albo konta bankowego,

– przejęcie kontroli nad komputerem wybranej przez przestępców ofiary – w momencie kliknięcia w podany przez przestępców link odbiorca jest przekierowywany na stronę przeprowadzającą w tle ataki na przeglądarkę internetową – w chwili, gdy atak ten się powiedzie, przestępcy uzyskują kontrolę nad wybranym komputerem,

– przejęcie kontroli nad komputerem przez zainfekowane załączniki – po otwarciu przez odbiorcę takiego załącznika przestępca zyskuje dostęp do komputera odbiorcy.

– W ochronie przed omawianym zagrożeniem przydaje się przede wszystkim podejście zdroworozsądkowe oraz każdorazowe sprawdzanie otrzymanej wiadomości e-mail, w tym przede wszystkim takiej, która wymaga od odbiorcy podjęcia natychmiastowego działania.

Cyberterroryzm

Samo słowo „terroryzm" wywodzi się od łacińskiego terminu *terror* oznaczającego „stosowanie przemocy, gwałtu, okrucieństwa w celu zastraszenia kogoś"[27]. Jednak samo pojęcie terroryzmu, pomimo całkowitej zgodności badaczy, polityków i organizacji międzynarodowych co do tego, że obecnie stanowi jedno z najpoważniejszych zagrożeń, nie zostało dokładnie i jednoznacznie określone.

Warto w tym miejscu przedstawić definicję terroryzmu, jaka została opracowana przez FBI (ang. *Federal Bureau of Investigation*) – zgodnie z nią terroryzmem jest „bezprawne użycie siły lub przemocy wobec osób lub mienia, w celu zastraszenia lub wywarcia przymusu na rząd, ludność cywilną albo część wyżej wymienionych, co zmierza do promocji celów politycznych lub społecznych"[28].

Jednym z rodzajów współczesnego terroryzmu jest cyberterroryzm, będący dość nowym zjawiskiem – jego podstawowa historia sięga jedynie do okresu ostatniego dwudziestopięciolecia. Za twórcę terminu cyberterroryzmu uznaje się pracownika Institute for Security and Intelligence z Kalifornii, B. Collina, który już w latach osiemdziesiątych XX wieku użył go dla połączenia terroryzmu i cyberprzestrzeni[29]. Współczesny cyberterroryzm zakłada wykorzystanie nowoczesnych

[26] P. Danhieux, *Phishing i oszustwa w e-mailach*…, s. 1-2.
[27] *Słownik języka polskiego*, Warszawa 2002.
[28] B. Hoffman, *Oblicza terroryzmu*, Warszawa 2001, s. 27.
[29] D. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 79.

technologii komputerowych i teleinformatycznych, czyli tych wszystkich obszarów, z których członkowie społeczeństw korzystają na co dzień.

W oparciu o definicję opracowaną przez B. Collina cyberterroryzm to „świadome wykorzystanie systemu informacyjnego, sieci komputerowej lub jej części składowych w celu wsparcia lub ułatwienia terrorystycznej akcji”[30]. Natomiast zgodnie z definicją, jaka została wpracowana przez FBI, przyjmuje się, że cyberterroryzmem jest „obmyślony, politycznie umotywowany akt przemocy wymierzony przeciwko informacjom, programom, systemom komputerowym lub bazom danych, który, mając charakter niemilitarny, przeprowadzony jest przez ponadnarodowe lub narodowe grupy terrorystyczne”[31].

Zagrożenie cyberterroryzmem dotyczy każdej jednostki organizacyjnej państwa oraz każdego podsektora infrastruktury krytycznej. Co ważne, zagrożenie to dotyczy nie tylko pojedynczych państw, ale równie często całych ich grup i organizacji międzynarodowych.

Odnosząc się do podziału na obszary zagrożeń cyberterrorystycznych, obecnie mamy do czynienia z atakami na[32]:

– systemy wojskowe, jakie przechowują informacje o rozmieszczeniu wojsk, broni oraz satelitów, a także podmioty, które prowadzą badania nad nowymi rodzajami uzbrojenia. Podstawowymi sprawcami są agenci obcych wywiadów działający na polecenie innych państw,

– systemy przedsiębiorstw gospodarczych, które przechowują istotne dla działalności danego przedsiębiorstwa informacje. Ich głównymi sprawcami są przede wszystkim osoby działające na polecenie konkurencji (albo też byli pracownicy przedsiębiorstwa, chcący się w pewien sposób „zemścić”),

– systemy wchodzące w skład infrastruktury krytycznej państwa (systemu transportu, sektora bankowo-finansowego albo też służb do działań specjalnych), w ramach których przechowuje się istotne z punktu widzenia bezpieczeństwa państwa informacje. Sprawcami tego typu przestępstw mogą być zarówno pracownicy, którzy są powiązani z tego typu systemami, jak i terroryści, którymi kieruje chęć zysku.

Oddziaływanie omawianego rodzaju ataku w każdym przypadku posiada wielowymiarowy charakter. Dodatkowo przyczynia się on do dezorganizacji i destrukcji sporej części danej społeczności (czasami zdarza się, że nawet całej). Szczególnie destrukcyjne są przede wszystkim ataki na systemy energetyczne, ale również na sieci bankowe i systemy łącznościowe – w taki sposób przestępcy oddziałują na poszczególne rządy oraz na opinię publiczną.

---

[30] K. Kośla, *Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski*, [w:] M. Jędrzejewski, *Analiza systemowa zjawiska infoterroryzmu*, Warszawa 2002, s. 480.

[31] R. Maciejewski, *Cyberterroryzm w polityce bezpieczeństwa państwa. Problemy ochrony infrastruktury krytycznej*, Poznań 2019, s. 50.

[32] J. Kowalewski, M. Kowalewski, *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki informacyjne” 2014, nr 1-2, s. 28.

Malware

Zgodnie z podstawową definicją *malware* to złośliwe oprogramowanie, które prowadzi do utrudnień i przeszkód w pracy na komputerze. Jego cel może również posiadać przestępczy charakter – dzieje się tak, gdy celem hakera jest pozyskanie poufnych danych albo też zaszkodzenie użytkownikowi danego komputera w jakikolwiek sposób. Do *malware* zalicza się[33]:

– wirusy komputerowe – programy, które, działając bez wiedzy użytkownika komputera, wykonują wiele operacji utrudniających lub też wręcz uniemożliwiających poprawne działanie systemu operacyjnego komputera. Wirusy są przenoszone przez zainfekowane pliki (nosiciela), które są dostarczane do komputera choćby za pomocą pamięci USB, płyty CD albo też Internetu. Skutkiem działania wirusów na komputerze jest między innymi zmiana lub skasowanie danych, wyświetlanie niepożądanych obrazów lub odgrywanie niechcianych dźwięków, przejęcie kontroli nad komputerem albo też całkowite zablokowanie możliwości korzystania z niego,

– robaki (ang. *worms*) – programy, których obszar działania jest zbliżony do działania wirusów, jednak nie potrzebują one pliku nosiciela, ponieważ są rozpowszechniane poprzez sieć, do której dany komputer jest podłączony,

– konie trojańskie (trojany) – programy, które, podając się za znane i przydatne użytkownikowi komputera oprogramowanie, w rzeczywistości są oprogramowaniem złośliwym. Do uruchomienia trojana dochodzi na przykład w przypadku otwarcia załącznika w wiadomości e-mail, odwiedzenia zainfekowanej strony albo też uruchomienia programu pobranego z sieci,

– oprogramowanie szpiegujące (ang. *spyware*) – oprogramowanie wykonujące działania ukryte przed użytkownikiem komputera. Ma ono za zadanie zebranie informacji o użytkowniku (na przykład o odwiedzanych przez niego stronach) oraz wykradanie poufnych danych, takich jak loginy i hasła dostępu,

– *rootkity* – oprogramowanie, które zmienia działanie systemu operacyjnego komputera i ukrywa ten fakt przed jego użytkownikiem. *Rootkity* pozwalają na przejęcie komputera przez osoby trzecie, które mogą w dalszej kolejności wykorzystać go do popełnienia przestępstwa (na przykład ataku hakerskiego).

Co ważne, złośliwe oprogramowanie jest wykorzystywane obecnie nie tylko przez pojedynczych hakerów, ale również przez całe grupy przestępcze. Najskuteczniejszym sposobem na zapobiegnięcie atakowi hakerów w zakresie *malware* jest zainstalowanie na komputerze antywirusa oraz narzędzia typu *anti-malware*. W ten sposób można usunąć złośliwe oprogramowanie z komputera i zapobiec jego zainfekowaniu[34].

[33] T. Pączkowski, *Słownik cyberbezpieczeństwa…*, s. 38.

[34] D. Doroziński, *Hakerzy. Technoanarchiści cyberprzestrzeni*, Gliwice 2001, s. 121.

Hacking

O początkach *hackingu* mowa jest już od chwili powstania pierwszych sieci telefonicznych – to właśnie wtedy pojawili się tak zwani phreakerzy (ang. *phone freak* – telefoniczny maniak). Włamywali się oni do sieci telekomunikacyjnych w celu nawiązania bezpłatnego połączenia. W tym samym czasie pojawiła się również inna grupa przestępców – tak zwanych crackerów (ang. *crack* – łupać), którzy specjalizowali się w łamaniu zabezpieczeń systemów telekomunikacyjnych – obecnie pojęcie to jest wykorzystywane w celu określenia „łamaczy" haseł oraz zabezpieczeń. To właśnie te grupy przestępców uznawane są za poprzedników współczesnych hackerów (co istotne, część z nich właśnie w ten sposób rozpoczynała swoją przestępczą działalność).

W początkowym okresie pojęcie „hacker" posiadało całkowicie inne od współczesnego znaczenie – przede wszystkim tym mianem określano zdolnego programistę. Dopiero później, w latach siedemdziesiątych ubiegłego wieku, na skutek przenikania się subkultury hackerów z subkulturą phreakerów, zaczął on nabierać współczesnego znaczenia – czyli osoby, która działa w podziemiu komputerowym i włamuje się do komputerów oraz całych sieci komputerowych (często dla zysku, sławy, ale także w imię szlachetnych pobudek). Wszystko to prowadzi do tego, że przez osobę hackera przeważnie rozumie się jednostkę, która zarówno włamuje się do komputerów i sieci komputerowych, jak i działa w celu zakłócenia ich normalnej pracy. W potocznym rozumieniu pojęcie to używane jest dla określenia w sposób ogólny przestępców, którzy działają w Internecie[35].

W związku z powyższym przyjmuje się, że hacking może być pojmowany na kilka sposobów. Pierwszym z nich jest rozumienie *sensu stricto*. W takim przypadku przez hacking można rozumieć zachowanie, które polega na pozyskaniu dostępu do systemu informatycznego albo sieci komputerowych. W rozumieniu *sensu largo* hackingiem są wszelkiego rodzaju zamachy dokonywane na bezpieczeństwo systemów i danych informatycznych (w tym na przykład zniszczenie danych komputerowych lub ich modyfikacja) – można więc przyjąć, że są nim praktycznie wszystkie przestępstwa dokonywane w sieci internetowej, poza paroma wyjątkami, takimi jak na przykład rozpowszechnianie pornografii[36].

W oparciu o podstawową definicję przyjmuje się, że hacking to czynności wykonywane przez hakera. Do takich zalicza się między innymi łamanie haseł, włamywanie się na serwer albo też kradzież tożsamości[37].

Cyberstalking

Cyberstalking to forma cyberprzemocy, którą jest – w oparciu o definicję – „wykorzystanie technik informacyjnych i komunikacyjnych do świadomego, wielokrotnego

[35] D. Littlejohn Shinder, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci?*, Gliwice 2005, s. 67.
[36] F. Radoniewicz, *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w Działaniu. Sprawy Karne" 2013, nr 13, s. 122.
[37] T. Pączkowski, *Słownik cyberbezpieczeństwa…*, s. 33.

i wrogiego zachowania się osoby lub grupy osób, mającego na celu krzywdzenie innych"[38]. O zjawisku *cyberstalkingu* mowa jest od mniej więcej 20 lat – jednak wcześniej istniało zjawisko stalkingu, z którego się ono bezpośrednio wywodzi. Stalking można zdefiniować jako złośliwe i powtarzane śledzenie oraz prześladowanie wybranej osoby, które może zagrażać jej bezpieczeństwu lub życiu. Etymologia słowa stalking wiąże się z angielskim terminem *to stalk*, oznaczającym tropienie zwierzęcia, a także skradanie się, skrywanie i śledzenie. Przywołane pojęcie zaczęto używać od mniej więcej 1989 roku, kiedy to amerykańskie media zaczęły donosić o stalkingu aktorki Rebekki Scheaffer, która została zamordowana przez chorego psychicznie fana.

Zgodnie z przepisami kodeksu karnego[39] za stalking grozi kara do trzech lat pozbawienia wolności. W sytuacji, gdy ofiara tego przestępstwa popełniła samobójstwo (lub podjęła jego próbę), kara zwiększa się do dziesięciu lat pozbawienia wolności. Ściganie sprawców stalkingu odbywa się na wniosek osoby pokrzywdzonej.

Cyberstalking przyjmuje różnorodne formy. Do najczęstszych z nich zalicza się[40]:

- wysyłanie fałszywych informacji albo plotek,
- wysyłanie obraźliwych wiadomości (e-mail, na czatach i innych komunikatorach),
- zamieszczanie obraźliwych komentarzy albo realnych gróźb na grupach i forach dyskusyjnych,
- podawanie się za kogoś innego i przesyłanie informacji w jego imieniu,
- zachęcanie innych użytkowników sieci do zniewagi, prześladowania i znieważania konkretnej osoby,
- próba monitorowania czyichś działań poprzez instalację oprogramowania śledzącego,
- kradzież tożsamości związana nie tylko z podszywaniem się pod kogoś, ale również z całkowitym przejęciem jej cech i właściwości,
- poszukiwanie różnego rodzaju informacji o ofierze w celu poznania tych, które mogłyby jej zaszkodzić albo też ją ośmieszyć.

Każde z wymienionych powyżej zachowań wywołuje u ofiary poczucie stałego zagrożenia oraz życia pod presją. Aby zabezpieczyć się przed cyberstalkerem, powinno się zadbać o własną anonimowość w sieci. Pomocne może być stworzenie oddzielnego e-maila do kontaktowania się z obcymi osobami oraz stosowanie zasady ograniczonego zaufania.

Pomysłowość cyberprzestępców jest co do zasady nieograniczona – powinno się przez to rozumieć, że bezustannie zwiększają oni zakres swojego oddziaływania na indywidualne osoby oraz instytucje. To z kolei prowadzi do tego, że poza wskaza-

[38] K. Tomaszek, *Stalker – psychologiczna charakterystyka sprawców przestępstw „uporczywego nękania"*, „Studia z Psychologii w KUL" 2012, t. 18, s. 137.

[39] Ustawa z dnia 6 czerwca 1997 roku – Kodeks karny….

[40] J. Groth, *Cyberstalking – perspektywa psychologiczna*, „Forum Oświatowe" 2010, nr 2, s. 87.

nymi powyżej rodzajami cyberprzestępstw, istnieje w cyberprzestrzeni jeszcze wiele innych zagrożeń, z jakimi mogą spotkać się użytkownicy komputerów oraz sieci Internet. Do innych zagrożeń komputerowych zalicza się[41]:

– *spoofing* – techniki zmierzające do podszycia się pod kogoś w Internecie,
– *grooming* – uwodzenie przez Internet (przede wszystkim osób nieletnich),
– *flaming* – celowe zaognianie wymiany zdań pomiędzy użytkownikami różnego rodzaju serwisów dyskusyjnych, grup i innych grup użytkowników, które prowadzi do eskalacji agresji wypowiedzi,
– trollowanie – różnego rodzaju nieprzyjazne zachowania wobec innych użytkowników Internetu, których celem jest rozbicie prowadzonej dyskusji; zjawisko to jest obecne w miejscach, które są przeznaczone do wymiany myśli pomiędzy internautami, czyli na różnego rodzaju serwisach dyskusyjnych albo czatach.

Również powyższe uzupełnienie nie wyczerpuje całości katalogu wszystkich przestępstw komputerowych. Odnosząc się z kolei do cyberprzestępczości jako zjawiska o charakterze kryminologicznym, warto podkreślić, że ogólna liczba przestępstw w Polsce od 2003 roku nie zmniejsza się, choć i tak ogólny wskaźnik przestępczości jest niższy od średniej europejskiej. Przytoczone dane jednak nie dotyczą cyberprzestępczości. Ponadto w ciągu ostatnich kilkunastu lat znacznie zwiększyła się liczba wykorzystywanych urządzeń elektronicznych oraz ich użytkowników korzystających coraz częściej i chętniej z Internetu. To z kolei doprowadziło do powstania całkowicie nowych form i sposobów popełniania przestępstw. Sami użytkownicy Internetu jednak nie do końca zdają sobie sprawę z zagrożeń płynących z sieci, co przestępcy bardzo chętnie wykorzystują[42].

Podstawowe przestępstwa komputerowe, z jakimi borykają się użytkownicy w naszym kraju, to przede wszystkim oszustwa internetowe oraz przestępstwa przeciwko integralności i dostępności informacji. Zasadniczym celem przestępców w tych przypadkach jest wyrządzenie szkody lub też pozyskanie konkretnej korzyści majątkowej. Co prawda sprawca nie ma wpływu w tym przypadku na motywacje ofiary, ale jednocześnie bez jej upoważnienia wpływa na automatyczne gromadzenie, przetwarzanie oraz przekazywanie danych – wprowadza nowe zapisy, zmienia lub też usuwa zapisy już istniejące[43].

Zgodnie z danymi statystycznymi Policji na koniec 2016 roku liczba stwierdzonych oszustw komputerowych wynosiła 97 388, a liczba postępowań w związku z tym właśnie przestępstwem wynosiła niespełna 80 000. W tym samym roku liczba przestępstw określanych w kodeksie karnym jako oszustwa komputerowe wyniosła tylko 4207. Co ważne jednak, przez okres dziesięciu lat – czyli pomiędzy 2006 a 2016 rokiem liczba oszustw komputerowych wzrosła o prawie 850%.

[41] T. Pączkowski, *Słownik cyberbezpieczeństwa…*, s. 27.
[42] Rada Unii Europejskiej, *Sprawozdanie oceniające z siódmej rundy wzajemnych ocen poświęconej praktycznemu wdrożeniu i funkcjonowaniu europejskich polityk w dziedzinie zapobiegania cyberprzestępczości i jej zwalczania – Polska*, Bruksela 2017, s. 19.
[43] L. Krakowiak, *Cyberprzestępstwa w Polsce są statystycznie niewidoczne*, https://www.computerworld.pl/news/Cyberprzestepstwa-w-Polsce-sa-statystycznie-niewidoczne,413041.html [dostęp: 27.08.2021].

W tym miejscu niezbędne jest odniesienie się do danych na temat oszustw komputerowych, których ofiarami są podmioty gospodarcze. Wspomniane dane dotyczą 2019 roku, kiedy to liczba naruszeń cyberbezpieczeństwa wzrosła o 11% w porównaniu do roku poprzedzającego[44]. Z informacji, jakie zostały przedstawione przez Uniwersytet w Maryland, wynika, że przestępcy komputerowi atakują użytkowników co cztery sekundy, czyli każdego dnia dochodzi do średnio 2244 cyberataków. Co istotne, przeważnie ofiarami hakerów padają niewielkie korporacje, małe przedsiębiorstwa, które nie posiadają nowoczesnych zabezpieczeń ani też działu IT z wykwalifikowanymi pracownikami. Ponadto przedsiębiorstwa te o wiele częściej są skłonne do przekazania okupu. Wszystko to prowadzi do tego, że stają się one częściej celem ataków cybernetycznych. Nie wolno również zapomnieć o tym, że małe przedsiębiorstwa dość często upadają po ataku hakerskim – dochodzi do tego w ciągu sześciu miesięcy (około 60% firm)[45]. Co ważne, najbardziej narażone na ataki są przedsiębiorstwa działające w branży medycznej.

Zgodnie ze sprawozdaniem na temat zapobiegania cyberprzestępczości w Polsce cyberprzestępczość w dalszym ciągu jest działalnością podejmowaną zarówno przez zorganizowane grupy przestępcze, jak i przez indywidualnych przestępców. Ponadto na przeprowadzenie cyberataku decydują się organizacje terrorystyczne oraz społeczności ekstremistyczne[46].

W opinii polskich władz do najważniejszych zagrożeń w cyberprzestrzeni powinno się zaliczyć te, które w najbliższym czasie mogą stać się o wiele bardziej niebezpieczne[47]. Są nimi:

– zwiększająca się liczba przestępstw komputerowych popełnianych przeciwko ochronie informacji, bezpieczeństwu publicznemu i własności – związane są one ze znacznym i szybkim rozwojem informatyki wraz ze szczególnie szerokim jej wykorzystaniem w praktycznie każdej dziedzinie życia,

– postępujący w ciągu ostatnich lat rozwój telekomunikacji na światowym rynku (w tym również na rynku polskim) oraz umacnianie pozycji przedsiębiorstw produkujących sprzęt telekomunikacyjny – niestety, w ten sposób część sprzętu telekomunikacyjnego może być wykorzystywana do działań wywiadowczych,

– prowadzenie szpiegowskiej działalności w sieci, skupionej przede wszystkim na szkodzeniu czołowym instytucjom i przedsiębiorstwom, jakie działają w sferze infrastruktury krytycznej.

---

[44] T. Foryś, *Cyberbezpieczeństwo w 2019 r. – podsumowanie*, https://www.vida.pl/cyberbezpieczenstwo-w-2019-r-podsumowanie/ [dostęp: 27.08.2021].

[45] Ibidem.

[46] Rada Unii Europejskiej, *Sprawozdanie oceniające z siódmej rundy wzajemnych ocen poświęconej praktycznemu wdrożeniu i funkcjonowaniu europejskich polityk w dziedzinie zapobiegania cyberprzestępczości i jej zwalczania – Polska…*, s. 20.

[47] Rada Unii Europejskiej, *Sprawozdanie oceniające z siódmej rundy wzajemnych ocen poświęconej praktycznemu wdrożeniu i funkcjonowaniu europejskich polityk w dziedzinie zapobiegania cyberprzestępczości i jej zwalczania – Polska…*, s. 20.

Możliwe jest również założenie, że wskazane powyżej niebezpieczeństwa będą dotyczyły również takich elementów jak wykorzystanie złośliwego oprogramowania, naruszenie bezpieczeństwa, kradzież tożsamości oraz nabywanie kart bankomatowych wraz z kryptowalutą. Co ważne, cyberprzestępcy ciągle udoskonalają wykorzystywane przez siebie metody pracy, przez co odpowiednim służbom trudno jest przewidzieć ich kolejne kroki.

W naszym kraju liczba przestępstw komputerowych nigdy nie została dokładnie oszacowana, co ma związek z tym, że dość często zdarza się, iż policja, zamiast stawiać przestępcom zarzuty z nowo określonych przepisów, woli odwoływać się do wcześniej stosowanych artykułów kodeksu karnego. To z kolei ma wpływ na statystyki dotyczące cyberprzestępczości i skłania do wniosku, że nie odpowiadają one stanowi faktycznemu.

Niezbędne jest podkreślenie, że w czasie, gdy Internet dopiero powstał i rozwijał się, przez co siłą rzeczy był dostępny dla niewielkiego grona osób, kwestia bezpieczeństwa była traktowana po macoszemu, właściwie jako problem wręcz marginalny. Obecnie jednak przestępczość komputerowa stanowi znacznie poważniejszy problem (do czego przyczynia się przede wszystkim nasycenie świata nowoczesnymi technologiami), czego wyrazem jest fakt, iż z roku na rok liczba przestępstw popełnianych za pomocą nowoczesnych technologii systematycznie się zwiększa. Dlatego też, poprzez angażowanie coraz większych środków finansowych przez bankowość internetową (w tym rosnąca liczbę przelewów internetowych i tych dokonywanych w ramach bankowości mobilnej), a także rozszerzającą się działalność portali ogłoszeniowych i aukcyjnych oraz sklepów internetowych, kładzie się coraz większy nacisk na zwalczanie przestępczości komputerowej[48].

CYBERBEZPIECZEŃSTWO, CZYLI BEZPIECZEŃSTWO W SIECI

Niestety, rosnąca liczba komputerów na całym świecie i praktycznie nieograniczony dostęp do Internetu sprawiają, że podczas korzystania z sieci coraz trudniej czuć się bezpiecznie. Transfer życia społecznego, gospodarczego i politycznego do świata wirtualnego powoduje konieczność jego ochrony. W tym miejscu należy wspomnieć o takim terminie, jak cyberbezpieczeństwo. W najprostszym ujęciu cyberbezpieczeństwo stanowi reakcję na zagrożenia związane z cyberprzestępczością. Zgodnie z oficjalną definicją Komisji Europejskiej „cyberbezpieczeństwo to zbiór zabezpieczeń i działań stosowanych w ramach ochrony przestrzeni irtualnej, jej dostępności, poufności oraz integralności przed zagrożeniami, na które jest narażona”[49]. W pojęciu tym zawiera się przede wszystkim zapewnienie bezpieczeństwa

[48] M. Stefanowicz, *Cyberprzestępczość – próba diagnozy zjawiska*…, s. 19-20.

[49] Komisja Europejska, Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń

w cyberprzestrzeni. To nic innego jak ochrona przetwarzania informacji zawartych w globalnej sieci komputerowej[50].

Niepokojące wydaje się być to, że użytkownicy sieci nie do końca zdają sobie sprawę z tego, jak bardzo potężnym jest ona narzędziem. Wiele osób widzi jedynie same pozytywy. Prawda jest taka, że w zasadzie jeszcze do niedawna nie zdawano sobie sprawy ze wszystkich niebezpieczeństw, jakie niesie ze sobą użytkowanie globalnej sieci komputerowej. Zagrożenie stało się namacalne dopiero po kilku atakach na, co bardzo ważne, osoby prywatne, ale także systemy odpowiadające za bezpieczeństwo państwa. Na początku uważano, że Internet będzie wykorzystywany jedynie do pozyskiwania i zdobywania informacji. Szybko jednak to wyobrażenie zostało zweryfikowane i zaczęto się poważnie niepokoić o bezpieczeństwo cyfrowe obywateli i państw. Zagrożenie odczuwały przede wszystkim kraje wysoko rozwinięte[51].

Koncepcja cyberbezpieczeństwa miała okazać się być pewnego rodzaju lekarstwem na lekkomyślność i naiwność osób, które w codziennym życiu korzystają z globalnej sieci komputerowej. W 2016 roku na konferencji NATO cyberprzestrzeń została uznana za jeden z obszarów działalności cyberprzestępców. W związku z tym Internet został dołączony do traktatowej odpowiedzialności (innymi obszarami wymienionymi w nim są morze, ziemia, powietrze i kosmos). Trzeba zdawać sobie sprawę z tego, że zasady, na jakich działa współczesny świat, w żaden sposób nie gwarantują poczucia bezpieczeństwa. Dlatego też żadna jednostka, grupa społeczna czy też państwo nie powinny się czuć w pełni bezpieczne. Zmylić obywateli mogą statystyki. Wydawać by się mogło, że jeśli mieszkamy w miejscu o bardzo niskim, wręcz znikomym poziomie przestępczości, to teoretycznie nic nam nie może grozić. Nic bardziej mylnego. Przestępcy internetowi są w stanie dotrzeć wszędzie, niezależnie od położenia geograficznego. Aby dokonać przestępstwa w cyberprzestrzeni, wystarczy jedynie urządzenie mające dostęp do Internetu – komputer, tablet, telefon, a ostatnio nawet zegarek.

Coraz częściej w przestrzeni publicznej mówi się również o cybernetycznej wojnie, która toczy się pomiędzy osobami zajmującymi się cyberatakami a tymi, które starają się im przeciwdziałać. Powszechnie mówi się również, że współczesne mocarstwa, realizując swoje ambicje, będą rezygnowały z tradycyjnych wojen związanych z dużymi nakładami finansowymi i znacznymi ofiarami w ludziach, na rzecz właśnie wojny w cyberprzestrzeni, w przypadku której wystarczające jest zatrudnienie wykwalifikowanych specjalistów[52].

[50] E. Lisocki, *Cyberterroryzm państwowy i niepaństwowy – początki, skutki i formy*, Gdańsk 2009, s. 78-79.
[51] A. Podraza, P. Potakowski, K. Wiak, *Cyberterroryzm zagrożeniem XXI wieku*, Warszawa 2013, s. 45.
[52] M. Adamczuk, *Ewolucja strategii i metod działania islamskich ugrupowań terrorystycznych i ich wpływ na bezpieczeństwo Polski*, „Bezpieczeństwo Narodowe" 2011, nr 19, s. 14.

PODSUMOWANIE

Internet jest rewolucyjnym wynalazkiem i ma wiele atutów, do których należą szybka komunikacja, błyskawiczny dostęp do informacji we wszystkich językach, e-urzędy, szybkie zakupy i realizacja płatności, rozmowy rekrutacyjne online, a nawet e-porady medyczne. Oprócz praktycznych zastosowań, mających na celu ułatwienie codziennego życia, urządzenia podłączone do Internetu dostarczają rozrywki. Nie należy jednak zapominać, że Internet, oprócz zalet, ma także wady, niosąc ze sobą coraz więcej zagrożeń, których źródłem jest cyberprzestępczość.

Jak dowodzi niniejsze opracowanie, cyberprzestępczość to stosunkowa nowa, ale niestety bardzo szybko rozwijająca się forma przestępczości. W większości państw istnieją osobne komórki, których działalność skupia się na ściganiu cyberprzestępczości. W Polsce od lat działa policyjny Wydział Wsparcia Zwalczania Cyberprzestępczości, i jest to wydzielona komórka organizacyjna Komendy Głównej Policji. Niestety, rozwój technologii sprawia, że większość metod zwalczania przestępczości internetowej stosunkowo szybko staje się przestarzała i nieskuteczna. Tymczasem ilość przestępstw popełnianych za pomocą komputerów stale rośnie, a główną przeszkodą w sprawnym ściganiu przestępców jest transgraniczność cyberprzestępczości, a także losowość w wybieraniu ofiar przestępstw.

Co więcej, zagrożenie cyberprzestępczością znacząco wzrosło w ostatnich latach. Wszystko to sprawia, że zwalczanie cyberprzestępczości stanowi coraz większe wyzwanie. Użytkownicy komputerów nie zdają sobie sprawy z tego, że codzienne sytuacje, których doświadczają są cyberprzestępstwami i powinny zostać zgłoszone organom ścigania. A właśnie fakt, że poszkodowani w wyniku przestępstw komputerowych nie składają w swoich sprawach zawiadomień, sprawia, że cyberprzestępczości statystycznie nie widać.

Rodzaje cyberprzestępstw i narzędzia wykorzystywane w cyberprzestępczości skłaniają do wniosku, że zagrożenie cyberprzestępczością oraz problematyka zapewnienia bezpieczeństwa w sieci to najbardziej palący problem współczesnego świata. Świata, w którym zachodzące zmiany przyczyniają się z jednej strony do ułatwienia codziennego życia, a z drugiej – powodują całkowicie nowe zagrożona. Dlatego tak ważne jest edukowanie społeczeństwa i skupienie się na problemie edukacji informatycznej, prowadzonej od najwcześniejszych lat. Z uwagi na kreatywność przestępców wykorzystujących nowoczesne technologie coraz trudniej będzie zapewnić bezpieczeństwo użytkownikom komputerów korzystających z dostępu do sieci internetowej. Na szczęście formą przeciwdziałania zagrożeniu okazała się koncepcja bezpieczeństwa w przestrzeni wirtualnej, czyli cyberbezpieczeństwa. We współczesnym świecie to właśnie bezpieczeństwo informacji i wszelkich systemów informatycznych jest gwarancją bezpieczeństwa całego kraju.

Ogromna większość cyberprzestępstw to wciąż jeszcze stosunkowo drobne, mało wyrafinowane występki popełniane z użyciem łatwo dostępnych narzędzi. Oznacza to, że aby zostać cyberprzestępcą, nie trzeba posiadać specjalistycznej wiedzy. Dlatego na zakończenie warto zastanowić się, w jakim kierunku będzie ewoluowała cyberprzestępczość i jakie są prognozy z nią związane. Niewykluczone, że w najbliższych latach cyberprzestępcy będą dysponowali narzędziami, które pozwolą zabijać ludzi. Taki scenariusz jest realny za sprawą ataków na środowiska technologii operacyjnych, czyli oprogramowanie, które monitoruje lub kontroluje sprzęt, zasoby i procesy. Zatem cele i ambicje cyberprzestępczości będą ewoluowały w kierunku jeszcze większej skuteczności. Oznacza to, że wyłudzenie pieniędzy czy zakłócenie procesu produkcyjnego w przedsiębiorstwie nie będzie dla cyberprzestępców żadnym problemem. Z chęci zysku ich ambicją może być atak na podmioty, a nawet całe sektory odpowiedzialne za zdrowie publiczne i ratowanie życia (szpitale, laboratoria mikrobiologiczne, krajowe systemy ratownicze, centra zarządzania kryzysowego).

Bibliografia

Adamczuk M., *Ewolucja strategii i metod działania islamskich ugrupowań terrorystycznych i ich wpływ na bezpieczeństwo Polski*, „Bezpieczeństwo Narodowe" 2011, nr 19.

Czyżak M., *Cyberprzestępczość a rozwój społeczeństwa informacyjnego*, „Ekonomiczne Problemy Usług" 2015, nr 117.

Danhieux P., *Phishing i oszustwa w e-mailach*, „OUCH! Biuletyn Bezpieczeństwa Komputerowego" 2011, grudzień.

Denning D., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.

Doroziński D., *Hakerzy. Technoanarchiści cyberprzestrzeni*, Gliwice 2001.

Foryś T., *Cyberbezpieczeństwo w 2019 r. – podsumowanie*, https://www.vida.pl/cyberbezpieczenstwo-w-2019-r-podsumowanie/ [dostęp: 27.08.2021].

Golonka A., *Cyberprzestępczość – międzynarodowe standardy zwalczania zjawiska a polskie regulacje karne*, „Studia Prawnicze. Rozprawy i Materiały" 2016, nr 1 (18).

Groth J., *Cyberstalking – perspektywa psychologiczna*, „Forum Oświatowe" 2010, nr 2.

Grzelak M., Riedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, Kraków 2014.

Hoffman B., *Oblicza terroryzmu*, Warszawa 2001.

Hołyst B., Jałoszyński K., Letkiewicz A. (red.), *Wojna z terroryzmem w XXI w.*, Szczytno 2009.

Jedlińska R., *Problem przestępczości elektronicznej*, „Ekonomiczne Problemy Usług" 2017, nr 1.

Jędrzejewski M., *Analiza systemowa zjawiska infoterroryzmu*, Warszawa 2002.

Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.

Kośla R., *Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski*, [w:] M. Jędrzejewski, *Analiza systemowa zjawiska infoterroryzmu*, Warszawa 2002.

Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki informacyjne" 2014, nr 1-2.

Krakowiak L., *Cyberprzestępstwa w Polsce są statystycznie niewidoczne*, https://www.computerworld.pl/news/Cyberprzestepstwa-w-Polsce-sa-statystycznie-niewidoczne,413041.html [dostęp: 27.08.2021].

Lichocki E., *Cyberterroryzm państwowy i niepaństwowy – początki, skutki i formy*, Gdańsk 2009.

Littlejohn Skinder D., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci?*, Gliwice 2005.

Luterek M., *e-Government. Systemy informacji publicznej*, Warszawa 2010.

Maciejewski R., *Cyberterroryzm w polityce bezpieczeństwa państwa. Problemy ochrony infrastruktury krytycznej*, Poznań 2019.

Ney B., *Geoinformacja w społeczeństwie informacyjnym*, „Roczniki Geomatyki" 2005, tom III, zeszyt 3.

Pączkowski T., *Słownik cyberbezpieczeństwa*, Katowice 2017.

Podraza A., Polakowski P., Wiak K., *Cyberterroryzm zagrożeniem XXI wieku*, Warszawa 2013.

Rada Unii Europejskiej, Sprawozdanie oceniające z siódmej rundy wzajemnych ocen poświęconej praktycznemu wdrożeniu i funkcjonowaniu europejskich polityk w dziedzinie zapobiegania cyberprzestępczości i jej zwalczania – Polska, Bruksela 2017.

Radoniewicz F., *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w Działaniu. Sprawy Karne" 2013, nr 13.

Sienkiewicz P., Nowak J.S. (red.), *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*, Katowice 2008.

Siwicki M., *Cyberprzestępczość*, Warszawa 2013.

Słownik języka polskiego, Warszawa 2002.

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

Tomaszek K., *Stalker – psychologiczna charakterystyka sprawców przestępstw „uporczywego nękania"*, „Studia z Psychologii w KUL" 2012, t. 18.

Ustawa z dnia 29 sierpnia 2002 roku o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (tekst jedn. Dz.U. z 2017 r., poz. 1932).

Ustawa z dnia 6 czerwca 1997 roku – Kodeks karny (tekst jedn. Dz.U. z 2020 r., poz. 1517, ze zm.).

Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.

Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń", Komisja Europejska.