PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2018, t. VI, s. 421–431

http://dx.doi.org/10.16926/tiib.2018.06.30

Henryk Noga[1], Zbigniew Małodobry[2], Joanna Jarczak[3]
[1]*Uniwersytet Pedagogiczny im. KEN w Krakowie*
ul. Podchorążych 2, 30–084 Kraków
[2]*Państwowa Wyższa Szkoła Zawodowa*
im. rtm. Witolda Pileckiego w Oświęcimiu
ul. M. Kolbego 8, 32–600 Oświęcim
[3]*Akademia Ignatianum w Krakowie*
ul. M. Kopernika 26, 31–501 Kraków

CYBERPRZESTRZEŃ WSPÓŁCZESNYM MIEJSCEM PRZESTĘPSTWA

Streszczenie. Od drugiej dekady XXI wieku do chwili obecnej obserwujemy ciągły rozwój sieci komputerowej. Towarzyszą temu zagrożenia różnego typu przestępczością. W opracowaniu ukazano terminy i wyrażenia związane z cyberprzestępczością oraz wskazano na możliwości związane z występowaniem przestępstw i przeciwdziałaniem im w przestrzeni internetowej. Przytoczono również terminologię związaną z cyberterroryzmem i cyberbezpieczeństwem, która dotychczas nie została wprowadzona do przepisów międzynarodowych jako ogólnie akceptowalna. Zwrócono także uwagę, że nie można pominąć ograniczeń i braku kontroli nad nowymi technologiami i możliwościami Internetu dla przeciętnego użytkownika.
Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, zagrożenie, terroryzm, infrastruktura internetowa, świadomość odbiorców, ochrona prywatności, bezpieczeństwo informatyczne i informacyjne.

CYBERSPACE IS A MODERN CRIME SCENE

Abstract. From the second decade of the 21st century to the present, we observe the continuous development of the computer network. This is accompanied by threats of various types of crime. The paper presents terms and expressions related to cybercrime and indicates the possibilities related to the occurrence and counteracting of crimes in the Internet space. The terminology related to cyberterrorism and cybersecurity was also cited, which has not been introduced into international regulations as generally accepta-

ble. It was also pointed out that the limitations and lack of control over new technologies and Internet possibilities for the average user can not be overlooked.
Keywords: cyberspace, cybersecurity, threat, terrorism, Internet infrastructure, audience awareness, privacy protection, IT and information security.

Wprowadzenie

W dzisiejszych czasach wyzwaniem staje się zapewnienie bezpieczeństwa i ochrony informacji, ponieważ bezpieczeństwo informacyjne stanowiące dobro wyższe dla całego społeczeństwa jest trudne do osiągnięcia w obliczu wojen cybernetycznych i terroryzmu cybernetycznego. Definicji terminu *cyberbezpieczeństwo* jest wiele, uzależnione są one od osób, które tym słowem się posługują. Przede wszystkim definiować mogą ten termin pojedynczy użytkownicy internetu oraz całe przedsiębiorstwa korzystające z bogatszej infrastruktury w tym zakresie. Jednak to państwo wyznacza zadania i podejmuje działania dotyczące obrony swoich obywateli w cyberprzestrzeni przed zagrożeniami i atakami cyberterroryzmu [3]. W XXI wieku fenomenem o najbardziej rozbudowanej złożoności jest właśnie bezpieczeństwo informatyczne, zawierające takie elementy, jak: świadomość odbiorców, ochrona prywatności, zarządzanie dostępem do danych itp. Stały i nieograniczony dostęp do internetu oraz technologii informacyjnych jest obecnie nieodłącznym elementem życia każdego człowieka z osobna oraz całych grup i populacji, definiuje on współczesne społeczeństwo jako społeczeństwo informacyjne.

Możliwości cyberprzestrzeni

Dzisiejsze możliwości rozwoju cyberprzestrzeni stawiają ustawodawcom nie tylko krajowym, lecz również międzynarodowym, liczne wyzwania [3]. Historia internetu sięga przełomu lat 60. i 70. XX wieku. W latach 90. XX wieku rozpoczął się niekontrolowany rozwój sfery związanej z internetem. Spowodowany był wprowadzeniem nowego rodzaju usług dostępnych dotychczas jedynie w sferze podstawowego wymieniania, takich jak np. usługi pocztowe, które do lat 90. polegały na obsłudze indywidualnej w punkcie obsługi, tzn. w budynkach. W latach 90. ubiegłego wieku powstały poczty elektroniczne, przedsiębiorstwa za pośrednictwem stron internetowych rozpoczęły ekspansję na nowe rynki sprzedażowe, a sieci społecznościowe, np. Facebook, połączyły społeczeństwa z różnych kontynentów. Cyberprzestrzeń w XXI wieku jest określeniem transgranicznym, i jako taka potrzebuje regulacji ogólnonarodowych [2]. Początkowe cele badawcze i edukacyjne z biegiem czasu ewoluowały, a cyberprzestrzeń osiągnęła wymiar międzynarodowego nośnika informa-

cji, co wymagało już wprowadzenia nowych zabezpieczeń, ponieważ wzrosła liczba możliwych zagrożeń cyberprzestępczością. W krajach europejskich do lat 90. XX wieku nie było odpowiednich ustaw i regulacji prawnych mogących skutecznie zapewnić bezpieczeństwo różnego rodzaju użytkownikom. A trzeba sobie zdać sprawę, że w XXI wieku użytkownicy ci to już ogólnoświatowe społeczeństwa, przedsiębiorstwa i nawet całe państwa opierające swoje istnienie na sieci informatycznej. Obecnie dostęp do internetu, do różnego rodzaju usług i możliwości jest nieograniczony, a co za tym idzie, sfera zabezpieczeń również powinna podążać za tym rozwojem.

Bezpieczeństwo w wirtualnej rzeczywistości

Stosowanie dotychczas znanych rozwiązań w zakresie zabezpieczeń okazuje się dziś niewystarczające, i na dodatek całkowitej gwarancji bezpieczeństwa w taki sposób nie uda się osiągnąć [3]. Współpraca wielu krajów w tym aspekcie jest cały czas aktualna i ciągle aktualizowane są formy zabezpieczeń. Stosuje się różnego rodzaju zapory, programy itp., jednakże nie zawsze okazują się one wystarczające. Międzynarodowy charakter zjawiska, jakim jest internet nałożył na ustawodawców obowiązek wprowadzenia odpowiednich regulacji prawno-karnych. Obowiązek ten jest utrudniony przez rodzaj tego zjawiska, które nie posiada granic, a stwarza realne zagrożenie nie tylko w świecie wirtualnym, lecz również w pozawirtualnym [4]. Badania statystyczne prowadzone już od końca lat 90. ubiegłego wieku potwierdzają przerażającą i ciągle zwiększającą się liczbę nie tylko samych przestępstw w cyberprzestrzeni, ale również ich coraz to nowszych rodzajów. Od początku XXI wieku wprowadzono wiele nowatorskich inicjatyw dotyczących koniecznych szkoleń profilowanych, masowych kursów i specjalistycznych badań opinii publicznej dotyczących udogodnień i możliwości, jakie daje obecny, łatwy dostęp do internetu i treści w nim zawartych [2]. Dziś każda osoba z osobna przestała być anonimową liczbą statystyczną, bowiem sami bez zastanowienia udostępniamy, nie tylko innym ludziom, lecz również każdej z instytucji, w tym również przestępcom, dane osobowe, mogące w znaczący sposób narazić nas i nasze otoczenie na atak. Wraz z rozwojem społeczeństwa informacyjnego oraz rozszerzaniem zasięgu internetu postępuje również widoczne i celowe przenikanie i przejmowanie przez sferę internetu kolejnych aspektów działania i działalności człowieka. Dostęp do takich usług, jak zakupy online, poczta elektroniczna, czy też bankowość elektroniczna w dzisiejszych czasach jest czymś całkowicie normalnym, tzn nikt nie jest w stanie wyobrazić sobie cofnięcia się do rzeczywistości lat 80. ubiegłego wieku, gdzie te wszystkie usługi dostępne były jedynie w wyspecjalizowanych punktach. Na poczcie lub w okienku kasowym banku doko-

nywało się płatności za rachunki, teraz większość osób korzysta z tych usług przez odpowiednie strony internetowe [2]. Dostęp do internetu mamy teraz już nie tylko przez komputery, ponieważ cyfryzacja rośnie w tym samym tempie, co zwiększające się możliwości internetu. Postęp geometryczny, z jakim można mierzyć możliwości obecnego internetu wiąże się również z postępem, wzrostem przestępstw. Dostęp do internetu mamy również przez smartfony, tablety, samochody i innego rodzaju gadżety, które stały się przede wszystkim synonimem niczym nieograniczonego przepływu informacji i wolności słowa, tym samym stały się również narzędziem władzy mogącej wprowadzać rewolucje i zmiany społeczne na skale międzynarodową. Różne formy ludzkiej działalności te pozytywne, jak i negatywne są odzwierciedlane w wirtualnej rzeczywistości, przez ogólne poczucie anonimowości wykorzystujemy również świat internetu do swoich tzw. osobistych, nie zawsze zgodnych z prawem, celów [4]. Pewne firmy specjalistyczne zajmujące się badaniem zjawiska zwanego teraz cyberprzestępczością, stwierdzają w swoich raportach, że działalność cyberprzestępców w czasach dzisiejszych jest porównywalnie tak samo wysoka jak działalność przestępców w świecie niewirtualnym, a straty powstałe w wyniku takich działań są przeliczane na miliardy dolarów w skali roku. Wraz z rozwojem możliwości, które daje internet, wzrasta również słownik pojęć i terminów związanych z tego rodzaju działalnością. Większość tych terminów jest zaczerpnięta z terminologii amerykańskiej, np. od słowa *hate* w terminologii współczesnego internauty pojawiło się słowo *hejter* określające osobę, która w ciężkich, czasem również niekulturalnych słowach wypowiada się o innej osobie lub innym aspekcie [4].

Przestępstwa w „sieci”

Jak wynika z raportów firm specjalistycznych, prawie połowa użytkowników internetu, którzy padli ofiarą cyberprzestępstwa, jest winna sama sobie. Przez nieuwagę lub niedokładne sprawdzenie udostępnianych publicznie prywatnych danych internauci ci stali się ofiarami przestępstw. Głównym motywem działań przestępców ze sfery wirtualnej jest chęć zysku, co jest tym samym motywem, jakim kierują się przestępcy w świecie realnym. Pamiętać należy, że ogromna ilość przestępstw występujących w cyberprzestrzeni nadal znajduje się w szarej strefie, a tym samym nie jest brana pod uwagę w trakcie tworzenia tabel statystycznych [7]. Przestępstwa popełniane w cyberprzestrzeni posiadają charakterystyczny i niepowtarzalny profil, co czyni je często trudnymi do zidentyfikowania lub wykrycia. Podstawowymi powodami takiego stanu rzeczy są sami użytkownicy, którzy nie są w posiadaniu odpowiednich informacji, tzn. nie są świadomymi użytkownikami, jak również ich braki w odpowied-

nich i aktualizowanych programach zabezpieczających wrażliwe dane prywatne. Wszelkie słabości cyberprzestrzeni są współcześnie wykorzystywane przez cyberprzestępców do taniego, szybkiego i prawie niewykrywalnego zarobku. Stanowią tym samym siłę napędową tych rodzajów działalności. Terminologia związana z cyberprzestępczością i cyberprzestrzenią nie została jeszcze dokładnie zdefiniowana, tym samym nie została również umieszczona w regulacjach prawno-karnych dotyczących tej działalności [7]. Wymaga się jednakże od międzynarodowych i krajowych ustawodawców, w celu usprawnienia działania prawa i zapewnienia skutecznego zwalczania zagrożeń w cyberprzestrzeni, prowadzenia szczegółowych analiz i badań dotyczących cyberprzestępczości, a tym samym ujednolicenia terminologii w skali międzynarodowej. Zwalczanie nowoczesnych form przestępczości internetowej i komputerowej na dzień dzisiejszy nie jest oparte na odpowiednich rozwiązaniach prawnych, a powodem takiej sytuacji jest niechęć lub niezdolność określenia wspólnych stanowisk poszczególnych krajów. Terminologia i pojęcia stosowane i używane w piśmiennictwie są uważane za terminologię bardziej publicystyczną niż naukową, dającą zbyt szerokie możliwości coraz to nowszym grupom przestępczym [7]. Autor stwierdza również, że dotychczasowe pojęcia i definicje tworzone są bez zastanowienia, na gorąco, często krzyżują się znaczeniowo, a powodem tego są ustawiczne zmiany rozwojowe nowoczesnych technologii, stanowiące podstawowy budulec cyberprzestrzeni. A. Adamski określa również, że według prawa karnego materialnego wyróżnia się dwa rodzaje przestępstw związanych z komputerem: jedno z nich to przestępstwo przy użyciu komputera, tzn. to komputer jest narzędziem przestępstwa, a drugie to sytuacja, w której następuje zamach na systemy, dane lub programy komputerowe [1]. Przez kilka lat polscy ustawodawcy wprowadzali nowelizacje do Kodeksu karnego uchwalonego 6 czerwca 1997 roku tak, aby nowe regulacje dopasować do nowego rodzaju popełnianych przestępstw. Spopularyzowanie szerokiego dostępu do Internetu przy możliwości zachowania anonimowości oraz możliwość popełniania przestępstw na terenie innego kraju stały się początkiem nowego rodzaju przestępczości prowadzonej zarówno przez osoby indywidualne, jak i całe grupy. Ich działalność zwana jest cyberprzestępczością. Najpopularniejszymi rodzajami przestępstw internetowych są w obecnych czasach oszustwa z wykorzystaniem elektronicznych instrumentów płatniczych, przede wszystkim chodzi o pozyskiwanie wrażliwych danych, takich jak hasła, loginy, numery pesel i piny. Pozyskanie tego typu danych umożliwia przestępcom wiele różnego rodzaju przestępstw, np. przelanie wszystkich środków finansowych z konta jednego użytkownika na konto przestępcy, bez możliwości namierzenia tego przestępcy. Przestępca będący w posiadaniu danych użytkownika internetu może na jego konto zaciągać pożyczki, do których spłaty zostaje zobowiązany użytkownik [7]. Sprawy sądowe dotyczące wyjaśnienia takich sytuacji ciągną się bardzo długo, jednakże spłata zaciągniętych w ten sposób długów nie zosta-

je wstrzymana, tym samym użytkownik ponosi podwójne koszty (zapłata za zaciągnięty dług oraz koszty sądowe). Groźnym rodzajem przestępstwa staje się również pornografia, rozsyłana i rozpowszechniania za pośrednictwem internetu, nie tylko dotycząca osób dorosłych, lecz przede wszystkim dzieci. Osoby posiadające skłonności pedofilskie bardzo często pozyskują i rozpowszechniają treści i materiały zawierające pornografię dziecięcą oraz nawiązują kontakty z małoletnimi w celach seksualnych. Osoby takie wykorzystują wiele różnych sposobów w celu przyciągnięcia uwagi małoletniego, np. na współczucie, obrażanie szkoły i nauczycieli itp. [7]. Nieuświadomieni małoletni bardzo często ulegają wpływom pedofili, a rodzice małoletnich nieświadomi rozpoczęcia kontaktów swoich pociech z osobą nieodpowiednią lub nawet groźną, nie są w stanie w odpowiednim momencie skutecznie zareagować, tym samym bardzo często dochodzi do przestępstw na tle seksualnym dokonywanych przez osoby posiadające skłonności pedofilskie. Często również ofiary takich ataków przez wstyd i bezradność nie informują osób dorosłych o takich sytuacjach lub takich próbach, w ten sposób lista potencjalnych przestępców nie jest aktualna i pełna. Do codzienności cyberprzestępstw należy już zaliczyć handel nielegalnymi towarami akcyzowymi, bezprawne pobieranie i rozpowszechnianie filmów, gier, muzyki, oprogramowania. Do najświeższych nowo powstałych rodzajów przestępstw internetowych należy sprzedaż nielegalnych środków odurzających nazywanych często błędnie dopalaczami. Grupy przestępcze specjalizują się w wymuszaniu oraz stosowaniu gróźb karalnych w stosunku do przedsiębiorstw. Przestępcy uzyskują dostęp do wrażliwych danych lub bardzo skutecznie ograniczają przedsiębiorstwu możliwość działania poprzez wprowadzenie złośliwego oprogramowania. Cyberterroryzmem określa się planowane, dokonywane i koordynowane w cyberprzestrzeni działania związane z używaniem sieci komputerowej w celu utrzymywania łączności między terrorystami lub też w celu dzielenia się informacjami mogącymi posłużyć do ataku terrorystycznego [5]. We współczesnym świecie elektronika jest głównym źródłem wszystkich informacji i wpływa bezpośrednio i pośrednio na wszystkie sfery ludzkiego życia. To komputery bowiem zbierają, wytwarzają, gromadzą i przesyłają informacje wykorzystywane we wszystkich dziedzinach, takich jak: szkolnictwo, nauka, bezpieczeństwo, handel, obronność kraju, transport, finanse, ochrona zdrowia, sport itd. Komputery i internet tworzą współcześnie jedną wielką globalną infrastrukturę, która funkcjonuje w cyberprzestrzeni i jest w posiadaniu danych i systemów, które są kluczowymi czynnikami dla wielu dziedzin ludzkiego życia. Dzisiaj internet nie ma żadnych granic, ponieważ możliwości, jakie daje użytkownikom, to również możliwość skutecznego usunięcia lub ukrycia dowodów popełnionego przestępstwa, pozwalająca przestępcom na osiągnięcie zamierzonych celów niskim kosztem oraz nagłymi i niemożliwymi do przewidzenia atakami [5]. Wielu użytkowników internetu nie jest świadomych, że stali się ofiarami przestępstw. To uświadomienie przychodzi bardzo

późno, a skutki bycia ofiarą takiego przestępstwa mogą być bardzo różnorakie. Analizując opinie na temat portali społecznościowych, bardzo często napotyka się na opisy wręcz dramatycznych sytuacji, w których użytkownik lub dana grupa użytkowników stali się ofiarami ataku, a w konsekwencji ostracyzmu społecznościowego zdecydowali się na ucieczki lub zastosowanie nawet bardziej dramatycznych rozwiązań, jak np. samobójstwo. Z powodu ostracyzmu społecznościowego największą liczbę ofiar odnotowywuje się u małoletnich, gdzie średnia wieku to 11–15 lat. Wiek ten jest bardzo trudny, ponieważ dzieci wchodzą wtedy w okres dojrzewania, a zmiany zachodzące w ciele i na ciele mogą powodować u rówieśników brak akceptacji oraz ataki. W czasach przed rozpowszechnieniem dostępu do internetu takich ataków nie odnotowywano, bowiem miały one charakter bardzo zawężony, tzn. do danej grupy rówieśniczej, do danej miejscowości, więc ich rozpowszechnienie nie mogło być tak skuteczne jak w dzisiejszych czasach. Fenomenem nowoczesnej przestępczości są systemy teleinformatyczne oraz sieci, które mogą służyć przede wszystkim do popełniania tradycyjnych przestępstw, takich jak oszustwo lub zniewaga, ale mogą służyć również w przestępstwach takich, które pojawiły się dopiero wraz z rozpowszechnieniem się cyberprzestrzeni, np. przechwytywanie transmisji, kradzież zasobów informatycznych i baz danych [5]. Gospodarki na całym świecie już od pół wieku mierzą się ze wzrastającą falą przestępstw w cyberprzestrzeni. Straty poniesione w wyniku cyberprzestępczości liczone są już nie w milionach, lecz w miliardach dolarów w skali globalnej. Niezwykle trudnym jest określenie skali zjawiska cyberprzestępczości, ponieważ wykracza ono ponad możliwości poznawcze kryminologii w Polsce. Związane jest to również z faktem nieposiadania wystarczających i odpowiednich mechanizmów dotyczących gromadzenia danych, tym samym wszystkie dane zebrane stanowią jedynie ułamek faktycznej skali zjawiska [5]. Przyczyną takiego stanu rzeczy jest w pierwszej kolejności ogromna problematyczność definicyjna, co przekłada się na problemy funkcjonariuszy policji i organów ścigania co do prawidłowego zakwalifikowania prawnego danego przestępstwa. Dotychczas znane metody i sposoby poszukiwania sprawców przestępstw w odniesieniu do cyberprzestrzeni nie mogą zostać zastosowane, a zmienność i ciągła ewolucja rodzajów przestępstw związanych z infrastrukturą internetową jeszcze bardziej utrudniają pracę funkcjonariuszy policji, tym samym utrudniając im złapanie i ukaranie sprawcy przestępstwa w odpowiedni sposób, opisany w Kodeksie karnym. W dzisiejszych czasach łatwiej stać się ofiarą cyberprzestępstwa niż pospolitego przestępstwa, np. kradzieży portfela. Nie oznacza to jednak, że pospolite przestępstwa nie występują, one nadal się pojawiają, tylko ich liczba nie rośnie tak szybko i z taką prędkością jak liczba przestępstw związanych z cyberprzestrzenią [5]. Na fakt ten mają również wpływ otwarte granice państwowe w Europie oraz ogromna możliwość anonimowości i ukrycia się przed odpowiedzialnością, także karną. W przypadku pospolitego przestępstwa prę-

dzej czy później jakieś fakty, dane, ślady itp. wskażą przestępcę, w przypadku zaś przestępcy poruszającego się w cyberprzestrzeni i posiadającego odpowiednią wiedzę i technologię, jego wykrycie jest bardzo utrudnione. Najbardziej popularnym rodzajem przestępstwa w cyberprzestrzeni jest obecnie tworzenie tzw. botów [5]. Bot jest to program, który usuwa wszystkie informacje z komputera użytkownika, umożliwiając tym samym przejęcie go przez sprawcę przestępstwa i pozyskanie wrażliwych danych, które w późniejszym czasie mogą posłużyć do innych przestępstw z użyciem tych danych. Boty są to programy, które wpuszczone do sieci krążą sobie swobodnie i wyszukują komputery o słabej formie zabezpieczeń (w tym również słabo zabezpieczone komputery w przedsiębiorstwach) lub komputery w ogóle nie posiadające zabezpieczeń. Są to tzw. wirusy komputerowe, przed którymi bronić użytkowników powinny odpowiednio skonstruowane programy antywirusowe. Niestety, jak pokazują niechlubne statystyki, twórcy takich wirusów posiadają większe zasoby finansowe, a co za tym idzie, również technologiczne, co przekłada się na fakt, że większość programów antywirusowych już w momencie zaistnienia na rynku można określić jako przestarzałe i niewystarczające [4]. Tworzenie bowiem programów antywirusowych opiera się w głównej mierze na analizie już istniejących zagrożeń, tym samym jakakolwiek zmiana i unowocześnienie wirusa powoduje, że dopiero co stworzony program mający przeciwdziałać takim zagrożeniom staje się bezużyteczny. Portale społecznościowe, takie jak Facebook, Instagram, Tweeter również mają w swoich statystykach zapisane próby ataków, bowiem cyberprzestępcy, tworząc bardzo podobne do oryginalnych stron odsyłacze powodowali, że użytkownicy tych portali nieświadomie i nieodpowiednim osobom podawali swoje wrażliwe dane. Firmy zajmujące się na co dzień opracowywaniem programów antywirusowych i innych mających zabezpieczać użytkowników przed atakami ze strony cyberprzestępców również są w podobny sposób wykorzystywane. W XXI wieku większość osób przyzwyczaiła się do korzystania ze smartfonów, które także umożliwiają stały dostęp do sieci internetowej, do portali społecznościowych, do usług finansowych itp., tym samym one również stały się celem ataków przestępców. Na fakt ogromnego przyrostu liczby ataków cyberprzestępców ma przede wszystkim wpływ niekontrolowane i nieświadome podawanie wrażliwych danych w momencie pobierania aplikacji na telefon mających ułatwić życie użytkownikowi [3]. Jak wynika z przeprowadzonych ankiet, ¼ użytkowników przyznaje się do niesprawdzania przekazywanych informacji podczas pobierania aplikacji, a ponad połowa ankietowanych wręcz świadomie przekazałaby swoje wrażliwe dane w zamian za uzyskanie dostępu do *darmowych* lub *w promocyjnej cenie* możliwości skorzystania z interesujących propozycji [1].

Ryzyko funkcjonowania w cyberprzestrzeni

Straty finansowe kraju związane z nielegalnym handlem za pośrednictwem internetu, lub sprzedażą nielicencjonowanych produktów są ogromne. Powiększająca się liczba sprzedawców oferujących nie tylko swoje produkty, lecz również usługi w internecie w konkurencyjnych cenach w stosunku do rynku tradycyjnego powoduje wzrost liczby transakcji dokonywanych właśnie drogą elektroniczną [2]. Nabywcy są świadomi ryzyka związanego z możliwością stania się ofiarą przestępstwa, a niejednokrotnie robią to świadomie, np. rynek muzyczny funkcjonujący w Polsce szacuje, że w wyniku piractwa i nielegalnego udostępniania treści traci co roku wiele milionów dolarów. Straty te muszą się przełożyć na wzrost cen towarów i usług dostępnych na rynku rzeczywistym (nie wirtualnym). Nabywca, mając do wyboru zakup towaru lub usługi w korzystniejszej cenie, godzi się na ryzyko związane z przestępstwem, nawet ze świadomością, że czyniąc tak, sam staje się przestępcą. Zakup oprogramowań komputerowych w cenach rynku rzeczywistego jest możliwy i w większości realizowany przez przedsiębiorstwa, które przez przepisy prawa polskiego są zmuszone do takiego zakupu. Osoby prywatne lub zwykli użytkownicy, nie czując presji prawa karnego, korzystają z możliwości, jakie daje im dostęp do nieograniczonego zasobu internetowych towarów i usług. W obecnych czasach zakupy internetowe, nawet z dalekiej zagranicy, np. z Chin, wychodzą w przeliczeniu na krajową walutę dużo taniej niż zakupy tych samym produktów na rynku rzeczywistym [6]. Niejednokrotnie sami przedsiębiorcy, jeśli tylko mogą, korzystają z *promocyjnych* ofert z zagranicy, a towar zakupiony w promocyjnych cenach sprzedają na rynku krajowym z dużo większą marżą, czym powodują kolejne straty finansowe dla skarbu państwa. Do niepokojących wniosków dochodzi się, patrząc na analizy statystyczne, gdzie aż 75% populacji ankietowanych przyznaje się otwarcie do korzystania z nielegalnego oprogramowania lub zakupu podrobionych towarów w celu zaoszczędzenia pieniędzy. Faktem staje się to, że niedostateczna wiedza użytkowników internetu na temat zagrożeń i możliwości popełnienia przestępstwa jest najważniejszym problemem, z jakim musi zmierzyć się każde państwo, aby w przyszłości ograniczyć straty finansowe. Określenie konkretnego użytkownika będącego przestępcą internetowym lub też grupy takich osób jest trudne, ponieważ do szeregu użytkowników należy również dopisać dostawców tych usług, którzy pomimo posiadania możliwości monitorowania wykonywanych czynności na udostępnionych serwerach, nie robią tego z przyczyn prozaicznych – finansowych. Ponieważ za udostępnienie miejsca na serwerze użytkownik musi zapłacić, jednocześnie podpisując zobowiązanie, że na udostępnionym miejscu nie będzie publikował niczego o charakterze wykraczającym poza przepisy prawa lub mogącym przyczynić się do popełnienia przestępstwa. W Kodeksie karnym obecne nowelizacje pozwalają również ścigać usługodawców, którzy

nie kontrolują swoich klientów, a tym samym wyrażają niemą zgodę na popełnienie przestępstwa [1]. Strony pośredniczące w wymianie informacji są odpowiedzialne za upowszechnione materiały jedynie w sytuacji, gdy posiadają odpowiednią wiedzę o charakterze przechowywanych lub udostępnianych treści oraz jeśli posiadają rzeczywistą możliwość techniczną usunięcia tych treści. Tym samym nie do każdego usługodawcy da się zastosować w praktyce reguły ogólne, niejednokrotnie wymaga to bardzo wielu godzin pracy analityków i prawników. Ofiarami przestępstw internetowych mogą stać się również instytucje publiczne, które w sytuacji wykrycia u siebie takiego ataku z powodu posiadania np. niewystarczającego lub niezgodnego z obowiązującym prawem oprogramowania nie informują użytkowników o tym, aby w pierwszej kolejności nie zawieść zaufania klientów lub też, w drugiej kolejności, uniknąć wielomilionowych odszkodowań. W takich sytuacjach często instytucje, takie jak np. banki, swoje uchybienia w kwestii posiadania odpowiednich zabezpieczeń zrzucają na osoby trzecie, aby uniknąć odpowiedzialności.

Podsumowanie

Powstrzymanie nielegalnego wykorzystywania Internetu nie może opierać się jedynie na poszukiwaniu nowych środków zapobiegania cyberprzestępczości [3]. Przestępcy wykorzystują fakt złożoności zjawiska cyberprzestępczości oraz jego charakter transgraniczny. W celu zmniejszenia występowania przestępstw związanych z internetem należy w większym stopniu skupić się na uświadamianiu użytkowników internetu, a przede wszystkim na uświadamianiu usługodawców dostępu do internetu, o szkodliwości ich działań wynikających z zaniechania lub z tzw. przymykania oczu na fakt łamania przepisów prawa. Wszyscy użytkownicy internetu, zarówno usługodawcy, jak i odbiorcy pośredni i bezpośredni, muszą być informowani na bieżąco, na jakie straty narażają państwo oraz na jak ogromne ryzyko narażają się sami. W opinii M. Siwickiego, większy i lepszy skutek może przynieść uświadamianie korzystających z internetu niż zastraszanie represjami karnymi.

Od dnia 25 maja 2018 roku wchodzą w życie przepisy dotyczące ochrony danych osobowych kandydatów do pracy i pracowników, które do tej pory były określone w Kodeksie pracy oraz ustawie o ochronie danych osobowych [3]. Wiele podmiotów będących w posiadaniu takich danych zostało zobowiązanych do przygotowania i przeprowadzenia audytów przygotowawczych mających na celu przedstawienie, jakie dane osobowe są przetwarzane, skąd te dane pochodzą, jakie uprawnienia są związane z tymi danymi, czy dane te są lub będą komuś udostępniane oraz w jaki sposób są one zabezpieczone przed wyciekiem. Audyt taki ma przygotować rejestr czynności przetwarzania takich danych, aby

w przyszłości móc w prosty i szybki sposób odpowiedzieć na pytanie czy podmiot będący w posiadaniu wrażliwych danych był sprawcą czy też ofiarą cyberprzestępstwa [3].

Literatura

[1] Adamski A., Prawo karne komputerowe, Warszawa 2000
[2] Grzelak M., Liedel K., Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu,[w:] Kwartalnik Bezpieczeństwo Narodowe, nr 22, 02.2012, Biuro Bezpieczeństwa Narodowego, Warszawa 2012.
[3] Jaroszewska I., Wybrane aspekty przestępczości w cyberprzestrzeni, [w:] KPP. Monografie. Studium prawnokarne i kryminologiczne, Olsztyn 2017.
[4] Kulesza J., Międzynarodowe Prawo Internetu, Poznań 2010.
[5] Siwicki M., Cyberprzestępczość, Warszawa 2013, s. 47–48.
[6] Siwicki M., Nielegalna i szkodliwa treść w Internecie. Aspekty prawo karne, wyd. Wolters Kluwer Polska, Warszawa 2011, s. 258–259.
[7] http://prawo.vagla.pl/node/905, Przestępczość w Internecie. Zagadnienia podstawowe (data dostępu: 4.05.2018).
[8] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf, Symantec: Internet Security Threat Raport 2014 [on-line], Volume 19 (data dostępu: 4.05.2018).