UNIWERSYTET WARSZAWSKI

WYDZIAŁ PRAWA I ADMINISTRACJI

MARCIN KAROLEWSKI

Przestępstwa przeciwko ochronie informacji w Kodeksie Karnym z 1997 r. ze szczególnym uwzględnieniem art. 267 § 1 jako przepisu kryminalizującego „hacking" na tle unormowań Rady Europy

Praca magisterska
napisana w Zakładzie Prawa Karnego Porównawczego
pod kierownictwem dr Anny Walczak - Żochowskiej

WARSZAWA 2005

Na świecie jest 10 rodzajów ludzi
– ci, którzy rozumieją kod binarny
i ci, którzy go nie rozumieją;

W podziękowaniu

Bliskim –
za pomoc i wyrozumiałość;

środowisku –
za to, że jest i działa;

Abstrakt

Praca stanowi analizę polskich przepisów karnych, dotyczących ochrony informacji i zawartych w Rozdziale XXXIII Kodeksu Karnego z 1997 r.i porównanie krajowych rozwiązań z obowiązującymi unormowaniami Rady Europy. Szczególny nacisk został położony na istotę i prawnokarną regulację zachowania przestępczego zwanego potocznie „hackingiem".

Tytułem wprowadzenia do właściwej materii pracy omówiłem genezę powstania obecnego systemu społeczno – ekonomicznego oraz przybliżyłem charakter środowiska, w jakim zjawisko „przestępczości komputerowej" zachodzi.

Słowa kluczowe

Prawo karne – ochrona informacji – przestępczość komputerowa – hacking – Kodeks Karny - Cyberprzestępczość

Spis treści

Wstęp

Założeniem niniejszej pracy było dokonanie przeglądu przygotowania polskiego prawa karnego do konfrontacji ze zjawiskiem rosnącej przestępczości komputerowej (ze szczególnym uwzględnieniem przestępstwa „hackingu") w dobie lawinowej informatyzacji życia codziennego.

Rozwój ów jest czynnikiem, który przeniósł ciężar rozważań i analizy zjawiska przestępczości komputerowej z płaszczyzny *stricte* teoretycznej na praktyczną – tzw. Rewolucja Informacyjna stała się faktem, a powszechna komputeryzacja i tworzenie się społeczeństwa informacyjnego stworzyły swoistą niszę ekologiczną dla czynów niezgodnych z prawem, dotychczas nieznanych, popełnianych z zastosowaniem zaawansowanej technologii lub przeciw niej – przestępczości komputerowej.

Komputery wdarły się przebojem w każdą dziedzinę życia – usprawniają funkcjonowanie np. wszelakiego rodzaju komunikacji, telekomunikacji, energetyki. Tam, gdzie nie zastosowano ich w praktyce, istnieją teoretyczne podstawy ich wykorzystania. Powstanie i dynamiczny rozwój ogólnoświatowej otwartej sieci zwanej Internetem przyniosło początek elektronicznego handlu i bankowości (e-commerce, e-banking), przeżywające obecnie burzliwy rozkwit. Naturalną koleją rzeczy było powstanie kategorii czynów przestępnych, przystosowanych do egzystencji w tym specyficznym środowisku. Każda innowacja niesie ze sobą problem nowych zagrożeń – tych dotychczas nieznanych oraz istniejących, lecz w nowej postaci, przygotowanych do istnienia w nowych warunkach.

Samo pojęcie „przestępstw komputerowych" jest bardzo szerokie i do tej pory, mimo podejmowanych licznych prób, brak jest jego pełnej, nie budzącej wątpliwości, definicji. Ten stan rzeczy spowodowany jest m.in. różnorodnością przestępstw, metod działań przestępnych, oraz przedmiotów przestępstw.

W pracy niniejszej postaram się przedstawić porównanie polskich przepisów karnych odnoszących się do „przestępstw komputerowych" z ustawodawstwem unijnym oraz z przepisami wybranych państw członkowskich Unii Europejskiej. Szczególną uwagę poświęciłem art. 267 § 1 KK jako przepisowi kryminalizującemu przestępstwo „hackingu".

W rozdziale pierwszym przedstawiłem genezę powstania społeczeństwa informacyjnego, począwszy od upowszechnienia się technologii informatycznej po lawinowy rozwój globalnej sieci, uwzględniając jednocześnie początki wykorzystywania tej technologii w celach kolidujących z prawem. Rozdział drugi poświęcony jest w całości problematyce „przestępczości komputerowej" i obejmuje zarówno podsumowanie podjętych do-

tychczas prób zdefiniowania zjawiska, opis technik stosowanych przez sprawców i sposobów mających na celu zabezpieczenie się przed nimi, jak i przedstawienie skali zjawiska oraz kwestii problemów, jakie napotyka ściganie czynów należących do tej kategorii. Rozdział trzeci ma na celu przybliżenie zachowania określanego mianem „hackingu" i stanowi próbę odpowiedzi na pytanie czym jest to zachowanie, oraz kim, w związku z tym, jest „hacker". Zagadnienie powyższe jest istotne o tyle, iż stanowi punkt wyjścia do dalszych rozważań na temat stosunku nauk prawnych do tego zjawiska. W rozdziale czwartym zawarłem omówienie podstawowych standardów Rady Europy odnoszących się do szeroko rozumianej „ochrony informacji*"*. Treść rozdziału piątego stanowi omówienie problematyki „przestępczości komputerowej" pod kątem polskiej kodyfikacji karnej z 1997 r. Poza głównym przedmiotem analizy, jakim są uregulowania zawarte w przepisach rozdziału XXXIII Kodeksu Karnego – „Przestępstwa przeciwko ochronie informacji", przedstawię również regulacje znajdujące się w pozostałych częściach Kodeksu Karnego. Rozdział szósty poświęciłem w całości przestępstwu określanemu potocznie mianem „hackingu" – tak jego typizowaniu przez przepis art. 267 § 1 KK, także na tle regulacji przyjętej przez Konwencję o Cyberprzestępczości, jak i przez ustawodawstwa kilku wybranych państw członkowskich Unii Europejskiej. Tendencje rozwoju zjawiska „przestępczości komputerowej" oraz światowe i krajowe kierunki zmian w uregulowaniach prawnokarnych dotyczących tej materii omówiłem w rozdziale siódmym. Zakończenie pracy stanowią wnioski, jakie wyciągnąłem w trakcie analizowania przedstawionej materii.

Jak można zauważyć z powyższego przeglądu treści poszczególnych rozdziałów niniejszej pracy, wiele zagadnień zostało omówionych dość pobieżnie, niektóre wręcz celowo pominąłem (takie jak np. pozakodeksowe regulacje dotyczące materii „przestępczości komputerowej") starając się ustawić środek ciężkości na kodeksowej ochronie informacji.

W celu uniknięcia niejasności terminologicznych chciałbym zwrócić szczególną uwagę , iż jeden zwrot może być używany w kilku jego zakresach znaczeniowych, w zależności od kontekstu wypowiedzi. Najlepszym przykładem takiego stanu rzeczy może być pojęcie, które stanowi temat tej pracy, jako że poza znaczeniami, które nie charakteryzują zjawiska „hackingu" jako czynu przestępnego, także w regulacjach prawnych różnych krajów można spotkać odmienne interpretacje tego hasła. Skróty użyte w pracy wyjaśniłem bezpośrednio w tekście,

1. Rozdział I – Zagadnienia wprowadzające.

Społeczeństwo Informacyjne, o którego powstawaniu i rozwoju od kilku lat jest głośno, jest efektem Rewolucji Informacyjnej, której społeczności są elementem. Na samym początku pracy, traktującej o zjawisku „przestępczości komputerowej" i jego prawnej reglamentacji chciałbym, zanim przybliżę sam fenomen Rewolucji, zwrócić uwagę na rzecz na tyle istotną, iż w dalszych częściach pracy nastąpią do niej, bezpośrednie lub pośrednie, odwołania. Rewolucja Informatyczna to nic innego, jak współistnienie, na jednej płaszczyźnie, dwu elementów : elementu rozwoju technologii (błyskawicznego) oraz elementu rozwoju ludzkiej świadomości, która pozwala ludziom korzystać ze zdobyczy tejże Rewolucji. Oba warunki są niezbędne, ponieważ zachodzą pomiędzy nimi ścisłe relacje – właściwie istnienie każdego z tych elementów bez drugiego byłoby pozbawione sensu, jako że byt jednego z nich jest determinowany przez drugi. Technologia nie może rozwijać się bez ludzi, natomiast technika, z której ludzie nie potrafią korzystać, nie ma racji bytu we współczesnym, jakże utylitarnym, świecie.

1.1 Rozwój informatyki.

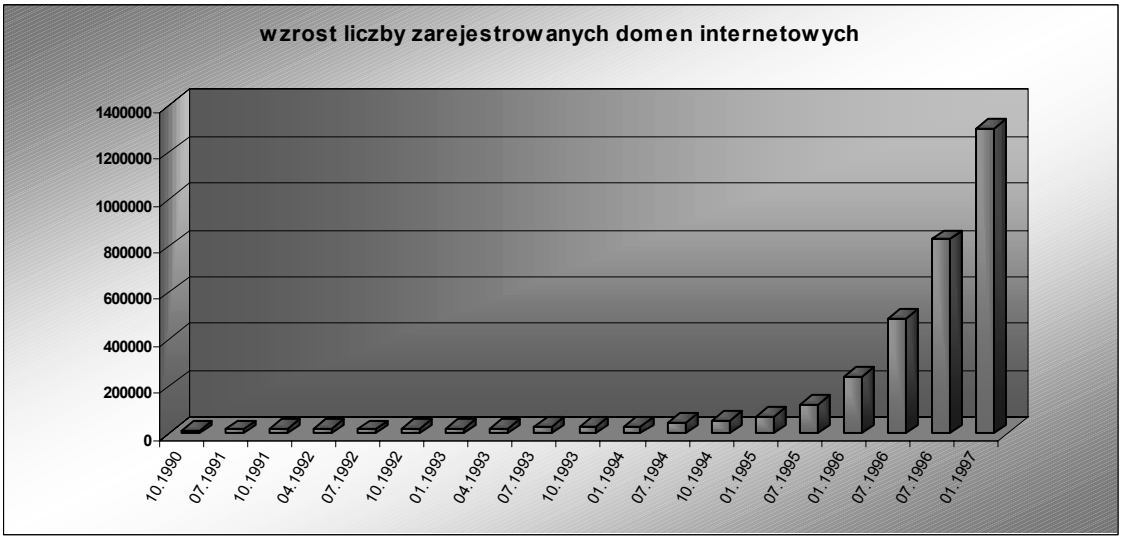
Rewolucja Informacyjna, której obecnie jesteśmy świadkami, (a pośrednio również i twórcami) ma bardzo krótką, w stosunku do ludzkiej cywilizacji, bo nawet nie sześćdziesięcioletnią, historię. Era elektronicznego przetwarzania danych rozpoczęła się w roku 1946, kiedy na uniwersytecie stanowym w Pensylwanii zbudowano pierwszą na świecie maszynę liczącą - ENIAC[1]. Ta ważąca 30 ton i zajmująca 170 m^2 powierzchni maszyna zdeterminowała kierunek rozwoju społeczeństw, prowadząc je systematycznie do zmian, określanych obecnie mianem Rewolucji Informacyjnej. Sam ENIAC rewolucji nie zapoczątkował – był jedynie (a zarazem aż) pierwszym krokiem uczynionym przez ludzkość w kierunku rozwoju technologii zinformatyzowanego przetwarzania danych. Aby mogły nastąpić zmiany określane mianem „rewolucyjnych", potrzeba było wystąpienia kilku czynników.

Genezę samej Rewolucji można umiejscowić ledwie dwadzieścia lat wstecz – na początku lat 80-tych ubiegłego stulecia, gdy upowszechniły się komputery domowe (ZX Spectrum, Atari, Commodore), a firma IBM wypuściła na rynek pierwszy model komputera osobistego. Komputer przestał przypominać rozmiarami szafę i przyjął kształt możliwego do ulokowania w każdym miejscu zgrabnego pudełka. Sprzęt komputerowy stał się

[1] *Electronic Numerical Integrator And Computer*

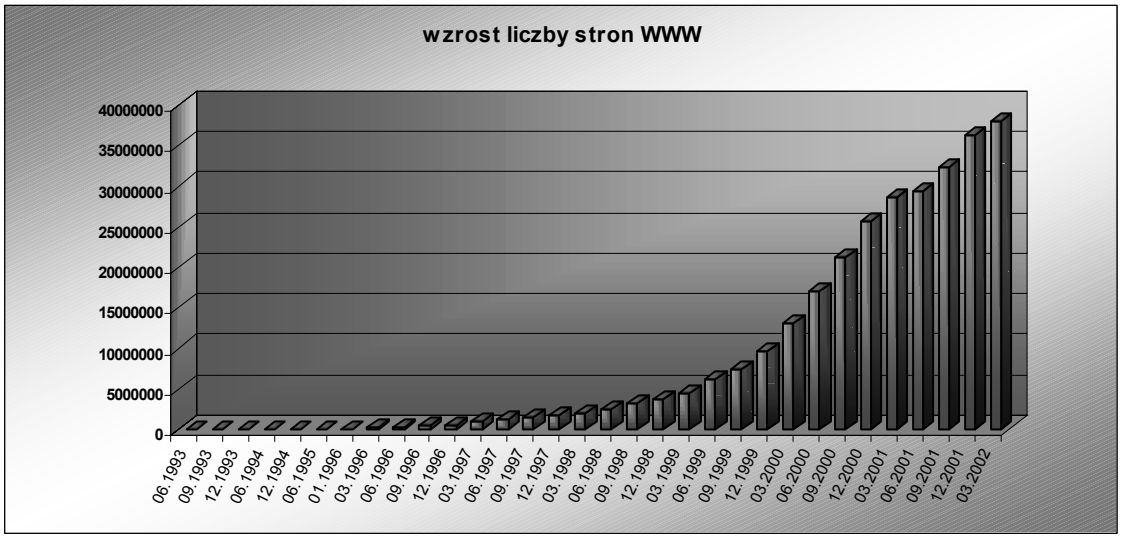
ogólnie dostępny dzięki spadkowi cen i prostocie użytkowania – narzędzie, służące do pracy nielicznym wybranym „trafiło pod strzechy" i stało się powszechnym, wykorzystywanym również do nauki i rozrywki.

Innym wydarzeniem, które odegrało poważną rolę w procesie światowej informatyzacji, było powołanie do życia w 1957 r. przez Departament Obrony Stanów Zjednoczonych projektu ARPA[2]. Początkowo wojskowa, a następnie także akademicka, sieć ARPA (ARPAnet) uświadomiła jej twórcom i użytkownikom istnienie olbrzymiego potencjału, tkwiącego w połączonych ze sobą komputerach. Służąca pierwotnie do wymiany poglądów pomiędzy ośrodkami akademickimi, stała się podwaliną pod największą światową sieć komputerową. Aby jednak stała się powszechną, potrzeba było zapewnienia dostępności, uproszczeń procedury obsługi oraz stworzenia rozwiązań unaoczniających korzyści z niej płynących. W 1971 r. Ray Tomlinson opracował program obsługujący pocztę elektroniczną (powszechny dziś e-mail), w marcu 1972 r. powstała wersja programu dla ARPAnet'u – wprowadzono znak „@" („małpa"), a w lipcu Larry Roberts napisał pierwszy w historii program do zarządzania pocztą elektroniczną. Pierwsze międzynarodowe przyłączenie do ARPAnet'u miało miejsce w 1973 r. (University College of London). W 1985 r. zarejestrowano pierwszą domenę internetową – symbolics.com, zaś w 1989 r. Tim Berners Lee stworzył technologię WWW (World Wide Web), która, stosowana od 1991 r., zaprezentowała światu obecnie przez nas oglądane oblicze Internetu. Rozwój sieci, poprzez zakładanie stron WWW i rejestrację domen, przebiegał w lawinowym tempie (rys. 1 i 2)[3].



rys. 1 – wzrost liczby zarejestrowanych domen internetowych

[2] *Advanced Research Project Agency*
[3] *za : Hobbes' Internet Timeline – the definitive ARPAnet & Internet history v5.6;* http://www.zakon.org/robert/internet/timeline/



rys. 2 – wzrost liczby stron WWW

1.2 Informatyzacja społeczeństw – powstanie społeczeństwa informacyjnego.

W ten sposób powstał Internet w obecnym kształcie – ogólnie dostępny i wszechstronny, które to cechy zadecydowały o wykorzystaniu go w każdej niemal dziedzinie życia codziennego – prywatnego czy zawodowego. Doprowadził do sytuacji, gdzie usługi świadczone są w miejscu pobytu konsumenta, a nie, jak dotychczas, usługodawcy. Przykładem takiego stanu rzeczy mogą być sklepy internetowe, dokonujące transakcji online, banki, zezwalające na kontrolę i dysponowanie rachunkiem przez właściciela (bądź też nie) za pomocą klawiatury. Trudno w związku z tym nie zgodzić się z poglądem, iż jesteśmy uczestnikami transformacji systemu gospodarczego. W niemal każdej dziedzinie życia Internet zostawia swój ślad. W każdej sferze usług dokonuje zmian dotychczasowych instytucji lub pozostawia swój, konkurujący z tradycyjnym, elektroniczny odpowiednik. Internet jest zinformatyzowanym odbiciem obrazu naszej cywilizacji, więc zjawiska mające miejsce w jego wnętrzu są tak samo różnorodne, jak procesy zachodzące w społeczeństwach, przez które jest budowany. Internet to ludzie, którzy korzystając z niego, jednocześnie go tworzą. Nie dziwi więc, a przynajmniej nie powinien, fakt, iż razem z niewątpliwymi usprawnieniami i korzyściami, informatyzacja przyniosła ze sobą także problemy – te, z którymi ludzkość boryka się od dawna, lecz w nowej, cybernetycznej szacie,

oraz nowe, które bez niej nie mogłyby egzystować. Dotyczy to w związku z tym także prawnej sfery życia, więc i dziedziny prawa karnego.

Cyberprzestrzeń ujęta jako medium ma charakter globalny i chociażby tylko ta jego cecha – transgraniczność – jest przyczyną wielu komplikacji. Nie poruszam tutaj problematyki kontroli sieci (lub inaczej – cenzury Internetu), jako że na ten temat od kilku lat toczy się ożywiona dyskusja pomiędzy zwolennikami a przeciwnikami takich działań i zagadnienie to mogłoby być tematem osobnej pracy. Niewątpliwie medium, posiadające jednocześnie cechy ponadgraniczności i powszechności, jest przekaźnikiem informacji bogatych w treści o przesłaniu zarówno pozytywnym, jak i negatywnym, natomiast sposobu, jak eksploatować pierwsze przy jednoczesnym wyeliminowaniu drugich dotychczas nie znaleziono. Internet jest środowiskiem bardzo specyficznym, rządzącym się w wielu przypadkach swoimi prawami i mającym cechy właściwe tylko sobie, dlatego też korzystanie z sieci wymaga odpowiedniego przygotowania użytkownika – w przypadku, gdy mowa jest o wzajemnym oddziaływaniu cyberprzestrzeni i sfery prawnej, użytkownikiem tym jest państwo, a ściślej – jego organy prawotwórcze. Patrząc na to z drugiej strony, mianem użytkownika można określić obywateli danego kraju, o ile w przypadku światowej sieci można mówić o podziale cyberspołeczności na grupy narodowe.

Można bezsprzecznie ogłosić istnienie globalnego Społeczeństwa Informacyjnego, czyli społeczeństwa opierającego się (poprzez system gospodarczy, oparty na wiedzy, a nie, jak dotąd, na pracy i kapitale, a także styl życia) na informacji i technologiach informacyjnych. Zgodnie z jedną z definicji, społeczeństwo informacyjne[4] (lub społeczeństwo oparte na wiedzy[5]) to nowy system społeczeństwa, kształtujący się w krajach o wysokim stopniu rozwoju technologicznego, gdzie zarządzanie informacją, jej jakość, szybkość przepływu są zasadniczymi czynnikami konkurencyjności zarówno w przemyśle, jak i w usługach, a stopień rozwoju wymaga stosowania nowych technik gromadzenia, przetwarzania, przekazywania i użytkowania informacji[6]. W innym ujęciu społeczeństwo informacyjne to „społeczeństwo, w którym informacja stała się zasobem produkcyjnym określającym nowe przewagi konkurencyjne w stosunku do otoczenia, a równocześnie zapewniającym rosnący poziom adaptacyjności społecznej, w wyrazie ogólnym i w wyrazie jednostkowym, do zwiększającej się lawinowo zmienności tego otoczenia. Jak z tego wynika, w podejściu do społeczeństwa informacyjnego akcentuje się nie tyle aspekt technologiczny (technologie informacyjne), ile aksjologiczny, wykształcenie się nowej formacji cywilizacyjnej z nowym sposobem postrzegania świata i zmodyfikowanym systemem war-

[4] *ang. Information Society*
[5] *ang. Knowledge-based Society*
[6] *Ministerstwo Łączności – ePolska. Plan działania na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001 – 2006 z dnia 14 czerwca 2001 r.*

tości społecznych."[7]. Powstaje pytanie, czym jest owa „informacja", na której opiera się cały nowy system społeczny i ekonomiczny ?

1.3 Pojęcie „informacji". Informacja jako dobro prawnie chronione.

Upowszechnienie się sprzętu komputerowego (dzięki relatywnie niskim cenom, umożliwiającym jego zakup praktycznie nieograniczonemu gronu nabywców), powstanie ogólnoświatowej Sieci (poprzez udostępnienie sieci zamkniętych szerszej rzeszy użytkowników) i jej rozkwit, a także rozwój technologii w sektorze telekomunikacji (telefonia i telewizja satelitarna) oraz wprowadzenie na rynek software'u, którego obsługa nie wymaga od użytkownika kwalifikacji informatycznych spowodowały wzrost znaczenia informacji na światowym rynku. W realiach systemu gospodarczego zdeterminowanego przez sferę usług, informacja, będąca dotychczas środkiem służącym do gromadzenia dóbr, sama stała się takim dobrem[8]. Obecna technologia pozwoliła na przetwarzanie tejże informacji w wieloraki sposób, a także na jej udostępnianie praktycznie bez ograniczeń – informacja stała się towarem posiadającym swoją wartość. Powstaje więc naturalne w tych warunkach pytanie, czym jest „informacja", a także wyłania się zagadnienie jej własności, której uregulowanie to *conditio sine qua non* wprowadzenia każdego towaru do obrotu.

Ów wzrost znaczenia informacji, ukoronowany nadaniem jej statusu autonomicznego dobra prawnego nie mógł pozostać bez odzewu ze strony nauk prawnych. Coraz częściej wyodrębnia się w literaturze nową dyscyplinę prawa, jakim jest „prawo informacyjne" („informatyczne", „komputerowe"), pomimo, iż materia zainteresowań tej dziedziny egzystuje na pograniczu innych gałęzi prawa, lub zawiera się w kilku jednocześnie.

O samym przedmiocie tych rozważań – informacji – pozwolę sobie wypowiedzieć się szerzej, niżby się mogło wydawać z punktu widzenia poruszonej tematyki. Uważam to za niezbędne w celu dokładnego przedstawienia środowiska, w którym zachodzą zjawiska będące tematem niniejszej pracy – przestępstwa „*stricte*" komputerowe to przestępstwa przeciwko ochronie informacji.

Encyklopedie i słowniki dostarczają kilku definicji pojęcia informacji. Np. „Informacja – własność przysługująca materialnemu nośnikowi informacji (zwanemu sygnałem), której istotą jest redukcja niepewności; (...) informacja nie przysługuje nośnikowi w sposób absolutny – ten sam sygnał, w zależności od okoliczności, może dostarczać różnych in-

---

[7] J. Wierzbołowski, referat na konferencji naukowej „Integracja europejska wobec wyzwań ery informacyjnej (proindustrialnej)" zorganizowanej przez Centralny Urząd Planowania oraz Instytut Rozwoju i Studiów Strategicznych;
[8] A. Adamski – Prawo karne komputerowe, Warszawa 2000, str. XV;

formacji; (...) w informatyce : abstrakcyjny obiekt, który w postaci zakodowanej (jako dane) może być :

- przechowywany (na nośniku danych)
- przesyłany (za pomocą sygnałów elektrycznych, akustycznych)
- przetwarzany (w trakcie wykonywania algorytmu)
- użyty do sterowania (komputer sterowany programem będącym zakodowaną informacją)[9]."

W słownikach języka polskiego spotykamy się z definicją mówiącą, że informacja to „powiadomienie o czymś, świadomość, pouczenie; w cybernetyce – każdy czynnik, dzięki któremu ludzie lub urządzenia automatyczne mogą bardziej sprawnie, celowo działać[10]" bądź „wiadomość, wieść, rzecz zakomunikowana, zawiadomienie, komunikat; pouczenie, powiadomienie; dane.[11]" Ponadto możemy się dowiedzieć, że „miara informacji" to „(...) w matematyce, cybernetyce – miara braku entropii (nieokreśloności), miara organizacji systemu.[12]" Z punktu widzenia nauk prawnych oraz informatyki połączenie zakresu znaczeniowego „informacji" i „danych" w jednej z powyższych definicji wydaje się niewłaściwe (o czym poniżej), natomiast nie będę poruszał możliwości używania tych pojęć zamiennie na innych płaszczyznach, jako że do pracy niniejszej materia ta nie należy. Definicje encyklopedyczne i słownikowe kształtują informację jako wiadomość, która w zależności od przyjętych w danym miejscu i czasie konwencji może dostarczać różnorodnych informacji, której istotą jest redukcja niepewności, a jako abstrakcyjny obiekt w postaci zakodowanej może być przechowywana, przesyłana, przetwarzana i używana do sterowania. Cechy te można rozpatrywać z dwu punktów : z punktu widzenia celów, którym informacja może służyć oraz działań, które można w stosunku do tej informacji podjąć, by ten cel osiągnąć. Istotą informacji jest redukcja niepewności, a więc jest to czynnik zmniejszający ilość przedmiotów objętych niewiedzą bądź niepewnością. Tak więc można charakteryzować informację jako byt niematerialny, powstały w świadomości społecznej jako czynnik zwiększający prawdopodobieństwo podjęcia właściwych (z punktu widzenia danej społeczności) decyzji, zbliżających ową społeczność do osiągnięcia ustalonych przez nią celów. Z drugiej strony informację charakteryzują działania, które można w stosunku do niej podjąć – można ją przechowywać, udostępniać i przetwarzać, co również stanowi jej charakterystykę. Informację tworzy zapotrzebowanie (społeczne, grup gospo-

[9] *Wielka Encyklopedia PWN, Warszawa 2002;*
[10] *Słownik Języka Polskiego, PWN, Warszawa 1978;*
[11] *Władysław Kopaliński – Słownik Wyrazów Obcych i zwrotów obcojęzycznych, wyd. XVII, Warszawa 1979*
[12] *ibidem*

darczych bądź grup interesu) na nią, a jego waga determinuje jej wartość. Przy takim spojrzeniu na zagadnienie, w tym momencie bowiem mają zastosowanie prawa rynku – podaż i popyt, informacja staje się towarem, a jej cenę dyktuje również ilość i jakość oraz stopień powszechnej dostępności.

Dla zrozumienia, czym jest informacja w zakresie nauk prawnych (szczególnie w dziedzinie prawa karnego) należy przedstawić różnicę pomiędzy zakresem pojęciowym „informacji" i „danych". Stwierdzenie Norberta Wienera, iż „*informacja jest informacją, a nie materią i nie energią*" wskazuje na autonomiczny status informacji jako składnika rzeczywistości[13]. Pierwszy raz zwrócono uwagę na te pojęcia i różnice pomiędzy nimi („dane" i „informacja") w raporcie holenderskiej komisji ds. przestępstw komputerowych, opublikowanym w 1988 r., w którym czytamy m.in. „ *(...) Przez dane komisja (opierając się w znacznym stopniu na definicji Holenderskiego Instytutu Normalizacji) rozumie przedstawienie faktów, pojęć lub poleceń w ustalony sposób, który umożliwia ich przesyłanie, interpretację lub przetwarzanie zarówno przez ludzi, jak i w sposób zautomatyzowany (...) Informacja to wywołany danymi efekt – zamierzony lub doświadczony przez ich użytkowników. Uzyskiwanie informacji lub informowanie innych polega na posłużeniu się danymi i ma charakter subiektywny, gdyż może być silnie uzależnione od czynników społeczno-kulturalnych oraz społecznych i ekonomicznych ról, jakie pełni osoba lub osoby zaangażowane w te sytuacje (...) W przeciwieństwie do „informacji" „dane" są neutralne i przybierają uzgodnioną postać liter, znaków, wzorów lub sygnałów, które mogą być przechowywane, przetwarzane lub przesyłane bezpośrednio przez ludzi lub przy użyciu specjalnych środków fizycznych albo urządzeń technicznych.*"[14] Podobnie pojęcia te zdefiniowano w rekomendacji OECD[15] przyjętej w sprawie Bezpieczeństwa Systemów Informacyjnych, zgodnie z którą „ *'dane'[16] – przedstawienie faktów, pojęć lub poleceń w sposób sformalizowany i umożliwiający ich komunikowanie, interpretację lub przetwarzanie, zarówno przez ludzi, jak i urządzenia; 'informacja'[17] – jest to znaczenie, jakie nadajemy danym przy pomocy konwencji odnoszących się do tych danych.[18]"*[19] Można więc wywnioskować, iż dane stanowią substrat procesu interpretacji, którego wynikiem jest informacja. Porównanie tych dwu pojęć na gruncie prawa karnego ma znaczenie o tyle, iż np. posiadanie dostępu do danych nie jest równoznaczne z dostępem do informacji (jako że np. pozostaje

[13] *A. Adamski – Prawo karne komputerowe, op. cit., str. 37*
[14] *Information Technology and Criminal Law, Report of the Dutch Committee on Computer Crime, Ministry of Justice the Hague, 1988 [w:] A. Adamski – Prawo karne komputerowe, op. cit., str. 38*
[15] *Organizacja Rozwoju i Współpracy Gospodarczej*
[16] *data*
[17] *information*
[18] *... is the meaning assigned to data by means of conventions applied to that data*
[19] *Recommendation of the Council of the OECD concerning Guidelines for the Security of Informations Systems OECD/GD (92) 10 Paris, 1992 (aneks) [w:] A. Adamski – Prawo karne komputerowe, op. cit. str. 39*

kwestia interpretacji). Ponadto informacja jest przedmiotem ochrony przestępstw „*stricte*" komputerowych[20], natomiast dane to przedmiot wykonawczy tych przestępstw.

Tak więc, wskutek przeobrażeń cywilizacyjnych, informacja nabrała statusu autonomicznego dobra prawnego, a jako takie wymaga ochrony. Nie oznacza to, iż potrzeba ta pojawiła się w ostatnich latach. Informację chroniono od momentu, gdy tylko zaistniała, natomiast do momentu zastosowania informatycznych metod jej przetwarzania, ochrona obejmowano „tradycyjne" formy jej występowania – tajemnicę korespondencji, tajemnicę państwową, służbową i zawodową. Od momentu zautomatyzowania procesu przetwarzania informacji, zaistniała potrzeba zapewnienia ochrony jej zdigitalizowanej formie. Biorąc pod uwagę coraz większe znaczenie tego rodzaju informacji w dzisiejszej gospodarce i życiu codziennym zapewnienie przetwarzanej elektronicznie informacji ochrony prawnej jest zagadnieniem priorytetowym, jako że korzystając z informacji jako środka umożliwiającego osiągnięcie pewnych celów, dane, z których się ją wywodzi muszą być kompletne i poprawne, natomiast systemy przetwarzające – sprawne. Rosnąć więc będą – wraz z rozwojem zastosowań elektronicznych – wymagania co do poziomu bezpieczeństwa, który definiuje się powszechnie przy użyciu trzech podstawowych kryteriów :

1. dostępność (*availability*) danych, informacji, systemów informatycznych – wg definicji OECD oznacza ich osiągalność i możliwość używania w każdym czasie i w wymagany sposób[21] - czyli możliwość korzystania z nich przez osoby uprawnione zawsze, gdy zaistnieje taka potrzeba.

2. integralność (*integrity*) to „*cecha danych i informacji oznaczająca ich dokładność i kompletność oraz utrzymywanie ich w tym stanie*"[22]; integralność jest gwarancją nienaruszalności danych i programów komputerowych (poprzez nie wprowadzanie do nich zmian przez osoby do tego nieuprawnione).

3. poufność (*confideniality*) stanowi „*właściwość danych i informacji, polegającą na ujawnianiu ich wyłącznie uprawnionym podmiotom i na potrzeby określonych procedur, w dozwolonych przypadkach i w dozwolony sposób*"[23], czyli wyłączny dostęp do określonych informacji osób uprawnionych, a więc także ochrona danych przed dostępem do nich podmiotów do tego nieuprawnionych.

---

[20] *podział przestępstw komputerowych stanowi treść rozdziału I*
[21] *Recommendation of the Council of the OECD concerning Guidelines for the Security of Informations Systems OECD/GD (92) 10 Paris, 1992 [w:] A. Adamski – Prawo karne komputerowe, op. cit. str. 41*
[22] *j. w.*
[23] *Recommendation of the Council of the OECD concerning Guidelines for the Security of Informations Systems OECD/GD (92) 10 Paris, 1992 [w:] A. Adamski – Prawo karne komputerowe, op. cit. str. 41*

Ponadto, w literaturze dotyczącej bezpieczeństwa systemów informatycznych, listę powyższą uzupełnia się, omawiając zagadnienia związane z kryptografią, o dwa kolejne :

4. uwierzytelnienie (*authentication*), czyli sprawdzenie, czy dany użytkownik jest tym, za którego się podaje, oraz
5. niezaprzeczalność (*nonrepudiation*), czyli ochrona przed wyparciem się przez nadawcę faktu wysłania określonej informacji[24].

Ochronę elektronicznie przetwarzanej informacji wg powyższych trzech głównych kryteriów sprawuje się głównie przy pomocy środków techniczno-administracyjnych, spełniających funkcje prewencyjne[25]. Przepisy karne pełnią funkcje represyjną i nie tyle zabezpieczają przed wystąpieniem zagrożeń, co uruchamiają sankcje, gdy do takiego zagrożenia (bądź wystąpienia szkody) już dojdzie. W teorii sankcje karne mogą odstraszać od popełnienia czynu (w tym przypadku zamachu na system informatyczny), lecz jak się słusznie zauważa, prawidłowe funkcjonowanie takiego systemu zależne jest od współwystępowania co najmniej dwu warunków – czyn ten powinien być zachowaniem prawnie zabronionym pod groźbą kary i prawdopodobieństwo zastosowania sankcji wobec osób naruszających ten zakaz powinno być znaczne. W przypadku przestępstw przeciwko ochronie informacji drugi warunek jest spełniany bardzo różnie[26].[27]

Innym zagadnieniem, nie będącym co prawda tematem tej pracy, niemniej godnym wzmianki, jest potrzeba ochrony nie tylko informacji jako dobra prawnego, lecz także podmiotów, których ona dotyczy, jako że byt informacji jest określony istnieniem innego podmiotu, który mogłaby określać. Informacja ze swej natury musi odnosić się do podmiotu zewnętrznego, a nie do samej siebie.

1.4 Historia przestępstw popełnianych z wykorzystaniem komputera.

Trudno dzisiaj stwierdzić, kiedy dokładnie popełniono pierwsze w historii przestępstwo z wykorzystaniem komputera. Najwcześniejsze doniesienia o takim działaniu pochodzą z prasy amerykańskiej lat 60-tych ubiegłego stulecia i dotyczyły piractwa oraz szpiegostwa komputerowego. Pierwsze w Stanach Zjednoczonych przestępstwo komputerowe zanotowano w 1957 r., a pierwsze „federalne" dochodzenie w sprawie takiego

[24] *M. Molski, S. Opala – Elementarz bezpieczeństwa systemów informatycznych, wyd. Mikom, Warszawa 2002*
[25] *o metodach zabezpieczeń systemów informatycznych i informacji szerzej w rozdziale II*
[26] *A. Adamski – Prawo karne komputerowe, op. cit., str. 44*
[27] *o statystykach przestępstw komputerowych i ich wykrywalności szerzej w rozdziale II*

przestępstwa wszczęto w 1966 r.[28] Warto zaznaczyć, że daty te odnoszą się do przestępstwa wykrytego – nie ma odpowiedzi na pytanie, czy było ono pierwszym z tego rodzaju. Aby jednak można było powiedzieć o zjawisku przestępczości komputerowej, potrzeba było zaistnienia tego samego czynnika, co w przypadku komputeryzacji – upowszechnienia się sprzętu komputerowego. Od lat sześćdziesiątych nastąpił w krajach zachodnich systematyczny wzrost przestępczości komputerowej[29]. Już na początku lat 80-tych miało miejsce pierwsze głośne wydarzenie – w 1983 r., w jednej z pierwszych policyjnych akcji wymierzonych przeciwko przestępcom komputerowym, FBI aresztowała 6-cio osobową grupę, znaną jako „414". Oskarżeni byli o dokonanie około 60-ciu włamań, w tym do Laboratorium Los Alamos. Jednak dopiero wydarzenia schyłku lat 80-tych zwróciły uwagę opinii publicznej na zagrożenia płynące z postępującej komputeryzacji. W 1987 roku wydano pierwszy wyrok skazujący na podstawie „Computer Fraud and Abuse Act" z 1986 r. Oskarżonym o włamania do centrali AT&T był siedemnastoletni Herbert Zinn, używający pseudonimu „Shadow Hawk". Poważniejsze następstwa spowodował inny incydent – 2 listopada 1988 r. dwudziestodwuletni student Cornell University, Robert T. Morris uruchomił w sieci napisany przez siebie program (obecnie zasługiwałby na miano „robaka"), wykorzystujący luki w zabezpieczeniach UNIX-a. Program ten, nie zawierający jednak destrukcyjnych instrukcji, replikując swój kod, rozmnożył się błyskawicznie i przeciążając pamięć operacyjną komputerów doprowadził do sparaliżowania sieci. Dzień 3 listopada 1988 r. nazwano „czarnym czwartkiem" – „robakowi" Morrisa potrzeba było zaledwie 24 godzin, aby jego obecność stwierdzono na ok. 6 tysiącach dysków twardych, co w 1988 r. stanowiło 10 % komputerów włączonych do ARPAneťu[30]. Straty oszacowano na 15 do 100 (!!!) milionów dolarów[31]. Sprawa zakończyła się w sądzie wyrokiem skazującym (3 lata pozbawienia wolności z warunkowym zawieszeniem kary, 400 godzin pracy na cele społeczne i 10 tys. USD grzywny), cały incydent zaś był przyczyną utworzenia, z inicjatywy Departamentu Obrony USA, zespołu reagowania na incydenty zagrażające bezpieczeństwu sieci (CERT)[32]. Swoistą ciekawostką tej sprawy może być fakt, iż „robak" Morrisa składał się z mniej niż 100 linii kodu, a wg zamierzeń autora miał unaocznić niebezpieczeństwo wynikające z istniejących w sieci luk[33]. Innym wydarzeniem, sięgającym korzeniami w rok 1986, było prywatne dochodzenie Clifforda Strolla w sprawie systematycznych włamań do komputera uniwersyteckiego. Stroll, administrator systemu na uniwersy-

[28] *A.Bequai – Technocrimes. Lexington Mass. 1987 [w:] A. Adamski – Prawo karne komputerowe, op. cit., str. 1*
[29] *E. Pływaczewski – Przemówienie powitalne [w:] A. Adamski (red.) – Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Materiały z konferencji naukowej, TNOiK, Toruń 1994*
[30] *The Internet Worm of 1988; http://world.std.com/~franl/worm.html*
[31] *D. Doroziński – Hakerzy. Technoanarchiści cyberprzestrzeni, str. 47; tak duża rozpiętość w szacunku strat jest powszechnie spotykanym elementem problematyki przestępczości komputerowej; o odmiennych szacunkach strat spowodowanych przez robaka Morrisa i problemach związanych z ustalaniem dokładnych wysokości strat bliżej w rozdziale II;*
[32] *Computer Emergency Response Team*
[33] *m. in. chodziło o lukę w poleceniu "finger";*

tecie w Berkeley, stwierdził, że ataki te pochodzą z tego samego źródła, co ataki na komputery rządowe. Śledztwo, początkowo prywatne, a następnie międzynarodowe, zakończyło się aresztowaniem w 1989 r. niemieckich cyberszpiegów, sprzedających uzyskane informacje Związkowi Radzieckiemu. Historie tego śledztwa Stroll opisał później w swojej książce[34].

Opisane powyżej przypadki można określić jako jedne z najbardziej spektakularnych wydarzeń w początkach historii działalności, która można obecnie określić „przestępczością komputerową". Historie Mitnicka, Poulsena, grup takich jak Legion of Doom miały nastąpić dopiero później, choć rozgłos nadany im przez media spowodowały, że można spotkać się z opinią (niemal wręcz powszechną), iż pierwszym przestępcą, posługującym się komputerem, był właśnie Kevin Mitnick. Historia Morrisa i „hackerów z Hanoweru" mają o tyle wielkie znaczenie, iż zademonstrowały możliwości, jakimi dysponuje Sieć (a przez to i użytkownik) i w jaki sposób można je wykorzystać do działalności niezgodnej z prawem. O ile w latach 70-tych i 80-tych problemy związane z nadużywaniem technologii komputerowej do celów sprzecznych z panującym porządkiem prawnym postrzegano raczej w skali lokalnej, to w latach 90-tych nadużycia te zostały uznane za jedną z form przestępczości transgranicznej[35]. Można stwierdzić, iż rzucono prawodawcom wyzwanie, którego nie mogli nie przyjąć.

1.5 Kształtowanie się karalności przestępstw komputerowych.

Reakcja ze strony prawodawców była niezbędna przede wszystkim z powodu zmian, jakie w istniejących stosunkach gospodarczych i społecznych powoduje każdy przełom technologiczny, a które wymagają dostosowania porządku prawnego do nowopowstałych realiów.

R. Hollinger dokonał podziału historii postrzegania technologii komputerowej jako nosiciela zagrożeń na gruncie prawa w Stanach Zjednoczonych A. P. na cztery główne etapy :

1. lata 1946 – 1976, kiedy to odkryto istnienie nadużyć komputerowych; wiązało się to z książką Dana Parkera, w której udokumentowano fakt istnienia zjawiska36;

---

[34] C. Stroll – The Cuckoo's Egg; Tracking a Spy through the Maze of Computer Espionage, New York 1989
[35] S. Redo – Prevention and control of computer related crime from the United Nations perspective [w:] A. Adamski (red.) – Prawne aspekty ..., op. cit.
[36] D. Parker – Crime by Computer, New York 1976;

2. okres 1977 – 1987, w którym skryminalizowano te nadużycia (wspomniane niżej ustawodawstwo stanu Floryda, a także 48 ustaw stanowych i dwie federalne);
3. lata 1988 – 1992 to okres demonizacji „hackerów", będący efektem głośnych spraw Roberta T. Morrisa i „hackerów z Hanoweru" (wspomniane powyżej);
4. okres cenzury, trwający od 1993 r., jest przejawem presji politycznej na ograniczenie swobodnego przepływu informacji w Internecie[37], uzasadnianej koniecznością zablokowania propagowania w sieci treści szkodliwych[38].

Przystosowanie systemów prawnych do realiów rewolucji Informacyjnej przebiegało w kilku etapach, a jego początki sięgają lat 70-tych. Wówczas kierunek reform ustawodawczych wyznaczyła ochrona prywatności człowieka w związku z przetwarzaniem danych osobowych i jego zautomatyzowaniem. W 1973 r. w Szwecji uchwalono pierwszą na świecie ustawę o ochronie danych osobowych[39]. W latach 80-tych zaczęto penalizować nadużycia popełniane z wykorzystaniem nowoczesnych technologii. W ustawodawstwie karnym wielu krajów pojawiły się typy przestępstw komputerowych. Pierwsze przepisy dotyczące tego rodzaju przestępczości pojawiły się w ustawodawstwie stanu Floryda (1978) oraz we Włoszech[40]. Kolejną tendencją było objęcie własności intelektualnej w zakresie oprogramowania komputerowego ochroną ze strony prawa autorskiego, w miejsce dotychczas istniejącego modelu ochrony patentowej. W latach 90-tych natomiast, gdy globalne społeczeństwo informacyjne stawało się faktem, zaczęto poszukiwać rozwiązań karnoprocesowych, pozwalających ścigać przestępstwa popełniane przy użyciu sieci komputerowych. Wyrazem tego jest Zalecenie Komitetu Ministrów Rady Europy Nr R(95)13 z dnia 11 września 1995 r. w sprawie „Problemów karno procesowych związanych z technologią przetwarzania informacji"[41]. Starano się także określić zasady odpowiedzialności za rozpowszechnianie w Internecie treści „nielegalnych i szkodliwych". Prace w kierunku przyjęcia przez kraje Unii Europejskiej wspólnych uregulowań prawnych dotyczących tych treści (m. in. o charakterze rasistowskim, pornograficznym, dotyczących

[37] *używając prostej terminologii, rzecz dotyczy cenzury Internetu, na temat której dyskusja toczy się od lat i sądząc po nieustępliwości adwersarzy trwać będzie jeszcze długo;*
[38] *R. Hollinger – Crime, Deviance and Computer, Dartmouth, 1997, str. XVIII* [w:] *A. Adamski – Prawo karne ..., op. cit., str.2-3;*
[39] *A. Adamski – Prawo karne komputerowe, op. cit., str. XVI;*
[40] *ibidem*
[41] *Problems of Criminal Procedural Law Connected with Information Technology. Recommendation No. R(95) 13 adopted by the Committee of Ministers of the Council of Europe on 11 September 1995 and explanatory memorandum, Council of Europe Publishing, 1996* [za:] *A. Adamski – Prawo karne komputerowe, op. cit., str. XVII;*

handlu dziećmi i kobietami, propagujących terroryzm, przemoc i nienawiść) zapoczątkowała Komisja Europejska w 1996 roku[42].

[42] *Communication on Illegal and Harmful Content on the Internet, approved by the European Commission on 16 October 1996; Green Paper on the Protection of Minors and Human Dignity in Audio-visual and Information Services, approved by the European Commission on 16 October 1996; Report of the Commission communication on illegal and harmful content on the Internet (COM (96) 0487 – C4-0592/96) of 20 March 1997, Committee on Civil Liberties and Internal Affairs* [w:] *A. Adamski – Prawo karne komputerowe, op. cit., str XVIII;*

2. Rozdział II – Przestępczość komputerowa

Określenie „przestępstwa komputerowe" w chwili obecnej jest swoistym hasłem, pod którym kryje się wieloaspektowa problematyka ochrony informacji w warunkach jej automatycznego przetwarzania[43] i określającym pewien zbiór czynów zabronionych, których cechą wspólną jest występowanie wśród ich przesłanek (przedmiotów wykonawczych bądź przedmiotów przestępstwa) komputerów, informacji bądź danych przechowywanych i przetwarzanych w formie elektronicznej, urządzeń telekomunikacyjnych lub teleinformatycznych. Zbiór ten, na dzień dzisiejszy, jest zbiorem otwartym, jako że, biorąc pod uwagę stopień postępu technologicznego i związane z nim ewoluowanie metod działań przestępczych, nie wydaje się możliwe stworzenie aktualnej przez dłuższy czas *numerus clausus* tych przestępstw. Ponadto, abstrahując od kwalifikacji prawnej, zaliczenie pewnych czynów do powyższej grupy zależy (lub powinno zależeć) także od innych czynników, np. przynależności do określonej grupy zawodowej[44].

2.1 Pojęcie i podział tzw. „przestępstw komputerowych"

Zdefiniowanie pojęcia „przestępstw komputerowych" nastręcza wielu trudności, spowodowanych m.in. różnorodnością metod przestępczego działania, która jest również przyczyną powstania wielu bardzo zróżnicowanych definicji. Poniżej przedstawię kilka z nich w celu zobrazowania rozpiętości ich zakresu znaczeniowego. Trzeba przy tym pamiętać, iż różnice pomiędzy tymi definicjami są efektem tworzenia ich w ramach określonego zagadnienia, a nie jako ogólnych powszechnego zastosowania. Jak stwierdził A. Adamski „Ciągły postęp techniczny nie sprzyja trwałości formułowanych w piśmiennictwie definicji przestępczości komputerowej"[45].

Cechą wspólną wszystkich definicji „przestępstw komputerowych" jest występowanie przynajmniej jednego z elementów takich jak a) system komputerowy, b) jego połączenia oraz c) nośniki zdigitalizowanej informacji[46]. Można więc przyjąć (jako punkt

---

[43] A. Adamski – Wstęp [w:] A. Adamski (red.) – Prawne aspekty ..., op. cit., str. 7; podobnie S. Iwanicki – Przemówienie powitalne, tamże, str. 18-19;

[44] ciekawą kwestią jest brak klauzuli niekaralności dla pewnych grup zawodowych, np. dla policjanta, podążającego tropem sprawcy „komputerowego włamania"; zagadnienie opisuje W. Wiewiórowski – Profesjonalny haker. Paradoks odpowiedzialności karnej za czyny związane z ochroną danych i systemów komputerowych. Materiały z konferencji naukowej „Bezpieczeństwo sieci komputerowych a hacking. Internetki V, Lublin, 4-5 marca 2005", wyd. UMCS, Lublin 2005; jednocześnie należy dodać, że przy wykonywaniu tzw. „audytów bezpieczeństwa", czy też wzajemnym testowaniu zabezpieczeń przez np. administratorów sieci kontratyp istnieje w postaci „zgody pokrzywdzonego" („zgoda dysponenta dobrem") por. L. Gardocki – Prawo karne, wyd. C. H. Beck, Warszawa, 2001, str. 122 - 124;

[45] A. Adamski – Prawo karne ..., op. cit., str. 32

[46] B. Fischer – Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne. Kantor wydawniczy „Zakamycze" 2000.

wyjścia) bardzo ogólną definicję, wg której przestępstwa komputerowe to czyny skierowane przeciwko systemowi komputerowemu (w tym przypadku komputer bądź system komputerowy służy za cel zamachu), jak również czyny popełniane przy pomocy komputera (komputer służy za narzędzie przestępstwa)[47]. Jak zaznaczyłem powyżej, jest to definicja bardzo ogólna, jako że możliwe jest popełnienie przestępstwa zabójstwa przy wykorzystaniu komputera w sposób, który nie będzie się mieścił nawet w szeroko pojętych ramach „przestępczości komputerowej" (np. zbrodnia zabójstwa popełniona przez uderzenie ofiary komputerem w głowę)[48]. Postuluje się jednak nadawanie temu określeniu szerokiego znaczenia, obejmującego wszelkie zachowania przestępne związane z funkcjonowaniem systemów elektronicznego przetwarzania danych[49].

Przykładem szerokiego ujęcia problemu może być definicja używana przez Interpol[50], według której „przestępczością komputerową" jest przestępczość w zakresie technik komputerowych[51], bądź tez definicja D. B. Parkera, który określił to pojęcie jako „ akty przynoszące straty, szkody lub uszkodzenia, do których wykonania wykorzystano systemy przetwarzania danych."[52] Warto dodać, że definicje te były niewystarczające już w chwili ich tworzenia[53]. Innym przykładem takiego ujęcia jest określenie, że „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"[54]. Ze względu na kryteria definiujące poziom bezpieczeństwa elektronicznie przetwarzanej informacji, przyjęte przez OECD w 1992 r.[55], czyli dostępność, integralność i poufność, można określić „przestępstwa komputerowe" jako czyny naruszające w jakikolwiek sposób te trzy kryteria[56].

W literaturze przedmiotu również prezentowane są różnorodne propozycje podziałów „przestępstw komputerowych" – na potrzeby niniejszej pracy będę posługiwał się

---

[47] ibidem.

[48] nie spotkałem się w literaturze, w związku z definiowaniem pojęcia „przestępczości komputerowej" z zastrzeżeniem warunku „użycia sprzętu komputerowego zgodnie z jego przeznaczeniem w celu popełnienia przestępstwa"; warunek ten wydaje się być oczywistym, z drugiej jednak strony, wspomniany przeze mnie przykład wskazuje możliwość popełnienia czynu przestępnego spełniającego wszystkie przesłanki szerokiej definicji „przestępczości komputerowej", faktycznie jednak nie mieszczącego się w jej ramach;

[49] S. Iwanicki – Przemówienie powitalne [w:] A. Adamski (red.) – Prawne aspekty ... op. cit., str. 18;

[50] International Criminal Police Organization

[51] B. Fischer – Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne. Kantor wydawniczy „Zakamycze" 2000 [za:] K. J. Jakubski – Sieci komputerowe a przestępczość [w:] Materiały konferencyjne Trzeciego Forum Teleinformatyki „Bezpieczeństwo Systemów Teleinformatycznych", Legionowo 22 – 23 października 1997 r.

[52] A. Płaza – Przestępstwa komputerowe, Rzeszów 2000 [za :] D. B. Parker – Computer related crime,, Journal of Forensic Science, nr 9/74.

[53] definicja D. B. Parkera pochodzi z 1974 r.

[54] K. J. Jakubski – Przestępczość komputerowa – zarys problematyki. Prokuratura i Prawo, nr 12/96, str. 34;

[55] kryteria przyjęte przez OECD zostały opisane w rozdziale I;

[56] A. Adamski – Prawo karne ..., op. cit., str. 40-41; także : A. Płaza – Przestępstwa komputerowe, Rzeszów 2000;

podziałem „przestępstw komputerowych” na „przestępstwa komputerowe” *sensu stricte i sensu largo* jako podziałem wiodącym :

1. Pierwsza z tych grup obejmuje czyny typizowane pod kątem przedmiotu ochrony, jakim jest informacja i stanowią one przede wszystkim treść rozdziału XXXIII Kodeksu Karnego; są to zamachy na systemy, dane i programy komputerowe, czyli zamachy, które mogą istnieć tylko w środowisku technologii komputerowej (w związku z tym stanowią relatywnie nowe zjawisko). Ze względu na dobro prawnie chronione można je określać mianem „przestępstw przeciwko bezpieczeństwu elektronicznie przetwarzanej informacji” lub „przestępstw przeciwko ochronie informacji”[57].
2. druga grupa zawiera katalog przestępstw, możliwych do popełnienia przy użyciu elektronicznych systemów przetwarzania informacji (komputer stanowi narzędzie przestępstwa), skierowanych przeciw tradycyjnym dobrom prawnym. Jednocześnie warto zaznaczyć, iż przy pomocy zaawansowanej technologii przetwarzania danych możliwe jest popełnienie przestępstw, których taka forma popełnienia nie jest przewidziana przepisem[58][59].[60]

Podziału „przestępstw komputerowych” ze względu na kolejność pojawiania się wraz z rozwojem technologii dokonał U. Sieber :

1. Przestępstwa w zakresie ochrony danych (naruszenie praw jednostki)[61]
2. Przestępstwa gospodarcze z użyciem komputerów :
    a) manipulacje komputerowe :
        - operacje rozrachunkowe,
        - manipulacje bilansowe,
        - manipulowanie stanem kont bankowych,
        - nadużycia kart bankomatowych i innych środków płatniczych,
        - nadużycia telekomunikacyjne;

[57] *A. Adamski – Prawo karne ..., op. cit., str. 30;*
[58] *zniesławienie lub groźba karalna, której dopuszczono się za pomocą poczty elektronicznej;*
[59] *A. Adamski – Prawo karne ..., op. cit., str. 31;*
[60] *podział ten można również traktować jako rozróżnienie przestępstw na te skierowane przeciwko systemowi komputerowemu (komputer – cel) i te popełniane przy użyciu komputera (komputer – narzędzie);*
[61] *chronologii działań legislacyjnych związanych z rozwojem technologii automatycznego przetwarzania danych i przestępczości skierowanej przeciw niej poświęcona jest część rozdziału I do niniejszej pracy;*

b) sabotaż i szantaż komputerowy;

c) hacking komputerowy;

d) szpiegostwo komputerowe;

e) kradzieże software'u i inne formy piractwa dotyczące produktów przemysłu komputerowego.

3. Inne rodzaje przestępstw :

a) rozpowszechnianie za pomocą komputerów informacji pochwalających użycie przemocy, rasistowskich i pornograficznych,

b) użycie techniki komputerowej w tradycyjnych rodzajach przestępstw[62].

Angielski prawnik Hugo Cornwall, na podstawie badań, dokonał podziału „przestępstw komputerowych" na cztery zasadnicze grupy[63] :

1. niemożliwe do dokonania poza środowiskiem komputerowym;
2. ułatwione przez zastosowanie komputerów;
3. popełniane przy biernym udziale komputerów;
4. dokonywane przez zawodowych przestępców z wykorzystaniem komputerów[64].

Innym podziałem, będącym właściwie wyliczeniem czynów przestępczych, jest „lista minimalna" i „fakultatywna", zawarta w Zaleceniu Rady Europy Nr (89)9. Konwencja o Cyberprzestępczości posługuje się również takim wyliczeniem przestępstw, ujętych w cztery zasadnicze grupy[65].

Ponadto można wyodrębnić, pod kątem funkcji systemu komputerowego, następujące grupy przestępstw, w których komputer spełnia rolę :

1. „obiektu" przestępstwa,
2. „narzędzia" przestępstwa,

---

[62] M. Molski, S. Opala – Elementarz bezpieczeństwa ..., op. cit., str. 17-18; także A. Płaza – Przestępstwa komputerowe, op. cit. str. 7-8 [za:] U. Sieber – Przestępczość komputerowa, a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka, Przegląd Policyjny, Nr 3(39)/95;

[63] podział ten zasadza się na kryterium roli komputera w popełnieniu przestępstwa jako środowiska, w którym przestępstwo jest popełniane lub narzędzia popełnienia;

[64] B. Fisher – Przestępstwa komputerowe ..., op. cit., str. 25; także M. Molski, S. Opala – Elementarz bezpieczeństwa ..., op. cit., str. 18 [za:] H. Cornwall – Datatheft. Computer Fraud, Industrial Espionage and Information Crime, Mandarin Paperibacks, London 1990;

[65] lista przestępstw i ich podziały, zawarte w obu wymienionych dokumentach zostaną bliżej opisane w rozdziale poświęconym inicjatywom Rady Europy;

3. „źródła” innej przestępczości,
4. źródła i środka dowodowego[66].

Powyższe definicje i podziały odnoszą się do problemu „przestępczości komputerowej” w aspekcie materialnego prawa karnego. Ponadto można mówić o „przestępstwach komputerowych” w aspekcie karnoprocesowym, oznaczającym zawieranie przez system komputerowy dowodów działalności przestępczej. Z tej perspektywy do grupy „przestępstw komputerowych” będą należały wszelkie czyny zagrożone przez prawo karne sankcją, których ściganie wymaga uzyskania od organów ścigania i wymiaru sprawiedliwości dostępu do informacji (danych) przechowywanych i (lub) przetwarzanych w systemach komputerowych lub teleinformatycznych. W związku z tym pojęcie „przestępstw komputerowych” w aspekcie procesowym obejmować będzie zarówno przypadki, w których komputer występuje jako narzędzie, jak i cel przestępstwa[67], a także, w szerokim rozumieniu, gdy będzie zawierał dowody popełnienia przestępstwa (nawet jeśli będzie to przestępstwo nie związane z technologią komputerową).

2.2 Przestępczość komputerowa – techniki przestępcze.

Przyjmując za punkt wyjścia do dalszych rozważań wspomnianą wyżej definicję Interpolu można podzielić metody przestępczego działania[68] na kilka głównych grup. Wyznacznikiem podziału jest przede wszystkim (ale nie tylko) cel (ofiara, dobro prawnie chronione) działań przestępczych. W obrębie każdej z tych grup natomiast można wyróżnić specyficzne metody działań przestępczych. Należy mieć na uwadze, że jednostka należąca do danej grupy może się posługiwać jedną lub kilkoma metodami, możliwe jest także zakwalifikowanie jej do więcej niż jednej grupy. Powodowane jest to wszechstronnością „ponadprzeciętnych użytkowników” zaawansowanych technologii i ich dążeniem do powiększania swojej wiedzy. Dotyczy to zwłaszcza entuzjastów, uprawiających sztukę dla sztuki, przestępcy natomiast są zainteresowani głównie osiągnięciem konkretnego celu, dlatego też korzystają często z doświadczenia innych oraz gotowych narzędzi.

Techniki przestępczego działania są również kryterium podziału „przestępstw komputerowych” w ich szerokim rozumieniu. Do głównych metod działania sprawców można obecnie zaliczyć[69] :

1. „hacking” – bardzo ogólnikowo można określić to działanie jako „przełamywanie zabezpieczeń”, „włamywanie się do systemu”; podstawowe

[66] *B. Fischer – Przestępstwa komputerowe ..., op. cit., str. 26;*
[67] *A. Adamski – Prawo karne ..., op. cit., str. 34;*
[68] *w związku z tym podział ten dotyczy także sprawców;*
[69] *ze względu na bardzo dużą różnorodność technik, występujących w obrębie każdej grupy dokonałem uogólnienia, aby przedstawić główne cele, jakie stawiają sobie do osiągnięcia przedstawiciele każdej z nich;*

techniki oraz definicje zostaną bardziej szczegółowo omówione w rozdziale II;

2. „cracking" to analiza kodu programu, po jego zdeasemblowaniu, dokonywana w celu odnalezienia fragmentu tego kodu odpowiadającego za rejestrację programu i odpowiedniej jego modyfikacji, umożliwiającej korzystanie[70]; jest to też metoda (bardzo szczególna) poznania języka maszynowego (asemblera), bądź znajdowania w programach luk; swoistą odmianą (nie noszącą znamion przestępstwa) jest wzajemne crackowanie napisanych przez siebie programów (tzw. „crackme"); często „cracking" określany jest mianem *„reverse engineering'u"*;

3. „phreaking" – „phreakerów" można określić mianem protoplastów dzisiejszych „hackerów"; są to specjaliści zajmujący się (w uproszczeniu) przełamywaniem zabezpieczeń telefonicznych, zazwyczaj w celu uzyskiwania darmowych połączeń[71]. „Phreaker'ami" byli np. Steve Jobs i Steve Wozniak (późniejsi twórcy komputera 'Apple'), którzy też zbudowali (z pomocą Johna Draper'a[72]) pierwszy „blue box"[73].

4. "carding" – technika oszustw związanych z kartami płatniczymi (kredytowymi, bankomatowymi) i telefonicznymi; przede wszystkim polega ona na zdobywaniu numerów kart istniejących lub generowaniu fałszywych (np. za pomocą programów wykorzystujących charakterystyczne cechy systemów kart) i dokonywaniu za ich pomocą transakcji;

5. pisanie wirusów – zakres tej materii jest niezwykle szeroki; wirus komputerowy to program, zwykle niewielkich rozmiarów, „przyklejający się" do innego programu (infekcja), ukrywający i samoreplikujący swój kod (replikacja), który także może ulegać, w trakcie procesu replikacji, przeobrażeniu (mutacji); zarażony plik staje się nosicielem kodu wirusa i zaraża inne pliki; wirusy, w zależności od ich działania, można podzielić na kilka głównych grup[74]; nie jest do końca stwierdzone, kiedy pojawił się

---

[70] jak napisałem powyżej, jest to bardzo duże uogólnienie, cracking bowiem obejmuje swoim zakresem także tworzenie „keygenów", generujących kody odblokowujące, wydobywanie z kodu numerów seryjnych itp.; cechą wspólną wszystkich tych działań jest „deasemblacja" programu i (lub – w przypadku posługiwania się narzędziami takimi jak np. SoftICE) analiza jego kodu;

[71] D. Doroziński – „Hakerzy. Technoanarchiści cyberprzestrzeni.", wyd. Helion 2001, str. 18

[72] alias Cap'n'Crunch; pseudonim wziął się z odkrycia przez niego faktu, że gwizdek dołączony do opakowania pieczywa tej marki potrafi wydobywać dźwięki o częstotliwości 2600 Hz, co pozwalało uzyskiwać darmowe połączenia telefoniczne;

[73] „niebieska skrzynka" pozwala przy tonie 2600 Hz uzyskiwać darmowe rozmowy międzymiastowe; pierwszym z całej serii „skrzynek" był „red box", czyli wybieracz tonowy, generujący dźwięki, który po przeróbce imitował dźwięk wrzucanych monet do automatu; z czasem powstało ponad 40 różnych rodzajów skrzynek;

[74] wirusy plikowo-dyskowe, wirusy MBR, wirusy polimorficzne, ukrywające się, rezydentne itp.;

pomysł napisania takiego programu ani kiedy tego dokonano po raz pierwszy[75]; wirusami szczególnego rodzaju można również określić „konie trojańskie" i „robaki", z tą różnicą, że nie potrzebują pliku-nosiciela;

6. tworzenie / wykorzystywanie robaków sieciowych – pomimo podobieństwa do wirusów komputerowych, robaki stanowią odrębną grupę zagrożeń; robaki – w przeciwieństwie do wirusów – nie potrzebują pliku „nosiciela", poza tym tworzone są zazwyczaj w innym celu – najczęściej działanie robaka polega na skanowaniu sieci w celu znalezienia adresów IP komputerów posiadających niezabezpieczona lukę, którą dany robak wykorzystuje i użycia ich np. w zmasowanych atakach typu DDoS; najsłynniejszym „robakiem" był „Cornell Worm" autorstwa Roberta Tappmana Morrisa[76];
7. „phishing" – nieuczciwe przechwytywanie poufnych danych dzięki podszyciu się po komunikat wysłany z legalnie działającej instytucji i przekierowując użytkownika na fałszywą stronę internetową, na której podaje swoje dane (np. dotyczące konta bankowego)[77]; w tym działaniu wykorzystuje się połączenie metod znanych z dystrybucji spamu z socjotechniką[78],[79]
8. warez (piractwo komputerowe) – pirackie wersje komercyjnego oprogramowania (użytkowego lub gier), zbierane i udostępniane na kilku (kilkudziesięciu) serwerach (przy czym hiperłącza do nich znajdują się na wielu stronach WWW) bez zgody ich autorów;
9. inne – takie jak np. :
    - prezentowanie w Internecie treści zabronionych prawem; dotyczy to zwłaszcza pornografii (ze szczególnym uwzględnieniem pornografii dziecięcej), jak również treści propagujących przemoc, rasizm itp.;

---

[75] wg. D. Dorozińskiego idea została przedstawiona w 1959 r. przez L. S. Penrose'a, który na łamach „Scientific American" opublikował artykuł o samopowielających się strukturach mechanicznych, por. D. Doroziński – Hakerzy ..., op. cit., str. 312; wg. innej wersji, teoretyczne podstawy tworzenia samoreprodukujących się programów zostały wyłożone w pracy dyplomowej Freda Cohena na Uniwersytecie w Dortmundzie, w roku 1980, por. M. Świtała – Wirusy komputerowe. analiza prawnokarna, Poznań 2001; specyficznym rodzajem pisania wirusów były tzw. „wojny rdzeniowe" („core wars"), będące właściwie grami, w których przeciwnicy pisali krótkie programy, mające za zadanie wzajemną eliminację;

[76] historię tego robaka przedstawiłem w rozdziale I;

[77] http://www.vagla.pl;

[78] M. Maj – Sieć zagrożeń w sieci Internet. Raport CERT Polska 2004; http://www.cert.pl

[79] ostatnio coraz częściej postrzega się „phishing" jako poważne zagrożenie – na stronach internetowych banków znajduje się coraz więcej ostrzeżeń i zasad postępowania – np. http://mbank.pl;

- „spamming" – „zalewanie" adresatów poczty elektronicznej niezamówioną i niechcianą korespondencją, zawierającą różnoraką treść (taką jak „nigeryjski szwindel" czy też pornografią, ale nie tylko); odmianą spamu wykorzystującą komunikatory internetowe jest „spim"[80][81]

- „bluesnarfing" – technika wykorzystująca lukę w systemie bezpieczeństwa modeli telefonów komórkowych wyposażonych w Bluetooth, pozwalająca na pobranie informacji z telefonu komórkowego bez wiedzy i zgody jego właściciela[82]; mianem tym można określić wszelkie działania zmierzające do wykorzystania komunikacji za pomocą technologii BT w celu uzyskania dostępu do systemu;

- „wardriving" – wyszukiwanie (np. w miastach) punktów dostępowych sieci bezprzewodowych, w wielu przypadkach niezabezpieczonych; samo „wejście" do takiej sieci, w związku z redakcją art. 267 § 1 („przełamanie zabezpieczeń) nie stanowi przestępstwa;

- „cybersquatting" – oszustwo domenowe ('domain name grabbing') polegające na rejestrowaniu atrakcyjnych nazw domen internetowych i późniejszym ich odsprzedawaniu;

W związku z nieustanną ewolucją techniczną, a co za tym idzie, ewoluowaniem działań przestępczych, powyższą listę można wzbogacać o nowe elementy niemal w nieskończoność – można przykładowo wymienić takie zachowania jak :hacktivism" (skrzyżowanie „hackingu" z aktywizmem, „hacking" ukierunkowany ideologicznie)[83], „cyberstalking" (dręczenie ofiary za pomocą telefonu / internetu przez nieznaną osobę, powodujące poczucie zagrożenia)[84], czy też „baiting", czyli „oszukiwanie oszustów", wiązanie ich zasobów bezsensownymi czynnościami[85]. Ponadto można się spotkać z terminem „scamming", obejmującym zakresem znaczeniowym tradycyjne oszustwa i wyłudzenia przeniesione na warunki Sieci (piramidy finansowe, fałszywe loterie, konkursy itp.)[86].

---

[80] *http://www.vagla.pl;*
[81] *w lutym br. w Stanach Zjednoczonych po raz pierwszy aresztowano sprawcę „spimmingu" - http://www.biznesnet.pl/pp/16066/Aresztowany-za-spam-na-komunikatory*
[82] *http://www.vagla.pl;*
[83] *Więcej o zjawisku w rozdziale poświęconym „hackingowi";*
[84] *szersze omówienie zjawiska znajduje się w raporcie „1999 Report on Cyberstalking : A new challenge for law enforcement and industries", dostępnym pod adresem: http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm;*
[85] *http://www.vagla.pl/definicje.htm;*
[86] *B. Szewczyk – Przestępstwa internetowe; http://stud.wsi.edu.pl/~dratewka/crime/przestepczosc.htm;*

Wyżej wymienione typy przestępczego działania są najczęściej stosowanymi metodami, z jakimi można się spotkać w cyberprzestrzeni, rzadko kiedy jednak występują one w stanie „czystym". Najczęściej spotyka się połączenie kilku różnych metod (zawirusowanie systemu, będące wynikiem spammingu w celu instalacji konia trojańskiego, bądź robaka, aby przejąć kontrolę nad atakowanym systemem w celu późniejszego wykorzystania go – jako komputera „zombie" – do ataku typu DDoS). Częstokroć, choć same wypełniają znamiona czynów typizowanych w przepisach karnych, stanowią formę stadialną przestępstwa „właściwego", czyli działania prowadzącego do wystąpienia skutku, o który chodzi sprawcy.

2.3 Sposoby zabezpieczeń.

Rozważając kwestię ochrony systemów przed atakami różnego rodzaju należy zacząć od dwu kwestii, które co prawda stały się obecnie niemal truizmem, lecz nadal są jak najbardziej obowiązujące. Pierwsza dotyczy samej osoby użytkownika – powtarzane od lat przez wszystkich specjalistów branży IT słowa, że najlepszym, a na pewno podstawowym, zabezpieczeniem, jest świadomy użytkownik. Kwestia druga dotyczy dynamiki ochrony – wiąże się ze świadomością użytkownika o ciągłej ewolucji metod przestępczego działania, w związku z czym jest on na bieżąco z najnowszymi metodami ochrony. Konieczna jest korelacja świadomości użytkownika co do istnienia zagrożeń i ich rodzaju z podejmowanymi, adekwatnymi działaniami, wspartymi środkami technologicznymi.

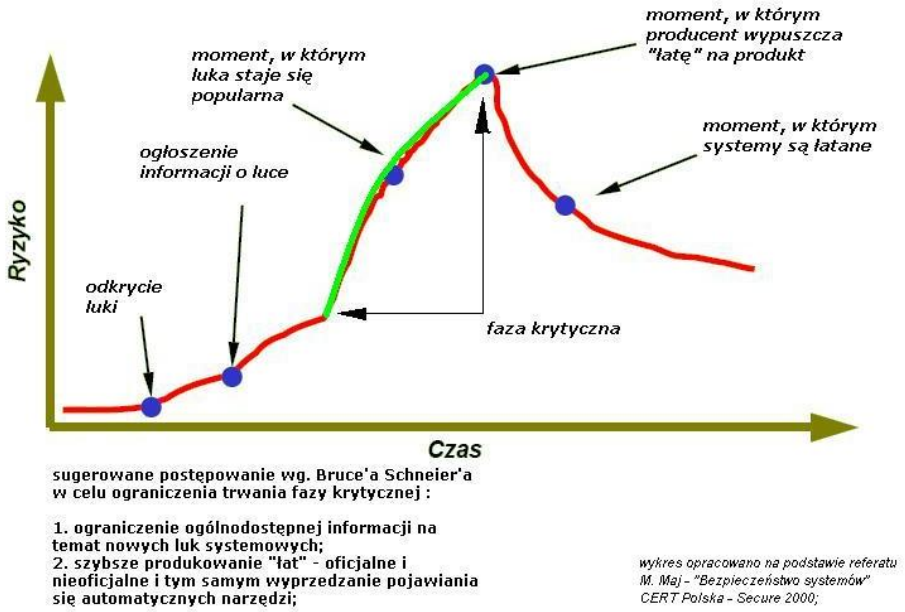
Świadomy użytkownik jest podstawą zabezpieczenia systemu komputerowego przed atakiem. Świadomość ta powinna obejmować zagrożenia systemu, jak i podstawową umiejętność zapobiegania im. Na gruncie „lokalnym", czyli odosobnionego systemu (użytkownika prywatnego) działania zapobiegawcze koncentrują się na instalacji oprogramowania antywirusowego, *firewalla*, programu do wyszukiwania złośliwego oprogramowania i właściwej ich konfiguracji. Można to uznać za niezbędne minimum. Ponadto trzeba pamiętać o usuwaniu podejrzanych załączników z poczty elektronicznej bez ich otwierania, okresowej zmianie haseł dostępu oraz pełnym skanowaniu antywirusowym minimum raz w tygodniu. Jak stwierdziłem na samym początku, są to rzeczy powtarzane przez wszystkich ludzi związanych z bezpieczeństwem systemów komputerowych i obecnie stały się niemal banałem, ale zdziwienie może budzić, jak wielu użytkowników jeszcze o tych zasadach nie słyszało, bądź się do nich nie stosuje.

Temat dynamiki ochrony praktycznie wyczerpuje ciągła aktualizacja stosowanych przez użytkownika zabezpieczeń – w tym przypadku oprogramowania. Co kilka dni pojawiają się kolejne *update'y* programów antywirusowych, *firewalli*, *anti-spyware'ów*, zawierające definicje nowych, dopiero co powstałych „złośliwych programów". Niemniej

ważną kwestią jest instalowanie „łat" do systemów operacyjnych, *service pack'ów"* i innych dodatków pojawiających się – dość często – na internetowych stronach producentów. Ponadto aktualizacją należy objąć oprogramowanie instalowane na komputerze – zwłaszcza te, za pomocą którego komputer łączy się z siecią. Główną grupę stanowią w tym momencie przeglądarki internetowe, przez które odbywa się duża część ataków, a to z powodu luk, jakie w sobie zawierają oraz ich powszechności. Niesławnym liderem w tej kategorii jest powszechnie nadal używany Internet Explorer Microsoftu (korzysta z niego ok. 75 % internautów[87]), w którym, w okresie od stycznia 2003 r. do grudnia 2004 r., wykryto 58 luk, z których 24 zasługiwało na miano „luk krytycznych"[88], stanowiły więc one 41 % wszystkich luk programu (dla konkurencyjnych przeglądarek takich jak Firefox, Mozilla i Opera wskaźniki te wynosiły kolejno 11, 12 i 13 %)[89]. Jeszcze gorzej statystyka przedstawia się pod kątem stopnia „załatania" luk – MS Internet Explorer jako jedyna przeglądarka nie miała „zalatanych" wszystkich „luk krytycznych", z których najstarsza datuje się na 14 sierpnia 2003 r.[90] Lekkie traktowanie przez producenta dysfunkcji zawartych w jego oprogramowaniu budzi uzasadnione obawy zwłaszcza gdy pod uwagę weźmie się fakt, że skutkiem rozwoju technologicznego jest m. in. skrócenie czasokresu pomiędzy ogłoszeniem luki, a powstaniem narzędzia, które ją wykorzystuje – przykładem może być robak „Witty", który pojawił się dwa dni po ogłoszeniu istnienia luki, jaką wykorzystywał[91]. Należy dodać, iż działania użytkownika w celu zabezpieczenia swojego systemu mogą pójść dalej niż korzystanie z publikowanych łat. Można stwierdzić, że niezbędnym staje się także działanie „aktywne", czyli gromadzenie wiedzy na temat stanu otoczenia i ewentualnych, pochodzących stamtąd zagrożeniach[92]. Przykładem celowości takiego działania jest ogłaszane od dłuższego czasu przez specjalistów z branży zabezpieczeń pojawienie się robaków wykorzystujących tzw. „0-day exploit", czyli skrypt wykorzystujący lukę w oprogramowaniu, której jeszcze oficjalnie nie ogłoszono.

---

[87] M. Maj, P. Jaroszewski – „Bezpieczeństwo przeglądarek internetowych"; źródło : CERT Polska, http://www.cert.pl;
[88] objaśnienia pojęć zawarte są w treści raportu, j. w.;
[89] ibidem;
[90] ibidem;
[91] CERT Polska, Raport 2004 – Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w 2004 roku; źródło : CERT Polska, http://www.cert.pl;
[92] J. Siwek – Cele sił zbrojnych – zdolność reagowania na incydenty komputerowe; materiały konferencji Secure 2003; źródło : CERT Polska, http://www.cert.pl;



rys. 3 – cykl życia luki systemowej; (*źródło : CERT Polska*[93]*)*

Rzecz się ma nieco inaczej w przypadku ochrony sieci teleinformatycznej należącej do większej firmy – powyższe wskazania ochronne oczywiście zachowują ważność, ale nie stanowią samoistnej ochrony, tylko stanowią wycinek całości, który określa się mianem „polityki bezpieczeństwa”[94]. Polityka bezpieczeństwa instytucji to „zasady, zarządzania i procedury, które określają, jak zasoby – włącznie z informacjami wrażliwymi – są zarządzane, chronione i dystrybuowane w instytucji i jej systemach komputerowych”[95].

Ochrona informacji realizowana jest na trzech płaszczyznach – technicznej, organizacyjnej i prawnej[96], z czego prawu karnemu, będącemu niejako posiłkową gałęzią prawa, pozostawiono rolę „środka ostatecznego”. Prawo to nie tyle chroni, co wprowadza system sankcji za działania godzące w tą ochronę. Płaszczyzna techniczna obejmuje wszelkie technologie i architekturę systemów teleinformatycznych, projektowane w celu zapewnienia bezpieczeństwa przechowywanym w nich danych, organizacyjna zaś zawiera się w szeroko rozumianym stosowaniu „polityki bezpieczeństwa”.

Zanim wprowadzi się jakikolwiek model ochrony (poniżej przedstawię kilka możliwych opcji) należy odpowiedzieć na pytanie co i przed czym należy chronić. Wg jednej z teorii[97] ochronie podlegają takie elementy jak zasoby materialne (cała infrastruktura produkcyjna lub usługowa), dane (informacje), zasoby komputerowe i reputacja. Ochrona danych obejmuje (w tym przypadku) ich poufność i autentyczność (nie uwzględnia więc

[93] *M. Maj – Bezpieczeństwo systemów; materiały konferencji Secure 2000; źródło : http://www.cert.pl;*
[94] *lub „polityką prywatności”;*
[95] *M. Molski, S. Opala – Elementarz bezpieczeństwa ..., op. cit., str. 46;*
[96] *S. Iwanicki – Przemówienie powitalne [w:] A. Adamski (red.) – Prawne aspekty ..., op. cit., str. 17;*
[97] *Kerberos – Zagrożenia bezpieczeństwa i przedmioty ochrony w systemie informatycznym. Modele bezpieczeństwa; źródło : http://kerberos.w.pl;*

ich dostępności). Zagrożenia poufności danych polegają na przeglądaniu (przeszukiwaniu zasobów w celu uzyskania konkretnych informacji), przenikaniu (działaniu związanym z dostępem do chronionych danych w trakcie legalnych operacji dokonywanych przez upoważnionych użytkowników), wnioskowaniu (wydobyciu niejawnych, szczegółowych danych ze zbioru danych ogólnie dostępnych). Zagrożenia autentyczności danych to zniekształcanie (modyfikacja nie zmieniająca sensowności), powtarzanie (ponawianie pewnych komunikatów, w związku z czym dokonywane są pewne operacje), wstawianie i niszczenie. Ochrona zasobów komputerowych wiąże się z zagadnieniem utrzymywania ich w stanie ciągłej dostępności dla upoważnionych użytkowników, natomiast kwestia ochrony reputacji jest związana m. in. z pozycją rynkową przedsiębiorstwa (np. w związku z zaufaniem klienteli). Jednocześnie podkreśla się (co również uczyniłem wcześniej) niezwykłe znaczenie, jakie dla polityki bezpieczeństwa ma aspekt ludzki[98].

Wyróżnia się następujące modele bezpieczeństwa, jakie są przeważnie stosowane :

- Brak ochrony („model zerowy") – nie stosuje się żadnych zabezpieczeń; stosowany w przypadku uznania istnienia rażącej dysproporcji poziomu ryzyka zagrożenia do kosztów wdrożenia polityki bezpieczeństwa[99];
- Bezpieczeństwo dzięki brakowi zainteresowania ze strony otoczenia – opiera się na przeświadczeniu o małej istotności systemu dla konkurencji i włamywaczy oraz na przeświadczeniu o dużym prawdopodobieństwie braku ataków;
- Ochrona na poziomie poszczególnych komputerów – najszerzej stosowany model ochrony; właściwa na poziomie pojedynczego komputera, ewentualnie małych siec lokalnych, ze względu na zróżnicowanie konfiguracji poszczególnych systemów i złożeniu na poszczególnych użytkowników odpowiedzialności za swoją stację roboczą, może okazać się zawodna w przypadku dużych sieci;
- Ochrona w skali całego systemu (całej sieci komputerowej) – polega na kontroli dostępów i usług poprzez sieć (a nie jak w przypadku poprzednim poszczególnych maszyn) za pomocą takich narzędzi jak procedury uwierzytelniania, architektury uwierzytelniające czy też szyfrowanie;[100]

[98] *Kerberos – Zagrożenia bezpieczeństwa …, op. cit.;*
[99] *jak łatwo zauważyć, przyjęcie tego schematu wyklucza możliwość prawnokarnej ochrony poufności informacji na gruncie art. 267 § 1 KK;*
[100] *Kerberos – Zagrożenia bezpieczeństwa …, op. cit.;*

Poziomy bezpieczeństwa systemów komputerowych zostały zdefiniowane m. in. przez Departament Obrony USA w tzw. „Orange Book" („Trasted Computer Standards Evaluation Criteria"), które przewiduje siedem takich poziomów, a klasyfikacja ma charakter „zawierania", tzn. poziom wyższy zawiera w sobie cechy poziomów niższych i dodatkowo uzupełnienia. Najniższym poziomem bezpieczeństwa jest poziom D1, oznaczający całkowity brak wiarygodności systemu, najwyższym, po poziomach C1, C2, B1 – B3, poziom A1, oznaczający, iż cała konfiguracja sprzętowo-programowa wymaga matematycznej weryfikacji. Jednocześnie zwraca się uwagę na fakt coraz większego obciążenia systemu w związku ze stosowaniem kolejnych poziomów bezpieczeństwa[101].

Należy również pamiętać, że polityka bezpieczeństwa obejmuje (lub powinna) wszelkie sytuacje, które mogą zagrozić niezakłóconej pracy systemu – począwszy od katastrof naturalnych po błędy ludzi. Poniższy wykres przedstawia typy zagrożeń i przybliżoną częstotliwość ich występowania.

rys. 4 – częstotliwość występowania typów zagrożeń systemów komputerowych. *(źródło : CERT Polska)*

Z powyższego wykresu wynika, że w ramach ogólnie pojętych zagrożeń systemów teleinformatycznych ataki z zewnątrz sieci stanowią znikomy odsetek zajść narażających systemy na szkody. Drugą kwestią jest ów „świadomy użytkownik" – sprawca ponad połowy incydentów.

Słusznie podkreśla się znaczenie czynnika ludzkiego w stosowaniu polityki bezpieczeństwa. Z czterech elementów, uznawanych za tzw. „elementy konieczne", tzn. wyjaśnień, podziału odpowiedzialności i kompetencji, jasnych sformułowań i opisów me-

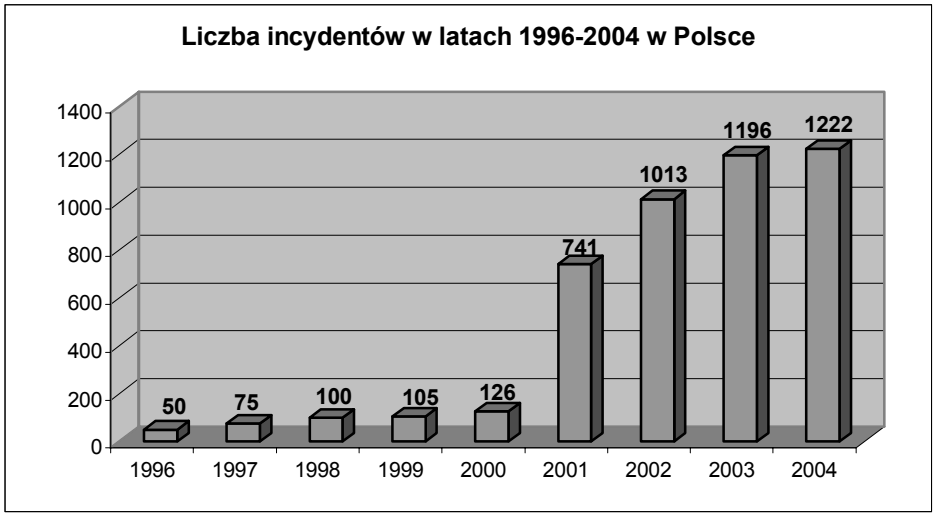
[101] *D. Doroziński – Hakerzy. Technoanarchiści ...., op. cit., str. 345 – 346;*

chanizmu realizacji polityki bezpieczeństwa[102], największe znaczenie autor, pod wpływem własnych doświadczeń, przypisuje pierwszemu. Użytkownik systemu, będącego elementem sieci komputerowej musi zostać przekonany do konieczności poddania się niekiedy dużym ograniczeniom w korzystaniu z systemu – odgórne narzucenie pewnych zasad bez dokładnego wyjaśnienia przyczyn zaowocuje jedynie obchodzeniem takich zarządzeń[103]. Ponadto użytkownik musi mieć świadomość bycia elementem złożonej całości, i w związku z tym ryzyka narażenia na niebezpieczeństwo nie tylko własnego komputera, ale również wszystkich z nim połączonych.

2.4 Statystyki przestępstw – skala zjawiska i straty przez nie powodowane.

Przestępczość „komputerowa" („elektroniczna", „internetowa") jest kategorią działań przestępczych o najwyższym wskaźniku tzw. „ciemnej liczby", czyli przestępstw niewykrytych, bądź wykrytych i niezgłoszonych. Przyczyn takiego stanu rzeczy jest kilka, z których największą rolę spełnia znikoma wiedza informatyczna użytkowników i niechęć zgłaszania incydentów tego rodzaju organom ścigania. Powody tej niechęci również można podzielić na kilka głównych grup. Oczywistym jest, że statystyką można objąć tylko te incydenty, które zostały wykryte i zgłoszone.

Poniższy wykres obrazuje skalę zjawiska według zgłoszeń incydentów do zespołu CERT Polska[104].

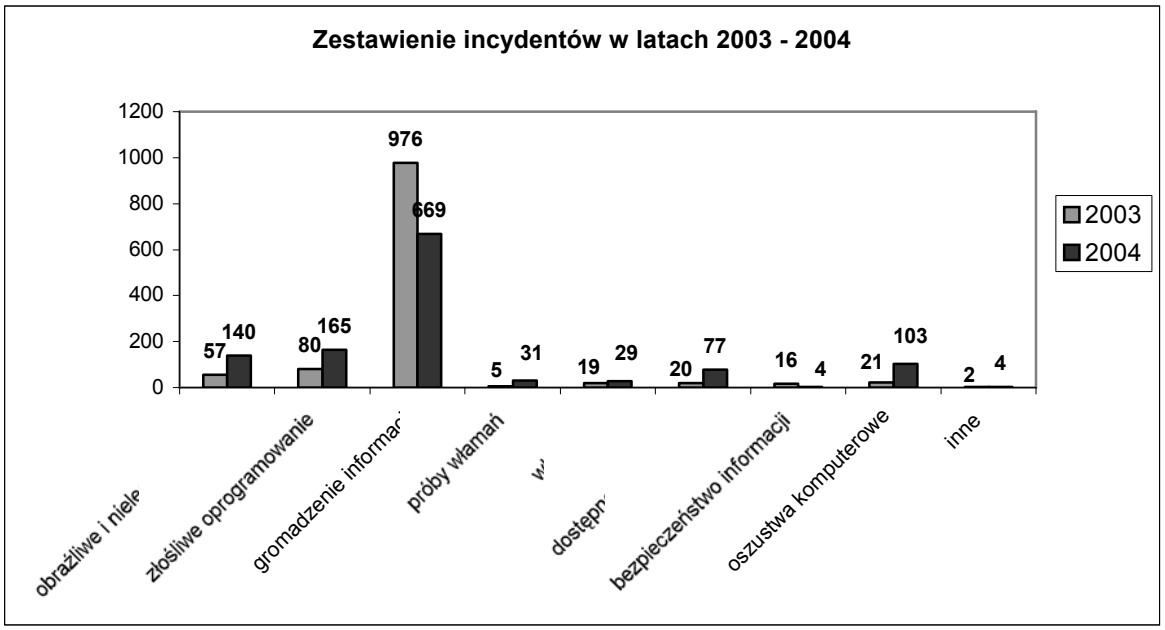


rys. 5 – liczba incydentów komputerowych w Polsce w latach 1996 – 2004. (*źródło : CERT Polska)*

[102] *M. Molski, S.Opala – Elementarz bezpieczeństwa ..., op. cit. str. 48;*
[103] *Autor spotkał się z przypadkami dezaktywacji np. „firewalla" czy programu antywirusowego, ponieważ te blokowały dostęp do zasobów sieci P2P (takich jak bardzo rozpowszechniona KaZaA), lub uniemożliwiały komunikację przy użyciu np. Gadu Gadu, czego efektem było częste zawirusowanie rzeczonych systemów;*
[104] *CERT Polska, Raport 2004 – Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w 2004 roku; źródło : CERT Polska, http://www.cert.pl;*

Jak podkreśla zespół CERT, znikomy wzrost liczby incydentów w ostatnich dwóch latach, jak wynikałoby z wykresu powyżej, jest zwodniczy. Wiele ataków jest z powodu ich automatycznego przeprowadzenia uznana za tzw. „szum sieciowy" i nie zostają zgłoszone, zwłaszcza jeśli nie idą z nimi w parze istotne dla poszkodowanego straty. Zdecydowana większość zgłoszeń ataków zautomatyzowanych pochodzi od wyspecjalizowanych jednostek, które dzięki swojemu charakterowi mogły rozwinąć systemy detekcji[105]. Należy mieć również na uwadze, iż kilkusetprocentowy wzrost liczby incydentów nie wskazuje na faktyczne zwiększenie zjawiska, ile na większą świadomość użytkowników, a przede wszystkim na pokonanie niechęci zgłaszania przez ofiary ataków takich zajść do jednostek reagujących.

Ciekawą kwestią jest rozkład gatunkowy zgłaszanych incydentów, zobrazowany na poniższym wykresie[106].

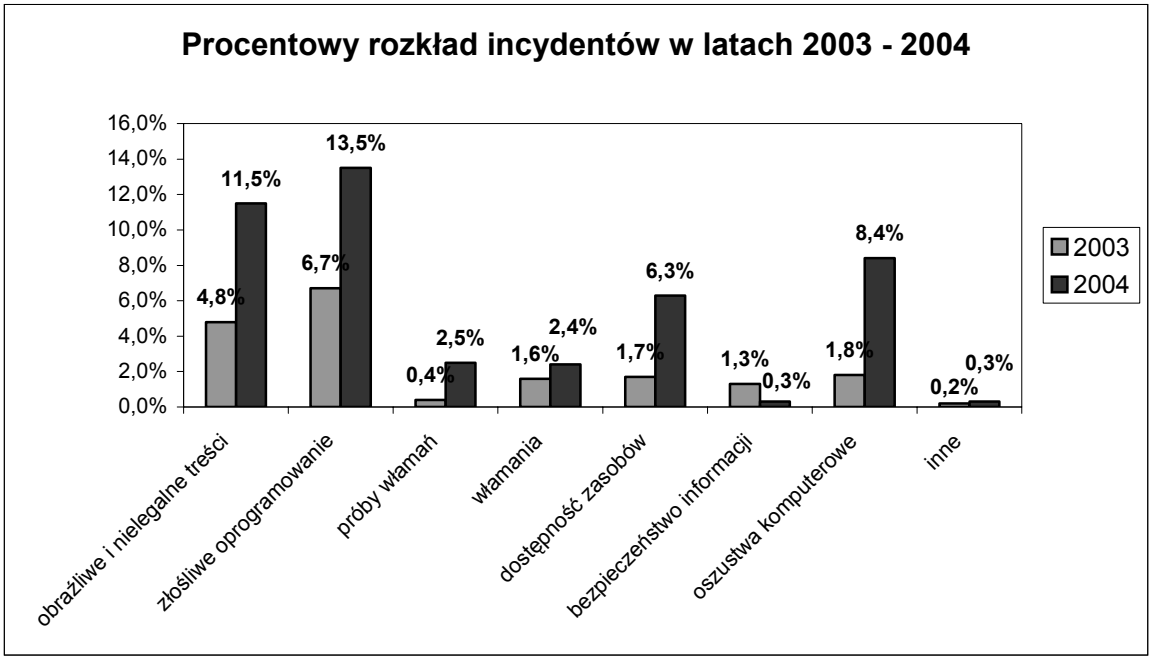


rys. 6 – liczba i rodzaje incydentów w latach 2003 – 2004. (*źródło : CERT Polska)*

Jak widać, zdecydowaną większość incydentów stanowi gromadzenie informacji, a przewaga ta, jak twierdzi zespół CERT Polska, wynika z automatycznego powiadamiania zespołu z zaufanych źródeł, takich jak inne instytucje zajmujące się zapewnieniem bezpieczeństwa sieci. W grupie tej wśród metod działania sprawców na czoło wysunęło się bezkonkurencyjnie skanowanie (659 przypadków na 669 ogółem); ciekawostką może być zarejestrowanie 9 przypadków stosowania „inżynierii społecznej". Ponieważ jednak

[105] *CERT Polska, Raport 2004 – Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w 2004 roku; źródło : CERT Polska, http://www.cert.pl;*
[106] *opracowano na podstawie raportów CERT za rok 2003 i 2004; źródło : http://www.cert.pl;*

tak wielka przewaga jednej kategorii zaciemnia nieco obraz całości, kolejny wykres opuszcza tą kategorię.



rys. 7 – procentowy rozkład incydentów w latach 2003 – 2004. *(źródło : CERT Polska)*

Najwyższy odsetek wśród tak zmodyfikowanej grupy stanowią drażliwe i nielegalne treści oraz złośliwe oprogramowanie. Do pierwszej grupy zaliczają się głównie przypadki *spammingu*, drugą stanowią wirusy i robaki sieciowe, a w mniejszym stopniu konie trojańskie. Ciekawą kwestią jest dość niski wskaźnik włamań i prób włamań, a także naruszeń bezpieczeństwa informacji – co do przyczyn takiego stanu rzeczy można jedynie wysnuć przypuszczenie dotyczące wciąż słabej wykrywalności i niechęci zgłaszania takich incydentów podmiotom zewnętrznym, lub też wielkiej ilości incydentów innego rodzaju, zaciemniających statystykę.

Na pytanie o motyw nie zawiadomienia policji o włamaniu do systemu komputerowego, pokrzywdzeni udzielali przede wszystkim następujących odpowiedzi – „nie zawiadomiłem policji, ponieważ :”[107]

a) nie chciałem, aby policja miała dostęp do systemu – 14,3 %

b) chciałem uniknąć strat związanych z przejęciem systemu przez policję – 14,3 %

c) nie chciałem, aby policja miała dostęp do „wrażliwej” informacji – 12,1 %

[107] *A. Adamski – Prawo karne ..., op. cit., str. 19, tabela nr 9;*

d) nie chciałem, aby wiadomość o zaistnieniu przestępstwa nabrała rozgłosu – 20,9 %

e) nie chciałem ryzykować utraty zaufania klientów – 19, 8 %

f) nie chciałem stracić konkurencyjności na rynku – 8,8 %

Analiza powyższych odpowiedzi dość jasno wskazuje na dwojakie podstawowe motywy starania się przez ofiary nie nadawania rozgłosu incydentom. Pierwszą grupę stanowi niechęć udostępniania policji zasobów zgromadzonych w atakowanym systemie, druga natomiast to konsekwencja istniejących warunków rynkowych – poszkodowany troszczy się, aby nie stracić klienteli przez wzgląd na kondycję prowadzonych przez niego w przyszłości interesów[108]. Pozostaje poniekąd kwestia poniesienia przez poszkodowanego dodatkowych strat związanych z zajęciem przez organy ścigania sprzętu komputerowego – nie potrzeba posiadać szczególnie bujnej wyobraźni, aby uzmysłowić sobie skutki finansowe zajęcia przez Policję serwerów któregokolwiek z wielkich portali internetowych – poza kosztami związanymi z zakupem nowego sprzętu pozostaje jeszcze problematyka *lucrum cessans.*

Kwestią, która również sprawia wiele problemów specjalistom, jest oszacowanie strat powstałych w wyniku incydentów komputerowych. Przyjmuje się w tym celu dwie podstawowe metody obliczeń strat, takich jak I-CAMP[109] i CICA[110], z czego za prostszy w obsłudze (w związku z czym bardziej funkcjonalny) przyjmuje się ten pierwszy[111].

Powyższe algorytmy służą jednak do obliczania kosztów restytucji systemu do stanu sprzed ataku, nie uwzględniają jednakże szkód takich jak np. pozbawienie ofiary spodziewanych zysków. W przypadku ataków na eBay czy Amazon.com ten właśnie element stanowił gros poniesionych przez te portale strat. Dokładne ustalenie wartości może być niekiedy wręcz niemożliwe, a z pewnością najeżone trudnościami i prawie na pewno otrzymane wartości nie będą w stu procentach odpowiadać rzeczywistości (ustalając straty można się posłużyć metodami statystycznymi, uwzględniając średni obrót lub zysk firmy w analogicznym czasie).

Można łatwo zauważyć, na podstawie analizy strat spowodowanych przez najbardziej spektakularne ataki na systemy informatyczne, iż z upływem czasu, rozwojem technologii i ewoluowania metod przestępczych (zwłaszcza w kierunku zautomatyzowania i uproszczenia przeprowadzanych ataków) zwiększają się koszta przywrócenia pracy za-

---

[108] w związku z powyższym w stanie Kalifornia rozważa się wprowadzenie – ze względu na ochronę klienta, będącego najczęściej nieświadomym - obowiązku zgłaszania incydentów przez podmioty przetwarzające dane osobowe;
[109] Incident Cost Analysis and Modeling Project;
[110] Cyber Incident Cost Assessment;
[111] M. Maj – Metoda szacowania strat powstałych w wyniku ataków komputerowych, materiały konferencji Secure 2002; źródło : CERT Polska, http://www.cert.pl;

atakowanych systemów do stanu pierwotnego. Kwestią równie interesującą jest, olbrzymia niekiedy, rozpiętość podawanych strat dotyczących tego samego ataku w zależności od źródła, które o tym informuje. Niekiedy jest to spowodowane zastosowaniem kilku metod szacowania strat i uwzględniania różnych czynników. Problematyczne jednak staje się zawarcie takich szacunków w akcie oskarżenia przeciwko sprawcy[112]. Przykładem może być słynna już sprawa rosyjskiego programisty, Wladimira L., który „włamał" się do systemu komputerowego Citibanku w 1994 r.; w zależności od źródła podającego tą informację szkody (a w tym przypadku uwzględniano jedynie wartość kilkudziesięciu przelewów, jakich sprawca dokonał, a nie koszta przywrócenia sprawności działania systemu) osiągnęły wartość od 2.7 miliona USD[113] do 10[114] - 11 [115]milionów USD. Podobnym przypadkiem był wspomniany już „*Cornell Worm*" R. Morrisa – straty związane z przestojem 6000 komputerów oszacowano na 5-12 milionów USD[116]. Problem dokładnego oszacowania strat istnieje także w kwestii karnoprocesowej – niekiedy, tak jak w Stanach Zjednoczonych, wręcz warunkuje istnienie przestępstwa (przestępstwo federalne ma miejsce, gdy straty poniesione w wyniku incydentu przekraczają wartość 5 tysięcy USD).

Powyższe statystyki odnoszą się głownie do lokalnych realiów i choć również mogą być przyczyną obaw i zastanowienia, warto się zapoznać z – szacunkowymi co prawda – statystykami w skali globalnej. Przykładowo, szacuje się, że straty spowodowane działalnością samych tylko robaków sieciowych sięgają miliardów USD, a jest to wynik zablokowania, np. poprzez ataki DDoS, internetowych węzłów komunikacyjnych, serwisów sieciowych, serwerów dostarczycieli usług internetowych, co z kolei uniemożliwia komunikację (wewnętrzną i zewnętrzną) przedsiębiorstw, banków i innych instytucji zajmujących się działalnością komercyjną. Wg firmy Mi2g straty spowodowane działalnością robaka „Code Red" sięgnęły 2.6 miliarda USD, a robaka „Slammer" – 1.2 miliarda[117]. Szkody wynikłe z infiltracji lokalnych systemów komputerowych przez outsidera są, w porównaniu z powyższymi wartościami, relatywnie niewielkie – wśród ankietowanych ofiar ingerencji w systemy zdecydowana większość poszkodowanych zgłaszało straty powyżej 50 tys. USD, z czego największy odsetek respondentów (19.0 %) oceniało swoje straty na mieszczące się w zakresie 200 – 500 tys. USD. Natomiast na więcej niż 1 milion USD

---

[112] np. w przypadku gdy rozmiar szkody ma wpływ na kwalifikację prawną czynu tak jak przykładowo będzie to dość istotna kwestia w chwili stawiania sprawcy zarzutu popełnienia czynu z art. 268, którego kwalifikowana forma § 3 uzależniona jest od wyrządzenia znacznej szkody majątkowej;
[113] P. Kościelniak – Nikt nie jest bezpieczny, Rzeczpospolita z dnia 8 maja 1997 r.;.
[114] P. Kościelniak, M. Kopyt – „Sieć apokalipsy". Elektroniczne przestępstwa, Rzeczpospolita z dnia 6 listopada 1997 r.; także A. Adamski – Prawo karne ..., op. cit., str. 119;
[115] http://gicek.tripod.com/;
[116] A. Adamski – Prawo karne ..., op. cit., str. 45 przypis 1; w źródłach internetowych można spotkać się z szacunkiem strat sięgającym 100 milionów dolarów, co wydaje się jednak wartością mało realną; por. : D. Doroziński – Hakerzy, Technoanarchiści ..., op. cit., str. 47;
[117] S. Górniak – Robaki sieciowe – historia i studium przypadku; materiały konferencji SECURE 2003 ; http://www.cert.pl;

swoje straty wyceniało 17,9 % poszkodowanych. W badaniach CSI/FBI z 1998 r. średnią wartość szkody, będącej wynikiem „kradzieży informacji mającej znaczenie majątkowe" oszacowano na 1.677 miliona USD. Koszty sprawdzenia i ponownej instalacji systemu, którego integralność została naruszona w wyniku nieuprawnionej ingerencji wahają się – wg danych brytyjskich – od 30 tys. funtów w przypadku lokalnej sieci komputerowej do 26 milionów funtów w przypadku weryfikacji dużej bazy danych[118].

2.5 Wybrane zagadnienia problematyki ścigania „przestępstw komputerowych"

Problematykę ścigania przestępstw komputerowych można podzielić na dwie główne grupy, a mianowicie na kwestie związane z wykrywaniem tych przestępstw i na problemy powstające w trakcie ścigania. Osobną kwestią, niemniej istotną, jest cały mechanizm współpracy międzynarodowej w materii przestępczości komputerowej, obejmujący nie tylko wzajemną pomoc w trakcie czynności operacyjnych, czy też dostosowanie prawa wewnętrznego do ogólnych standardów, lecz również np. wzajemne szkolenia personelu i wymianę doświadczeń na tym polu.

Zjawisko przestępczości komputerowej, jak pisałem powyżej, posiada bardzo specyficzne cechy, a charakteryzuje się, cytując bardzo lapidarne określenie, czterema podstawowymi cechami : dużą „ciemną liczbą", niskim prawdopodobieństwem wykrycia sprawcy, niechętnym informowaniem organów ścigania o zaistniałych incydentach przez pokrzywdzonych oraz lekceważeniem przez użytkowników zasad bezpieczeństwa[119]. Ściganie przestępstw należących do tej kategorii napotyka poważne problemy, często dotychczas niespotykane w przypadkach ścigania przestępstw „tradycyjnych".

Praktycznie te cztery cechy, jeśli dodać do nich piątą, a mianowicie transgraniczność, wyczerpują niemal całkowicie materię podstawowych problemów związanych ze ściganiem incydentów wymierzonych w poufność, integralność i dostępność informacji. Poza nimi istnieją problemy związane z zapleczem ludzkim i technicznym – nieustanny postęp rozwoju technologii pozostawia w tyle organy ścigania zarówno jeśli chodzi o poziom wiedzy technicznej jak i używany przez nie sprzęt.

Duża wartość „ciemnej liczby" spowodowana jest najczęściej faktem niezauważenia przez poszkodowanego ingerencji w system – i tak, przytaczając po raz kolejny przykład ataku typu DDoS, do jego przeprowadzenia konieczne jest przejęcie kontroli nad kilkudziesięcioma / kilkuset komputerami, a odbywa się to najczęściej za pośrednictwem robaka. W takiej sytuacji użytkownik komputera „zombie" może nie zauważyć, że jego

[118] *A. Adamski – Prawo karne ..., op. cit., str. 21 – 22;*
[119] *A. Adamski – Prawo karne ..., op. cit., str. 17;*

sprzęt służy jako narzędzie ataku, lub, co najwyżej, stwierdzi obecność złośliwego kodu i usunie go za pomocą programu antywirusowego. Szacuje się, że w skali roku ma miejsce ok. 20 milionów nadużyć komputerowych[120]. W przypadku zmasowanego ataku DDoS, w którym bierze udział kilka tysięcy komputerów, mamy do czynienia z tysiącami przypadków przestępstw komputerowych, z których większość zostanie niezauważona, bądź potraktowana marginalnie. Jest to kolejny przykład na to, iż wiedza jest potrzebna nie tylko sprawcy do popełnienia przestępstwa, lecz także ofierze, by mogła stwierdzić, że stała się ofiarą. Przestępstwo, którego popełnienie nie zostało zauważone, dla organów ścigania nie istnieje.

Drugą cechą jest niska wykrywalność sprawcy – ta kwestia również nie powinna budzić zdziwienia, jako że najczęściej sprawcy „zawodowi" maskują swoje działania do tego stopnia, iż wręcz niemożliwe jest stwierdzenie popełnienia przestępstwa, a jeśli już, to niemożliwa jest identyfikacja sprawcy. W najlepszym wypadku możliwe jest ustalenie numeru IP komputera, z którego dokonano przestępstwa i tutaj droga się kończy – „Sam numer IP komputera nie wystarcza, by wskazać osobę, która z niego korzystała. Numerowi IP nie da się postawić zarzutów"[121].

O tym, jak duży odsetek poszkodowanych, po stwierdzeniu faktu stania się ofiarą przestępstwa komputerowego, informuje o tym organy ścigania i jakie są główne przyczyny takiego stanu rzeczy pisałem w poprzednim podrozdziale. Wcześniej również poruszyłem problematykę „świadomego użytkownika", wiążącą się ściśle z zachowaniem podstawowych zasad bezpieczeństwa, a także ze zdolnością stwierdzenia faktu bycia celem ataku.

Opisane pokrótce elementy składają się na „ciemną liczbę" kategorii przestępczości komputerowej, która stanowi jednak tylko jedną płaszczyznę szeroko rozbudowanej problematyki ścigania bezprawnych zachowań w środowisku sieci teleinformatycznych. Niemniej ważną, lub wręcz ważniejszą, jest kwestia problemów wyłaniających się przed organami ścigania w trakcie prowadzenia czynności operacyjnych w przypadkach przestępstw stwierdzonych i zgłoszonych. W tym momencie ujawnia się całkowicie specyfika środowiska , w jakim zdarzenia te zachodzą.

Mając na względzie ponadgraniczny charakter omawianej przestępczości największym problemem, z jakim borykają się organy ścigania, jest kwestia spełnienia warunku podwójnej karalności. Jest to o tyle istotne, iż w realiach infostrad miejsce działania sprawcy i miejsce wystąpienia skutku mogą się znajdować na przeciwległych krańcach globu. Jak już pisałem, niespełnienie tego warunku skutkowało niemożnością postawienia

[120] *ibidem*
[121] *P. Waglowski – Aby spać mógł ktoś; http://www.vagla.pl/felietony/felieton_050.htm;*

zarzutów autorom wirusa „I love you", a jest to tylko jeden, szeroko nagłośniony przypadek. Podobnie rzecz się ma z każdym z zachowań przestępczych związanych z technologią przetwarzania danych. Inną kwestią jest współpraca międzynarodowa w zakresie wzajemnej pomocy w sprawach karnych. Sprawca, przesyłający nielegalne treści (np. „dziecięca pornografia"[122]) przy pomocy spamu może niekiedy czuć się bezpieczny, jeśli prawo karne miejsca jego pobytu nie przewiduje karalności działalności danego rodzaju[123].

Problematykę karnoprocesowych aspektów przestępczości komputerowej bardziej szczegółowo przedstawię przy okazji omawiania Zalecenia Nr (95) 13, tutaj zaznaczę jeszcze jeden, dość istotny, element, a mianowicie kwestię wiedzy. Jak wspominałem wcześniej, przestępcy posługujący się komputerem i dokonujący czynów godzących w poufność, integralność i dostępność systemów i danych informatycznych dysponują bardzo wysokim poziomem wiedzy, co determinuje konieczność podnoszenia kwalifikacji pracowników organów ścigania do, co najmniej, takiego samego poziomu. Biorąc pod uwagę różnorodność metod przestępczego działania, technik ataków, mnogość celów, a także szeroki asortyment oprogramowania i systemów operacyjnych, z jakich korzystają sprawcy, proces tworzenia wyspecjalizowanych jednostek policyjnych, powołanych do ścigania tego rodzaju przestępstw z konieczności musi być traktowany jak program wieloletni. Podobnie rzecz się ma z innymi organami wymiaru sprawiedliwości – gwarancją prawidłowego przebiegu postępowania sądowego w sprawie o popełnienie przestępstwa komputerowego jest minimalna chociaż wiedza sędziego w tej materii, że o wysokim stopniu wyspecjalizowania biegłego nie wspomnę[124]. Skuteczne ściganie przestępcy, którego sprawność działania powodowana jest jego wiedzą wymaga od ścigających posiadania co najmniej tego samego stopnia wyspecjalizowania w danej dziedzinie.

---

[122] używam takiej pisowni ze względu na trudności w definiowaniu pojęcia - por. P. Waglowski – Spam ofensywny seksualnie, [w:] J. Kosiński (red.) – Przestępczość teleinformatyczna. Materiały seminaryjne Szczytno 2004;

[123] przypadek własny autora – po otrzymaniu materiałów o charakterze pornograficznym z udziałem dzieci przy pomocy poczty elektronicznej przesłałem je do organów ścigania; odpowiedź otrzymałem po kilku tygodniach, z której wynikało, że niewiele można uczynić, jeśli serwer znajduje się poza granicami Polski; opis przypadku znajduje się pod adresem : http://www.vagla.pl/felietony/felieton_050.htm;

[124] kwestię biegłego w procesie karnym porusza Piotr Waglowski w felietonie „And justice for all dot com" http://www.vagla.pl/felietony/felieton_001.htm;

3. Rozdział III – „Hacking" i hackerzy – analiza zjawiska.

Do zjawiska „hackingu" i środowiska „hackerów", przy każdej próbie analizy, należy podchodzić z należytą ostrożnością. Ludzie tworzący podziemie, zwłaszcza należący do elity, doskonale wiedzą, iż nawet w przypadku inwigilacji systemu, nie dokonując w nim żadnych zmian, przekraczają granice prawa. Z tego powodu jedną z głównych cech charakteryzujących „hackerów" jest dyskrecja dotycząca własnej działalności.

3.1 Hackerzy. Niejasności terminologiczne.

Skąd wzięło się określenie „hacker" i co właściwie ono oznacza ? Podstawą jest „***hack*** – 1. po/siekać, po/rąbać, po/ciąć, po/krajać; ***to ~ one's chin*** zaci-ąć/nać się (przy goleniu 2. kop-nąć/ać (przeciwnika) w goleń 3. pokiereszować (pacjenta); pokrajać nieudolnie (pieczeń) 4. obcios-ać/ywać 5. kaszleć suchym urywanym kaszlem."[125], „hacker" zaś to cieśla (stolarz) korzystający w swej pracy z siekiery.

Słowniki, które definiują to pojęcie, są zazwyczaj wydawnictwami branży informatycznej, co nie wpływa jednak na jednorodność definicji :

- „osoba stawiająca sobie za cel łamanie reguł pracy w Internecie. Za punkt honoru stawia sobie wynajdywanie luk w systemach zabezpieczeń. Lubi podglądać cudze zasoby"[126]
- „entuzjastyczny użytkownik komputera"[127]
- „ktoś, kto jest w stanie używać lub modyfikować informacje zgromadzone w obcych komputerach"[128]
- „ktoś, kto uwielbia badać każdy szczegół systemu komputerowego", „obsesyjny programista", „ekspert od dowolnego programu"[129]
- „hobbysta komputerowy próbujący włamywać się do cudzych elektronicznych „skrzynek pocztowych", banków danych itp. dla zabawy albo

[125] *J. Stanisławski – Wielki słownik angielsko-polski. Wiedza Powszechna 1975*
[126] *„Internet od A do Z", str. 48;*
[127] *„The Little Oxford Dictionary" [w:] D. Doroziński - "Hakerzy. Technoanarchiści cyberprzestrzeni", op. cit., str. 16;*
[128] *„Longman" [w:] „Hackerzy ..." op. cit., str. 16;*
[129] *„Jargon Dictionary";*

dla zdobycia różnych tajnych danych jak haseł, numerów, stanów kont itd."[130]

- 1. programista posiadający umiejętność pisania programów bez uprzedniego opracowywania algorytmów, 2. użytkownik maszyny cyfrowej posiadający (przypadkowo) dostęp do chronionych danych, 3. entuzjasta informatyki[131]

Najpełniejszą i najlepiej oddającą charakter środowiska jest definicja zaproponowania przez Erica Raymonda w „The New Hacker's Dictionary", wg której „hacker" to „1. Osoba znajdująca przyjemność w poznawaniu systemów komputerowych oraz w jak najpełniejszym wykorzystaniu ich możliwości, w przeciwieństwie do większości użytkowników zadowalających się jedynie niezbędnym minimum. 2. Ktoś, kto z entuzjazmem (a nawet obsesją) oddaje się programowaniu zamiast teoretyzować na ten temat. 3. Osoba potrafiąca usprawnić wynik pracy innego hakera, dodać coś od siebie 4. Osoba potrafiąca biegle i szybko programować. 5. Ekspert odnośnie pewnego programu lub systemu, także ktoś wykonujący pracę z jego pomocą; przykładowo: "haker Uniksa". (Definicje od 1 do 5 są powiązane, a odpowiadające im osoby mogą należeć do kilku opisywanych grup) 6. Ekspert lub entuzjasta dowolnej dziedziny. Przykładowo, ktoś może być hakerem astronomii. 7. Ktoś, kto znajduje przyjemność w podejmowaniu intelektualnych wyzwań jakie niosą ze sobą przezwyciężanie lub omijanie napotykanych ograniczeń. 8. [z dezaprobatą] Obdarzony złymi intencjami ciekawski starający się wszelkimi możliwymi środkami wykraść poufne informacje. Stąd pochodzą: "haker haseł" oraz "sieciowy haker". Właściwym terminem dla takiego znaczenia jest cracker."[132]

Jakie były początki używania pojęcia ? Było to żargonowe określenie, wywodzące się ze środowiska programistów, a określało ludzi, którzy wzajemnie *„hackowali"*, czyli testowali, napisane przez siebie programy, w celu wyeliminowania w nich błędów, „dziur" („bugs")[133]. Razem z rozwojem Sieci (początkowo ARPANet'u, później Internetu) *„hackowali"* także administrowane przez siebie systemy – także w tym samym celu. Trudno więc nie uznać faktu, iż działania te przynosiły korzystne wyniki, trzeba jednocześnie pamiętać, że odbywały się one za zgodą autora programu czy też administratora systemu[134].

---

[130] W. Kopaliński – Słownik wyrazów obcych ..., op. cit.; ciekawostką jest wywodzenie pojęcia od niemieckiego słowa „hacken" – przylepiać się;
[131] A. Marciniak, M. Jankowski – Słownik informatyczny angielsko – polski, PWN 1991;
[132] http://www.ws-webstyle.com/cms.php/en/netopedia/bezpieczestwo_hacking/haker;
[133] A. Adamski – Prawo karne ..., op. cit., str. 3
[134] przeprowadzenie tzw. „audytu bezpieczeństwa" sieci komputerowej to również nic innego, jak próby jego „hackowania" mające na celu wskazania jego słabych punktów;

Określenie „hacker” ma obecnie dwa główne znaczenia : komputerowy pasjonat (chociaż pojęciem w tym znaczeniu posługuje się obecnie bardzo wąska grupa użytkowników komputerów) lub cyberprzestępca – różnica tkwi wyłącznie w wyobrażeniu oceniającego, gdyż zasadniczo nie ma jasno wytyczonej granicy pomiędzy tymi dwoma spojrzeniami. „Hacker” to przede wszystkim osoba niezwykle uzdolniona w kierunku informatyki, będąca przy tym komputerowym entuzjastą, którą kieruje chęć poszerzania swojej wiedzy, natomiast fakt, czy staje się przestępcą, czy nie jest determinowany dopiero przez sposób jej wykorzystania.

Chciałbym jednocześnie wyjaśnić różnicę pomiędzy tymi dwoma głównymi grupami, których członków określa się mianem „hackera”. Różnica ta polega na celu podejmowanych działań, ma więc (lub powinna mieć) odbicie w kwalifikacji prawnej. Do pierwszej grupy należy zaliczyć komputerowych entuzjastów, „grzebiących” w systemach w celach „edukacyjnych”, poznających zasady ich działania, luki w zabezpieczeniach itp. dla własnej satysfakcji. Złamanie zabezpieczeń systemu jest dla nich celem samym w sobie – nierzadko po włamaniu informują o tym fakcie administratora „zhackowanego” systemu wskazując lukę w zabezpieczeniach. Często przy tym przekraczają granice ustalone prawem, rzadko kiedy jednak dokonują jakichkolwiek szkód np. w spenetrowanych systemach, lub działają z chęci zysku, choć niewątpliwie działają na granicy prawa, lub ją przekraczają. Motywuje ich powiększenie swojej wiedzy, ewentualnie podniesienie prestiżu w środowisku (należy pamiętać, że w środowisku „undergroundu” jedno łączy się nierozerwalnie z drugim). Do drugiej grupy zaliczyć można osoby, dla których przełamanie zabezpieczeń systemu jest tylko środkiem prowadzącym do celu – może nim być kradzież danych, zmiany w systemie, sabotaż. Członkowie tej grupy mogą działać na zlecenie (kradzież danych, unieruchomienie serwera konkurencji), bądź też z własnych pobudek (zemsta na byłym pracodawcy). Można więc określić członków tej grupy jako przestępców posługujących się komputerem jako środkiem popełnienia przestępstwa. Na podstawie art. 267 § 1 KK można stwierdzić, że pierwsza grupa skupia się w swoim działaniu na „przełamaniu elektronicznych zabezpieczeń” i na tym poprzestaje, natomiast członkowie drugiej grupy nacisk kładą na „uzyskaniu informacji dla nich nie przeznaczonej”, przy czym jednocześnie starają się najczęściej omijać zabezpieczenia. Widać więc, że „hakerzy” spełniają jedną przesłankę czynu penalizowanego w art. 267 § 1 KK, w przeciwieństwie do drugiej grupy, której członkowie spełniają drugą przesłankę, co jednak często nie skutkuje możliwością postawienia zarzutu popełnienia przestępstwa z art. 267 § 1. W związku z powyższym myślę, że bardziej uzasadniony byłby podział na „hackerów” i „przestępców komputerowych” niż na „dobrych” i „złych” „hackerów” (taki podział w literaturze już nastąpił, mianowicie na „hackerów” i „crackerów”, co jednak doprowadziło do

dalszych nieporozumień, także wśród członków podziemia[135]).„Jargon Dictionary" posługuje się – poza wspomnianym rozróżnieniem „hacker" i „cracker" – podziałem na „samurajów" i „dark-side hackerów".

Filozofia działalności „hackerów" zasadza się na głoszeniu „twórczej siły wolnego przepływu informacji", w związku z czym głosi się powinność „hackera" do udostępniania swojej wiedzy i umożliwianiu gromadzenia tej wiedzy przez innych. Poszczególne kodeksy etyki „hackerskiej" różniące się między sobą poszczególnymi zapisami w tym punkcie są jednobrzmiące : „hacker dzieli się swoją wiedzą". Paradoksalny może się wydawać fakt, że ludzie działający na granicy prawa lub poza nią, postępują zgodnie z jedną z zasad etyki, postulującą „gromadzenie wiedzy we wszelkich możliwych dziedzinach". Nieco dalej posunięte twierdzenie, akceptowane tylko przez część środowiska, zakłada ogólnodostępność wszelkiej informacji – przy takiej wykładni uzyskiwanie nieuprawnionego dostępu do wszelkich serwerów jest postępowaniem etycznie dozwolonym[136].

W literaturze przedmiotu, poza podziałem na „dobrych" i „złych" „hackerów", dość często spotyka się również podział, którego wyznacznikiem są motywy działania sprawcy i jego kroki podjęte po uzyskaniu dostępu do systemu. Wyróżnia się w związku z tym następujące grupy (klasyfikacja zaproponowana przez CERT) :

1. „hackerzy" – dokonują naruszenia zabezpieczeń dla samego faktu i potwierdzenia swoich umiejętności;
2. „szpiedzy" – dokonują ataków w celu uzyskania informacji, które można wykorzystać w celach politycznych;
3. „terroryści" – próbujący swoimi atakami wywołać stan zagrożenia w celu osiągnięcia korzyści politycznych;
4. „szpiedzy przemysłowi" – często pracownicy firm, atakujący konkurencję w celu osiągnięcia korzyści finansowych;
5. „zawodowi przestępcy" – dokonujący ataków w celu osiągnięcia osobistych korzyści finansowych;
6. „wandale" – uzyskujący nielegalny dostęp do systemów w celu dokonania w nich zniszczeń;

---

[135] swojego czasu toczyła się dyskusja pomiędzy środowiskiem „crackerów" a Michałem „Lcamtufem" Zalewskim, która rozgorzała po opublikowaniu, jak się później wyjaśniło nieautoryzowanego przez tego ostatniego, artykułu w „Machinie"; w toku tej dyskusji „Lcamtuf", przytaczając „Jargon Dictionary" wskazał na podwójną definicję pojęcia „cracker", oznaczającą jednocześnie „złego hackera", włamującego się do systemów w celu dokonania w nim szkód, jak i osobę zajmującą się „reverse engineeringiem", czyli analizowaniem kodu programów w celu przełamania zabezpieczeń; por. http://hacking.pl/articles.php?id=56;

[136] http://www.ws-webstyle.com/cms.php/en/netopedia/bezpieczestwo_hacking/haker;

7. „turyści” – uzyskujący nielegalny dostęp w celu doznania uczucia strachu z tym związanego;

Chciałbym zaznaczyć, iż nie było zamiarem autora gloryfikowanie żadnej z wymienionych grup „hackerów”, co jednocześnie nie wyklucza sympatyzowania ze środowiskiem. Faktem jest jednak, że, niezależnie od bycia „dobrym” czy „złym”, cechuje ich niezwykle silna chęć poszerzania wiedzy i wykorzystywania tej wiedzy w praktyce.

Reasumując – w znaczeniu ogólnym „hackerem” jest każdy entuzjasta technik teleinformatycznych, natomiast w ujęciu autorów komentarzy Kodeksu Karnego będzie nim po użytkownik wykorzystujący swoje umiejętności w celach kolidujących z obowiązującym porządkiem prawnym.

3.2 Zjawisko „hackingu” w odbiorze społecznym.

Przez masowego odbiorcę „hacker” jest odbierany jako zagrożenie – tym większe, ze niewidzialne, a przede wszystkim niezrozumiałe. Ludzie, którzy oceniają „hackerów” jako przestępców, cyberterrorystów na ogół nie wiedzą, czym „hacker” się zajmuje, co robi, nie mówiąc już o tym, dlaczego to robi. Zawsze największy lęk to lęk przed nieznanym – a ponieważ „hackerów” nie można kontrolować, ponieważ stanowią oni podziemie, w świadomości społecznej będą źródłem zagrożeń, choćby dlatego, że, w ogólnospołecznej ocenie, nie są „normalni” jak 90 % populacji. Opinia publiczna negatywnie odbiera to środowisko za jego inność oraz, a może przede wszystkim, za wiedzę, „hackerzy” bowiem to ludzie nie tylko wybitnie uzdolnieni, ale także dysponujący olbrzymią wiedzą informatyczną (i nie tylko – wystarczy spojrzeć na działalność *social engineering,* chociaż metoda ta bardziej pasuje do grupy przestępców) i potrafiący ją wykorzystać w praktyce.

Na tym lęku społecznym, na lęku przed lepszymi, ukrytymi i nieznanymi, bazują środki masowego przekazu, będące dla większości ludzi głównym źródłem wiedzy. Informacje, jakimi karmią odbiorcę nie tylko znamionują duże luki w znajomości tematu lecz wręcz jego nieznajomość[137]. Okres, nazwany przez R. Hollingera[138] okresem demonizacji hackerów przypadł na przełom lat 80-tych i 90-tych ubiegłego stulecia i miał związek z nagłaśnianiem przez media pierwszych spektakularnych wyczynów „komputerowych

[137] *przykładem może być artykuł, jaki ukazał się w Gazecie Wyborczej z dnia 24 sierpnia 2004 „Łapią hakerów z warez city”, którego autorzy, opisując strukturę rozbitej przez policjantów z Gorzowa grupy przestępczej wszystkich jej członków określili mianem hakerów (zachowuję pisownię pojęcia użytą w treści artykułu), mimo dokładnego opisu czynów, jakich dopuszczali się członkowie poszczególnych szczebli hierarchii np. znajdowanie w Internecie filmów, muzyki i oprogramowania, czego za technike „hackerską” uznać nie można; por. : Gazeta Wyborcza, nr 198. 4712 z dnia 24 sierpnia 2004 r. „Łapią hakerów z Warez City”;*

[138] *szerzej o rozwoju postrzegania technologii komputerowej jako źródła zagrożeń w rozdziale I*

włamywaczy”[139], a także z produkcjami filmowymi (film „Gry wojenne”, mimo, iż niosący przesłania antywojenne, wskazywał również zagrożenie ze strony użytkowników sieci komputerowych)[140] – efektem było spopularyzowanie pojęcia, przy jednoczesnym nadaniu mu pejoratywnego znaczenia[141]. Ponadto nie sposób oprzeć się wrażeniu, iż określenie „hacker”, w odbiorze masowym przylgnęło do jakiegokolwiek przestępcy posługującego się komputerem.

Hackerzy są postrzegani przez społeczeństwo jako zagrożenie – i niestety, nie zawsze słusznie[142], a ten stan rzeczy ma kilka przyczyn, spośród których nie sposób wyłonić głównej. Przede wszystkim, o czym pisałem wcześniej, hackerzy są ucieleśnieniem ludzkiego lęku przed nieznanym – są elementem rzeczywistości, którego na pierwszy rzut oka nie można zakwalifikować do grupy zawodowej, społecznej, wyznaniowej itp. (wyjątkiem może być tu zjawisko „hacktyvism’u”, o którym kilka słów w dalszej części pracyj), albowiem hackerem się jest pomimo przynależności do jakiejkolwiek grupy zawodowej, a samo bycie hackerem nie stanowi o przynależności do żadnej z takich grup – hacker z założenia jest indywidualistą, mimo iż funkcjonuje bardzo wiele grup „hackerów”[143] (ostatnio firmy związane z bezpieczeństwem systemów zgłaszają fakt powstawania „mafii hackerskich”, w odniesieniu do przestępców),. Drugą kwestią, o czym również wspomniałem wcześniej, jest ludzki lęk (bądź niechęć lub nienawiść) przed lepszymi – a hacker niewątpliwie jest bardziej inteligentny i posiada większą wiedzę od zdecydowanej większości populacji ludzkiej. Zwykłemu użytkownikowi komputera wystarcza, że ten sprzęt działa – hacker chce wiedzieć dlaczego działa, w jaki sposób i – co chyba najważniejsze – jak można zmienić to działanie.

Pojęcie „hackingu” nie zostało zdefiniowane w polskim prawie karnym. Jedynie na podstawie analizy działań przestępczych i prawnokarnej kwalifikacji czynów można uznać (mając na względzie nieunikniony brak ostrości), że materię „hackingu” reguluje art. 267 § 1 KK stanowiący o „nieuprawnionym uzyskaniu, w wyniku przełamania zabezpieczeń, informacji dla sprawcy nie przeznaczonej”. W ten sposób „hacking” rozumiany jest na gruncie polskiego prawa karnego; pierwsze, co rzuca się w oczy, to pewna dysproporcja pomiędzy tym, co pisałem o *stricte* „hackingu” (czyli o nacisku położonym na przełamywaniu zabezpieczeń), a kwalifikacją polskiego Kodeksu Karnego, który nacisk kładzie na zaznajomienie się z informacją. Przepis polskiej ustawy karnej jest bowiem niczym

---

[139] szerzej o rozwoju przestępczości komputerowej w rozdziale I
[140] obecnie można przytoczyć kilka przykładów produkcji filmowych, mających niewiele wspólnego z rzeczywistością, będących natomiast bardzo widowiskowymi obrazami możliwości hackerów – „Hackers”, „Swordfish”, ... ; trudno się więc dziwić, iż w zwykłym użytkowniku komputera i Internetu taki pokaz budzi lęk i żądanie ze strony władz podejmowania działań wymierzonych w „komputerowych przestępców”; do tematyki filmowej powrócę jeszcze dalej;
[141] A. Adamski – Prawo karne .., op. cit., str. 3;
[142] zwłaszcza, gdy dotyczy to „komputerowych entuzjastów”;
[143] przykładem może być rodzima grupa „LSD” („Last Stage of Delirium”)

innym jak zmodyfikowaną wersją przepisu o ochronie tajemnicy korespondencji, pomimo, że istnieją dość poważne różnice pomiędzy dobrami prawnymi podlegającymi ochronie. Samo uznanie „hackingu" za dążenie sprawcy do „uzyskania informacji" rozwiązaniem chybionym, zwłaszcza w aspekcie motywów, jakimi kieruje się część tego środowiska.

W regulacjach prawnych innych krajów, bądź też międzynarodowych, przez pojęcie „hackingu" rozumie się ogólnie uzyskanie nieuprawnionego dostępu do systemu komputerowego (systemu służącego do przetwarzania danych, informatycznego, teleinformatycznego) – różnice tkwią w istnieniu (bądź nie) dodatkowych przesłanek, natomiast sama koncepcja jest stała – karalne jest „wejście" do takiego systemu bez autoryzacji.

W publikacjach prawnych, z założenia skupiających uwagę na kwalifikacji czynu , nie dokonuje się rozróżnienia pomiędzy poszczególnymi grupami „hackerów"[144] – jedynym kryterium jest fakt spełniania przesłanek czynu zabronionego, dlatego też jej przedmiotem są „przestępcy komputerowi".

Literatura informatyczna prezentuje nieco inne spojrzenie na zagadnienie, a dokładnie od innej strony. „Hacking" jest tam postrzegany pod kątem technik programistycznych lub budowy (struktury) „łamanych" systemów i programów. Ludzie zawodowo zajmujący się informatyką, o ile rzecz ich nie dotyczy bezpośrednio (np. kiedy są administratorami „zhackowanego" systemu) patrzą na problem niezmiernie obiektywnie, wręcz beznamiętnie. Abstrahując od faktu, że informatyk pasjonujący się tą dziedziną wiedzy również (wg szerokiej definicji) jest „hackerem", w literaturze zawodowej spotykamy się z podejściem suchego przedstawienia faktów i metod, bez zabarwienia emocjonalnego. Podstawą tej literatury jest bowiem zawodowa ciekawość i chęć poznania systemów i programów od strony ich słabości, a także sposobu myślenia tych, którzy te słabości znaleźli i wykorzystali. Na tym polu działania „hackerów" i administratorów systemów lub bezpieczeństwa danych są takie same – wykryć luki, słabości, dziury i błędy, różnica pojawia się w chwili znalezienia i dalszego wykorzystywania. Rzecz znamienna – po odkryciu włamania do swojego systemu administrator pomyśli o zawiadomieniu Policji czy zespołu CERT w drugiej kolejności – pierwsze co zrobi, to pomyśli „jak on to zrobił ?" i często bez negatywnego zabarwienia, a czasem wręcz z podziwem. W przypadku bezpieczeństwa teleinformatycznego, w warunkach ciągłego rozwoju *volens nolens* gros doświadczenia nabywa się drogą empirii – nieustający pojedynek administrator – „hacker" służy jednocześnie podnoszeniu kwalifikacji i nabywaniu wiedzy przez jednych i drugich i to w obu dziedzi-

[144] *W. Wiewiórowski – Profesjonalny haker. Paradoks odpowiedzialności karnej za czyny związane z ochroną danych i systemów komputerowych, materiały z konferencji „Internetki 2005", Lublin 4 marca 2005 r.;*

nach. „Hacker" i administrator posiadają tak naprawdę tą samą wiedzę odnośnie sposobów zabezpieczeń – różni ich tylko sposób jej wykorzystywania[145]

Niebagatelną, a wręcz można powiedzieć że wiodącą, rolę w kreowaniu odbioru podziemia informatycznego przez społeczeństwo odgrywa film. Ponieważ komputery są stałym elementem życia codziennego, w filmie również podniesiono ich rolę we współczesnym świecie – „hackerzy" pojawiają się najczęściej w przekazach o charakterze sensacyjnym. Ciekawym jest fakt, że pomimo przedstawiania w większości przypadków obrazów, w których występują jednocześnie „dobrzy" i „źli" „hackerzy", ich umiejętności (ekranowe oczywiście) budzą lęk, niezależnie od zasad, jakimi się kierują. Ciekawym wyjątkiem jest „AntiTrust" – obraz o środowisku nie tyle stricte „hackerów" co zapalonych programistów („hackerów" jako entuzjastów) i szczerze mówiąc, będący najbliższy realistycznego przekazu warunków panujących w programistycznym środowisku i na rynku pracy oraz możliwości, jakimi dysponuje tam jednostka. Biorąc pod uwagę, że okazyjnie zahacza też o problematykę oprogramowania „open source" na tle innych produkcji film ten wydaje się być niemal wybitnym. Wszystkie przekazy charakteryzują się wspólnym elementem, a mianowicie rażącym przejaskrawieniem możliwości (nie umiejętności, choć czasem również), jakimi dysponuje „hacker" – do zbiorowej świadomości trafia przekaz o „wszechmogących hackerach", co w pewnych sytuacjach powoduje społeczny lęk i żądanie podjęcia przez władze niezbędnych kroków. Dziwne natomiast wydaje się, że efektu takiego nie przynoszą filmy o stosowaniu przez władze technologicznej inwigilacji obywateli i manipulacji faktami[146] – problematyka ta nie wzbudza szerszego zainteresowania. Jeszcze kilka lat temu człowiek, który mówił o istnieniu systemu „Echelon" był powszechnie uznawany za paranoika, a i w chwili obecnej również się to zdarza[147].

3.3 Metody przestępczego działania;

W zależności od celu, jaki sprawca postawił sobie do osiągnięcia, często posługuje się on różnymi technikami i narzędziami, dokonując jednego ataku. Postaram się przedstawić wybrane techniki, jednocześnie dokonując ich krótkiej kwalifikacji prawnej na tle przepisów rozdziału XXXIII Kodeksu Karnego. Pominąłem w tym miejscu kilka sposobów, jakimi sprawcy często się posługują, ze względu na omówienie ich w rozdziale poświęconym art. 267 § 1. Ponadto, ze względu na ograniczenia wynikające z objętości pracy oraz zakresu stosowanych technik, omówienie wszystkich, choćby jak najbardziej po-

[145] o czym niestety zapomniał ustawodawca redagując art. 269b KK, wprowadzony „cybernowelizacją", który kryminalizuje „wytwarzanie i udostępnianie" narzędzi „hackerskich"; szerzej o tej problematyce w rozdziale poświęconym przestępczości komputerowej w polskim Kodeksie Karnym;
[146] np. „Enemy of the State";
[147] Systemowi ogólnoświatowej inwigilacji satelitarnej "Echelon" poświęcę więcej miejsca na końcu pracy;

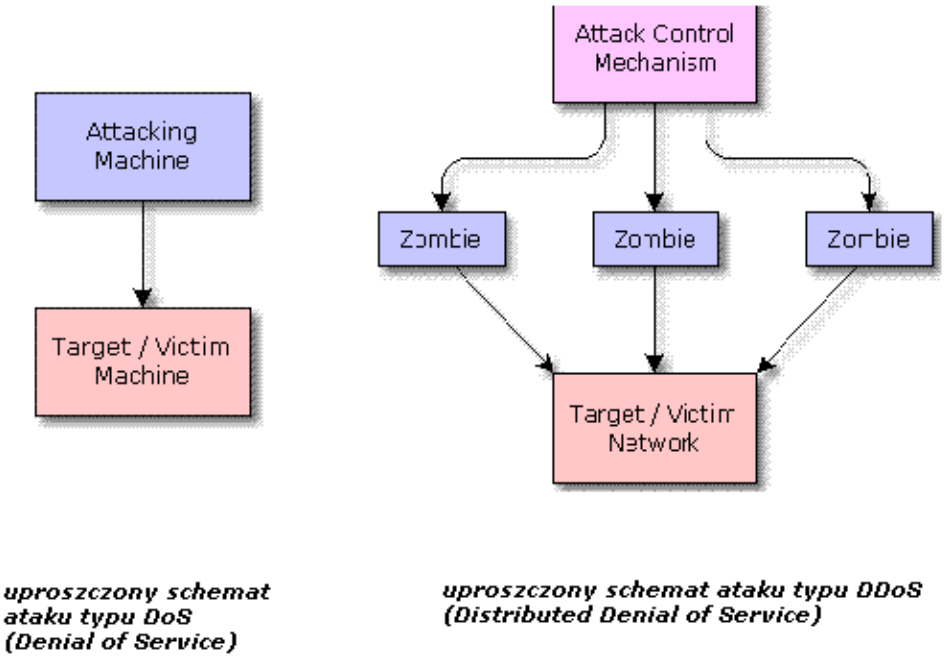
bieżnie, nie jest możliwe. Praktycznie skupię się na ataku typu DoS/DDoS, ze względu na szeroki wachlarz metod, jakimi może posłużyć się sprawca.

Chciałbym nadmienić, iż przełamywanie zabezpieczeń systemów i poprzestawanie na tym jest domeną „czystego hackerstwa", stanowiącego obecnie znikomy procent sprawców działających w Sieci. Regułą stało się włamywanie do systemu w celu dalszego wykorzystania. Przykładowa działalność przestępcy może polegać na uzyskaniu dostępu do obcego systemu np. za pomocą wysłania ofierze w spreparowanej odpowiednio poczcie elektronicznej „konia trojańskiego", za pomocą którego instaluje „backdoor", przez który wchodzi do atakowanego systemu, a następnie instaluje oprogramowanie do przeprowadzenia ataku typu DoS/DDoS. Powtarzając powyższą operację dowolną ilość razy dysponuje potencjałem pewnej liczby komputerów pozostających pod jego kontrolą (tzw. „zombie") i uruchamiając na nich zainstalowane oprogramowanie przeprowadza atak DDoS na wybrany przez siebie serwer. Powyższy schemat, niezwykle uproszczony, jako że można go wzbogacić o jeszcze kilka elementów, wskazuje na pewną charakterystyczną cechę współczesnych ataków sieciowych – jednoczesną złożoność i prostotę. Rzadko kiedy spotyka się hackera działającego za pomocą jednej techniki – także tutaj panuje pragmatyzm, a w przypadku długiej drogi, jaka dzieli sprawcę od celu, na każdym etapie, mającym swoją specyfikę, stosuje inne metody (każda metoda działania i każde narzędzie jest tylko fragmentem pewnej całości, jaką jest działanie sprawcy). Prawdopodobnie tak właśnie wyglądał schemat ataku na portale Yahoo, eBay czy Amazon.com, a także podstawową strukturę serwerów domenowych. Należy pamiętać, iż atak typu DDoS jest rodzajem, a nie sposobem działania – uruchomienie ataku typu DDoS wymaga posłużenia się kilkoma technikami. O niektórych wspomnę poniżej, na początku chciałbym przedstawić istotę ataku tego typu, a to ze względu na jego względną prostotę i spektakularne efekty, jakie wywołuje w przypadku powodzenia.

Istota ataku typu Distributed Denial of Service[148] zasadza się na „zalaniu" komputera – ofiary taką ilością pakietów – żądań, na które nie będzie w stanie odpowiedzieć, co zaowocuje zablokowaniem tego systemu. Atak DDoS jest formą rozwojową ataku typu DoS, od którego różni się ilością przejętych wcześniej i wykorzystanych komputerów „zombie", a co a tym idzie, mniejszym prawdopodobieństwem wykrycia sprawcy. Aby przeprowadzić atak typu DoS sprawca musiał uzyskać dostęp do niezabezpieczonego (lub niewystarczająco zabezpieczonego) systemu i zainstalować na nim odpowiednie oprogramowanie[149], które, na sygnał sprawcy, bądź na skutek wcześniejszego zaprogramowania (na określony czas – „bomba czasowa", lub na wystąpienie określonego zda-

[148] *Rozproszony atak DoS, rozproszony atak typu 'blokada usług';*
[149] *Kilka wybranych metod uzyskania takiego dostępu omówię poniżej;*

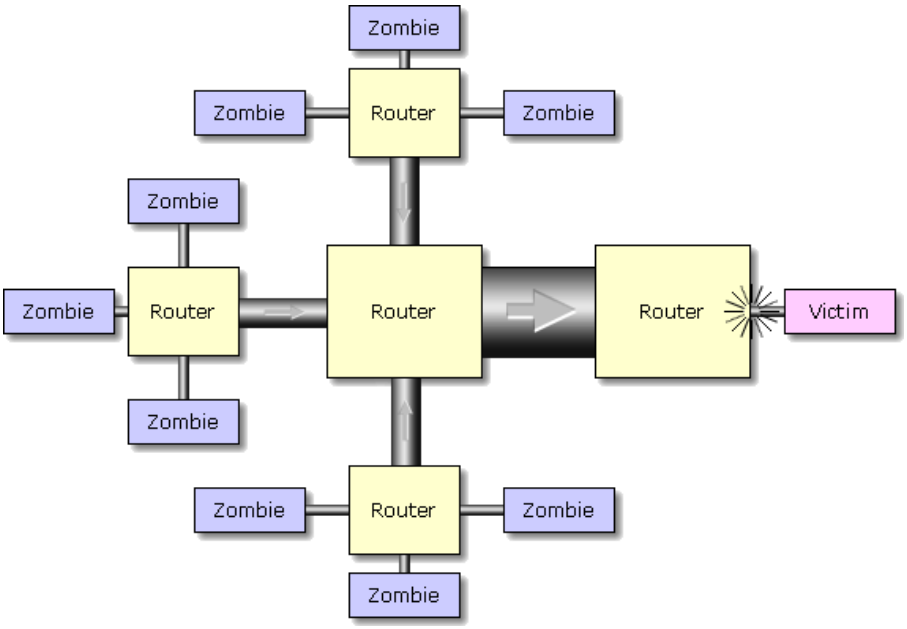
rzenia systemowego – „bomba logiczna"), w danym momencie wysyła do atakowanego, również wcześniej podanego, komputera - celu olbrzymią liczbę pakietów, na które ten nie jest w stanie odpowiedzieć, co z kolei powoduje jego dysfunkcję. Techniki przeprowadzenia ataku tego typu również różnią się między sobą, chociażby metodą przejęcia kontroli nad komputerem faktycznie przeprowadzającym atak („zombie"), jak i samą techniką blokowania usług (np. atak typu SYNFlood). Atak typu DDoS natomiast jest przeprowadzany nie z jednego komputera „zombie" lecz niekiedy z tysięcy, co daje realną możliwość zablokowania olbrzymich serwerów portali internetowych, lub, jak to miało miejsce w październiku 2002 r., wręcz serwerów domenowych klasy „root". Uproszczone schematy obu ataków przedstawia rysunek poniżej.



Rys. 8 – atak typu DoS (Denial of Service) i DDoS (Distributed Denial of Service); *(źródło : http://grc.com/dos/drdos.htm)*

Metoda ataku typu "odmowa usług" nieustannie ewoluuje – ostatnią opisaną nowością jest odmiana „*Distributed Reflection Denial of Service*", określana mianem nowej generacji ataku typu DDoS. Nie wchodząc w szczegóły techniczne, charakteryzuje się ona przejęciem kontroli nie nad poszczególnymi maszynami w danej sieci, lecz nad routerami, sterującymi komunikacją w tych sieciach i przeprowadzeniem ataku za pomocą wszystkich maszyn znajdujących się w danej podsieci[150].

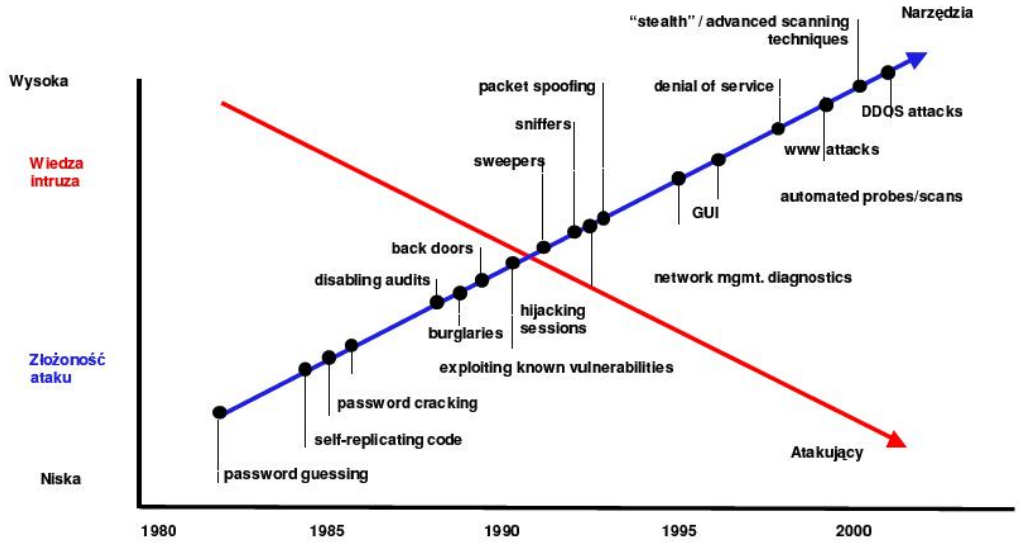
[150] *Steve Gibson – Distributed Reflection Denial of Service. Description and analysis of a potent, increasingly prevalent, and worrisome Internet attack; http://grc.com/dos/drdos.htm;*



Rys. 9 – schemat ataku typu DRDoS (Distributed Reflection Denial of Service); *(źródło : http://grc.com/dos/drdos.htm)*

Zanim zacznę omawiać wybrane techniki, jakimi zazwyczaj posługują się sprawcy wyżej wymienionych typów ataków, chciałbym nadmienić, iż od kilku lat obserwuje się zjawisko swoistej „automatyzacji" dokonywania ataków na systemy informatyczne – incydenty, które jeszcze kilka lat temu stanowiły domenę komputerowych „noblistów" w dniu dzisiejszym stały się udziałem sprawców posiadających wręcz mierną wiedzę informatyczną. Taki stan rzeczy to przede wszystkim konsekwencja powszechnej dostępności programów służących do przeprowadzania ataków, a działających w sposób niemalże automatyczny – działanie sprawcy ogranicza się do podania adresu sieciowego komputera, który ma zostać zaatakowany. Sprawcy takich incydentów, tzw. „script kiddies" korzystają z gotowych, napisanych przez innych, skryptów, a ich działanie ogranicza się do uruchomienia takiego programu. Taki stan rzeczy jest argumentem przemawiającym za koniecznością kryminalizacji „niewłaściwego użycia urządzeń", o którym mówi art. 6 Konwencji, czyli (w skrócie) wytwarzania i dystrybucji programów służących m. in. do ataków tego typu lub tworzenia wirusów czy robaków (słynne robaki takie jak „Anna Kournikova" czy „I love you" zostały „wyprodukowane" – bo nie napisane – przez takie właśnie oprogramowanie - "[K]Alamar's Vbs Worms Creator"[151]) Wzajemne relacje pomiędzy złożonością ataku a wiedzą intruza ilustruje poniższy wykres.

[151] *P. Waglowski – Nadchodzi czas wielkiej kwarantanny; źródło : http://www.vagla.pl/felietony/felieton_062.htm*



rys. 10 – relacje pomiędzy złożonością ataku a wiedzą intruza; *(źródło : CERT Polska)*

Ażeby dokonać ataku typu DDoS trzeba uzyskać dostęp (i przejąć kontrolę) nad komputerem (komputerami), które fizycznie będą przeprowadzały ten atak. Ponieważ tego typu atak opiera się na większej ilości komputerów „zombie", faza ta przeprowadzana jest zazwyczaj automatycznie, przykładowo za pośrednictwem robaków. Poniżej przedstawię pokrótce kilka dość znanych technik (uwzględnię jedynie tzw. „działania z zewnątrz") uzyskania dostępu do systemu[152].

„Password guessing" – czyli ataki korzystające z haseł, polegające na włamywaniu się do systemu poprzez podanie identyfikatora („loginu") i hasła. W tym celu intruz odszukuje (w systemach Unix'owych) pliki „passwd"/"shadowpsswd" i następnie próbuje rozszyfrować z nich, za pomocą odpowiednich programów (takich jak np. „John the Ripper") hasła konkretnych użytkowników. Nieodzownym elementem takiego działania jest posiadanie przez włamującego się pliku słownikowego, z którego wyrazy są porównywane z zaszyfrowanymi hasłami. Jak łatwo zauważyć, uzyskane za pomocą tej metody hasło jest „informacją, do uzyskania której sprawca nie był upoważniony" (o ile zapozna się z jego treścią) i „uzyskaną w wyniku przełamania zabezpieczeń" (deszyfracja), co stanowi przesłankę postawienia zarzutu z art. 267 § 1 KK, trzeba jednak szczerze przyznać, iż jest to wyłącznie teoria.

[152] *pominę tu techniki, jakie zostaną omówione w rozdziale poświęconym „hackingowi" w ujęciu Kodeksu Karnego;*

„Sniffing" („węszenie") posiada dwie odmiany – „bierne węszenie", polegające na „nasłuchiwaniu" ruchu pakietów w sieci i jego analizie i „aktywne węszenie", będące *de facto* przechwyceniem w protokole TCP. Aby móc zacząć nasłuchiwanie, sprawca musi zalogować się do sieci, korzystając ze zdobytego wcześniej identyfikatora i hasła.(np. przy pomocy sposobów socjotechnicznych), po czym, przy pomocy specjalnego oprogramowania („*sniffer*") rozpoczyna podglądać / kopiować ruch pakietów, dzięki czemu zdobywa coraz więcej informacji o atakowanej sieci. Technika powyższa stanowi najczęściej wstęp do „aktywnego węszenia" i stanowi formę „inwigilacji przy pomocy środków technicznych". W przypadku uzyskania informacji (np. w postaci haseł użytkowników) sprawcy „sniffingu" można postawić zarzut z art. 267 § 2 KK, o ile uzna się komputer wyposażony w „*sniffer*" za urządzenie specjalne, o którym mówi przepis, co jest przedmiotem sporów w doktrynie.

Atak typu DoS/DDoS należy kwalifikować jako zamach na dostępność i integralność informacji oraz systemów teleinformatycznych, poprzez spowodowanie dysfunkcji tych ostatnich. Zastosowanie, w przypadku działania zakończonego powodzeniem (czyli odmówienia przez atakowany system usług – zawieszenia systemu), mogą mieć następujące przepisy Kodeksu Karnego :

- art. 268 § 2 – jeśli działanie sprawcy zaowocuje udaremnieniem lub utrudnieniem zapoznania się z istotną informacją,
- art. 268a § 1 jako przepis chroniący dostępność danych informatycznych i integralność systemów służących do przetwarzania takich danych,
- art. 269 w przypadku zakłócenia lub uniemożliwienia przetwarzania, gromadzenia i przekazywania danych (o szczególnym znaczeniu dla wymienionym w treści przepisu podmiotów),
- art. 269a chroniący niezakłócone funkcjonowanie systemu komputerowego lub sieci teleinformatycznej;
- w przypadku pozyskania „narzędzia", służącego do popełnienia przestępstw z wyżej wymienionych artykułów, sprawca może ponieść odpowiedzialność karną z art. 269b

Ogólnie rzecz ujmując, w związku ze złożonością ataku omawianego typu, sprawca podlega odpowiedzialności karnej na każdym etapie przygotowania zamachu, począwszy od pozyskania odpowiednich „narzędzi", poprzez uzyskanie nieuprawnionego dostępu do wielu systemów informatycznych (najczęściej jednak odbywa się to automatycznie poprzez wykorzystanie luk w oprogramowaniu, co powoduje niemożność posta-

wienia zarzutu) i instalację na nich specjalnego oprogramowania (taka ingerencja w system stanowi naruszenie integralności zapisu danych lub integralności systemu informatycznego), na wystąpieniu skutku w postaci dysfunkcji atakowanego systemu kończąc (co jest kwalifikowane jako zamach na niezakłócone funkcjonowanie systemu informatycznego lub sieci teleinformatycznej).

4. Rozdział IV – Inicjatywy i standardy OECD i Rady Europy w zakresie ochrony informacji (przestępczości komputerowej).

Po tym, jak w latach 60-tych ubiegłego stulecia pojawiły się pierwsze sygnały dotyczące przestępczości związanej z przesyłaniem danych (głównie szpiegostwo komputerowe), zaczęto szukać rozwiązań pozwalających ścigać sprawców takich zachowań. W krajach Europy Zachodniej zainteresowanie społecznymi skutkami informatyzacji ze strony sfer rządowych datuje się na lata 70-te. Trzeba wspomnieć, że w przeciwieństwie do Stanów Zjednoczonych A.P., gdzie przepisy karne dotyczące tej dziedziny tworzono w sposób niemal spontaniczny, w Europie proces kryminalizacji nadużyć komputerowych miał charakter planowanego, skoordynowanego działania, co przejawiało się w tworzeniu standardów normatywnych, tworzonych przez specjalnie powołane komisje ekspertów[153]. Taki stan rzeczy ma swoje uzasadnienie historyczne – Stany Zjednoczone były kolebką Internetu i tam też miały miejsce pierwsze incydenty związane z przetwarzaniem zdigitalizowanych danych, kraje europejskie zaś, w miarę upowszechniania się technologii informatycznych, mogły etapami dostosowywać regulacje prawne do zmieniających się realiów. W chwili obecnej, na gruncie europejskim, ukoronowaniem wysiłków legislacyjnych w tym kierunku jest Konwencja Rady Europy o Cyberprzestępczości, niejako następczyni Zalecenia Nr (89) 9 i Zalecenia Nr (95) 13[154].

4.1 Przestępstwa związane z komputerem : analiza polityki legislacyjnej — Computer-Related Crime : Analysis of legal policy, OECD, Paris 1986;

Jako jeden z pierwszych z inicjatywą badań nad skutkami komputeryzacji i informatyzacji w życiu społecznym wystąpił rząd Szwecji – w maju 1977 roku powołano specjalną komisję (SARK), której raport opublikowano w 1979 r. zawierał on analizę zagrożeń, jakie niesie ze sobą brak kontroli nad rozwojem informatyzacji i jednocześnie wskazywał środki zapobiegawcze, z których można wyodrębnić dwa główne kierunki : uświadamianie o istnieniu tychże zagrożeń i ich rozmiarach oraz tworzenie ustawodawstwa, na którym można by było oprzeć przeciwdziałanie im[155]. Jak widać, oba te postulaty

[153] *A. Adamski – Prawo karne ... op. cit., str. 5*
[154] *Zaleceniu Nr (95) 13 poświęcę dalej nieco więcej miejsca z uwagi na pierwszeństwo w poruszeniu kwestii karnoprocesowych;*
[155] *ibidem*

po ponad ćwierćwieczu są nadal aktualne (z tym, że ustawodawstwa nie trzeba tworzyć od podstaw, a dostosowywać do zmieniających się wciąż warunków).

W 1981 roku inicjatywę rządu Szwecji podjęły OECD i rząd Hiszpanii, organizując wspólne seminarium, poświęcone zagrożeniom, jakie niesie ze sobą ekspansja informatyki. Badania nad możliwością wypracowania międzynarodowych, prawnokarnych norm dotyczących przeciwdziałaniu przestępstwom popełnianym z wykorzystaniem komputera OECD podjęła w 1983 roku i ich efektem był, opublikowany w 1985 roku, raport „Computer-Related Crime. Analysis of legal policy".

Zawierał on, m.in. przegląd istniejącego prawodawstwa kilku krajów członkowskich organizacji i postulował potrzebę zmian ustawodawczych. Jednak najważniejszym elementem tego raportu była lista nadużyć (wraz z postulatem penalizacji), na którą złożyło się pięć kategorii czynów :

1. oszustwo komputerowe,
2. fałszerstwo komputerowe,
3. sabotaż komputerowy,
4. nielegalne kopiowanie programów komputerowych,
5. uzyskanie nielegalnego dostępu do systemu komputerowego

W raporcie tym ponadto sformułowano roboczą definicję „nadużycia komputerowego", określając je jako każde nieetyczne[156] i nieuprawnione zachowanie, związane z automatycznym przetwarzaniem i przesyłaniem danych - jednocześnie członkowie komisji uznali tą definicję za mało praktyczną ze względu na jej ogólnikowość.

4.2 Zalecenie Nr (89) 9 o przestępczości komputerowej i końcowe sprawozdanie Komitetu Problemów Przestępczości Rady Europy – Council of Europe : Computer-Related Crime, Recommendation No. R(89)9 on computer-related crime and final report of the European Committee on Crime Problems;

Nawiązując do działań podjętych przez OECD, Rada Europy rozpoczęła własny program badań, powołując w 1985 15-stoosobowy Komitet Ekspertów. Do jego zadań należało wypracowanie wskazówek ułatwiających krajom członkowskim procesy legisla-

[156] *kwestia istnienia bądź nie tzw. „netykiety", czyli zasad, jakimi powinien kierować się, lub których powinien przestrzegać każdy użytkownik sieci jest wciąż nierozstrzygnięta; z jednej strony zbiór takich zasad byłby niewątpliwie bardzo przydatny, z drugiej stworzenie takich uniwersalnych zasad wydaje się być zgoła niemożliwe;*

cyjne, poprzez wskazanie rodzajów działań przestępczych, jakie powinny zostać zabronione w ustawodawstwie pod groźbą kary.

Komitet w 1989 roku przedstawił raport i projekt zalecenia, który został przyjęty przez Komitet Ministrów Rady Europy w dniu 13 września 1989 roku jako Zalecenie Nr R(89)9[157]. Dokument ten wzywał kraje członkowskie do uwzględnienia, w trakcie prowadzonych prac legislacyjnych, wskazówek zawartych w raporcie oraz do przedłożenia w 1993 r. Sekretarzowi Generalnemu Rady Europy informacji dotyczących zmian ustawodawczych, praktyki sądowej i doświadczeń we współpracy międzynarodowej na polu przestępczości komputerowej[158].

Podstawowym efektem pracy Komitetu Ekspertów było wypracowanie listy przestępstw komputerowych, która w stosunku do listy przedstawionej w raporcie OECD, została znacznie rozszerzona. Ze względu na brak jednomyślności w Komitecie, dotyczącej kryminalizacji wszystkich form zachowań, działania przestępcze ujęto w ramach dwu list : „minimalnej" i „fakultatywnej".

Lista „minimalna" obejmowała czyny, które, wg Komitetu Ekspertów, powinny zostać kryminalizowane we wszystkich krajach członkowskich, ze względu na ich transgraniczny charakter i znaczną szkodliwość – miało to przede wszystkim zapewnić zharmonizowanie ustawodawstwa karnego celem zapewnienia współpracy w zakresie ścigania przestępstw komputerowych. Lista „minimalna" objęła osiem kategorii czynów przestępnych :

1. oszustwo związane z wykorzystaniem komputera,
2. fałszerstwo komputerowe,
3. uszkodzenie danych lub programów komputerowych,
4. sabotaż komputerowy,
5. uzyskanie nieuprawnionego dostępu do systemu komputerowego,
6. podsłuch komputerowy,
7. bezprawne kopiowanie, rozpowszechnianie lub publikowanie programów komputerowych prawnie chronionych,
8. bezprawne kopiowanie topografii półprzewodników.

Lista „fakultatywna" obejmowała typy nadużyć komputerowych, których kryminalizacja, zdaniem Komitetu Ekspertów, ze względu na relatywnie mniejszą szkodliwość

[157] *Council of Europe, Computer-Related Crime : Recommendation No. R(89)9 on computer-related crime and final report of the European Committee of Crime problems, Strasbourg 1989*
[158] *A. Adamski – Prawo karne ... , op. cit., str. 6*

ma też mniejsze znaczenie niż w przypadku listy „minimalnej" i w związku z tym nie wymaga podejmowania skoordynowanych działań międzynarodowych i ich ewentualna penalizacja może pozostać w gestii swobodnej decyzji poszczególnych państw. Lista „fakultatywna" obejmowała cztery typy zachowań :

1. modyfikację danych lub programów komputerowych,
2. szpiegostwo komputerowe,
3. używanie komputera bez zezwolenia,
4. używanie prawnie chronionego programu komputerowego bez upoważnienia;

W związku z zawartym w tekście Zalecenia wezwaniem do uwzględnienia wyniku badań Komitetu Ekspertów w trakcie procesu legislacyjnego i przedłożenia Sekretarzowi Generalnemu zmian ustawodawczych, w 1993 roku Sekretariat Rady Europy zainicjował badania, dotyczące implementacji rozwiązań zawartych w Zaleceniu. Z ankiety, na którą odpowiedziało 16 państw wynika, że większość dostosowała, przynajmniej w części, ustawodawstwo do standardów zawartych w zaleceniu. W przypadku zachowań objętych tzw. listą „minimalną" największa zgodność dotyczy :

- nielegalnego kopiowania i rozpowszechniania programów komputerowych,
- bezprawnego kopiowania topografii półprzewodników,
- oszustwa komputerowego,
- uzyskania nieuprawnionego dostępu do systemu komputerowego;

Większość krajów – respondentów ankiety przewiduje karalność powyższych czynów w swoich ustawodawstwach karnych, jednakże zdefiniowanie tych czynów w prawie wewnętrznym odbiega niekiedy od proponowanych standardów. Różnice występują także w zakresie kryminalizacji czynów z listy minimalnej i opcjonalnej w poszczególnych krajach[159].

Warto w tym miejscu zwrócić uwagę, w przypadku kryminalizacji jakich zachowań stwierdzono największą zgodność ustawodawstwa krajowego z normami Rady Europy – teoretycznie owa zgodność w połowie dotyczyła czynów godzących (może pośrednio) w prawa majątkowe z tytułu praw autorskich.

[159] *A. Adamski – Prawo karne ..., op. cit., str. 8*

4.3 Zalecenie Komitetu Ministrów Rady Europy No. R(95)13 w sprawie problemów karnoprocesowych związanych z nowoczesną technologią przetwarzania informacji – Problems of Criminal Procedural Law Connected with Information Technology, Strasbourg 1995

Inną kwestią, niemniej ważną od skryminalizowania czynów godzących w ochronę zdigitalizowanej informacji, jest zapewnienie organom wymiaru sprawiedliwości odpowiednich mechanizmów ścigania sprawców przestępstw komputerowych. Problem tkwi w jednej z głównych cech tej grupy czynów, a mianowicie w jej transgraniczności – globalne sieci komputerowe są środowiskiem sprzyjającym popełnianiu przestępstw związanych z wykorzystaniem zaawansowanych technologii, jak i ukrywaniu dowodów ich popełnienia i śmiało można je określić mianem „środowiskiem mało przyjaznym dla organów ścigania”[160]. Dotychczasowe przepisy okazały się nieskuteczne w przypadku prowadzenia czynności procesowych związanych z uzyskiwaniem dowodów popełnienia przestępstw z sieci bądź systemów komputerowych, a także brak było odpowiednich regulacji w ustawodawstwie większości krajów regulacji dotyczących współpracy z organami ścigania administratorów systemu bądź ich użytkowników w celu identyfikacji i uzyskania dostępu do danych mogących posiadać wartość dowodową, a które możliwe są do uzyskania tylko w przypadku normalnego funkcjonowania systemu, co wyklucza zajęcie takiego systemu i poddanie go analizie w warunkach laboratoryjnych.

Taki stan rzeczy stał się przyczyną podjęcia działań zmierzających do usprawnienia postępowania karnoprocesowego, czego wynikiem jest Zalecenie Nr (95) 13, do którego załącznik, będący efektem czteroletnich prac grupy ekspertów, zawierający 18 zasad zarekomendowanych przez Komitet Ministrów Rady Europy rządom krajowym do uwzględnienia w ustawodawstwie wewnętrznym i praktyce sądowej i podania tychże do wiadomości przedstawicieli organów ścigania, wymiaru sprawiedliwości oraz innych podmiotów, które mogłyby z racji wykonywanych przez nie funkcji być zainteresowane stosowaniem tych rekomendacji[161]

Podstawowym celem wydania zalecenia Nr (95) 13 było dostosowanie prawodawstwa do zadań stawianych organom ścigania i wymiarowi sprawiedliwości w materii przestępczości komputerowej, w realiach nieustannego rozwoju technologicznego i ewoluowania tejże przestępczości. Można stwierdzić, że zasady, rekomendowane w tym Zaleceniu miały za zadanie nie dopuścić do ograniczenia przez ewolucję techniczną sku-

[160] *A. Adamski – Prawo karne ..., op. cit., str. 182;*
[161] *ibidem;*

teczności organów ścigania. Wspomniane zasady nie formułują postulatów tworzenia nowych instytucji prawnych, lecz rozszerza zakres istniejących na elementy związane ze środowiskiem teleinformatycznym w taki sposób, aby nie naruszać istniejącej struktury środków i gwarancji procesowych.

Pierwszym, węzłowym zagadnieniem poruszonym w załączniku do Zalecenia jest kwestia rozszerzenia zakresu uprawnień organów procesowych w stosunku do przeszukania i zatrzymania, uważanych za podstawowe instrumenty gromadzenia dowodów w sprawach przestępstw komputerowych[162], przy jednoczesnym wymogu adaptacji tych środków do środowiska sieci komputerowych (systemów teleinformatycznych, komputerowych), będących obiektami dynamicznymi, za pomocą wskazanych w załączniku zasad. Pierwsza z nich zawiera postulat jasno określonej przez prawo i przestrzeganej w praktyce różnicy pomiędzy przeszukaniem systemów komputerowych i zajęciem znajdujących się w nich danych a przechwyceniem danych w trakcie ich transmisji, czyli uzyskania tych danych w wyniku stosowania podsłuchu. Ponadto prawo karne procesowe powinno zezwalać na przeszukanie systemów komputerowych i zajęcie znajdujących się tam danych na zasadach odnoszących się do tej pory do tradycyjnej formy przeszukania i zatrzymania – osoba odpowiedzialna za system powinna zostać poinformowana o podjętych działaniach, a środki odwoławcze, przysługujące w przypadku przeszukania i zatrzymania powinny być stosowane w stosunku do przeszukania systemu komputerowego i zajęcia danych (zasada nr 2). Uprawnienie organów ścigania do rozszerzenia zakresu przeszukania na inne systemy połączone ze sobą siecią i zajęcia znajdujących się tam danych, w zakresie swojej jurysdykcji i z poszanowaniem niezbędnych gwarancji procesowych w przypadku zachodzenia przesłanek natychmiastowego podjęcia takich działań stanowi treść zasady nr 3. Zasada nr 4 formułuje postulat odpowiedniego stosowania przepisów procedury karnej odnoszących się do przeszukania i zajęcia tradycyjnego dokumentu w stosunku do danych przetwarzanych automatycznie w każdym przypadku gdy stanowią one funkcjonalny ekwiwalent tradycyjnego dokumentu.

Drugim zagadnieniem, poruszonym w Zaleceniu, jest problem uregulowania w prawie karnym procesowym kwestii korzystania ze środków technicznych przez organy ścigania w celu :

- stosowania technicznej inwigilacji takiej jak przechwytywanie informacji przekazywanych przy użyciu urządzeń telekomunikacyjnych dla celów postępowania karnego (zasada nr 5),

[162] *A. Adamski – Prawo karne ...,op. cit., str. 184;*

- gromadzenia danych ruchowych[163]w związku z prowadzonym postępowaniem (zasada nr 6),
- zabezpieczenia przed nieuprawnionym dostępem danych zgromadzonych w toku dochodzenia, ze szczególnym uwzględnieniem danych uzyskanych w wyniku przechwycenia informacji[164] przesyłanych za pomocą urządzeń telekomunikacyjnych, w przypadku, gdy są prawnie chronione i przetwarzane w systemie komputerowym (zasada nr 7),

Ponadto zasada nr 8 zaleca zapewnienie przez przepisy procedury karnej dopuszczalności stosowania podsłuchu telekomunikacyjnego i gromadzenia danych ruchowych w przypadkach dochodzeń w sprawach o poważne przestępstwa przeciwko poufności, integralności i dostępności systemów telekomunikacyjnych i komputerowych.

Kolejną kwestią poruszoną w Zaleceniu jest rozszerzenie obowiązku współdziałania świadków i biegłych z organami ścigania na środowisko komputerowe w materii zapewnienia pomocy świadków i biegłych w zakresie gromadzenia dowodów przestępstw komputerowych. Pomoc ta może przybierać postać udostępniania danych poszukiwanych przez organy ścigania lub ułatwieniu tym organom dostępu do systemu komputerowego, plików lub danych. Jednocześnie zasady te (zasady 9 i 10) przewidują, że wszelkie formy współdziałania muszą respektować prawne przywileje i gwarancje procesowe. Zasady odwołują się do gwarancji prawnych lub postulują tworzenie nowych, zwłaszcza w kwestii praw podejrzanych i interesu świadków.

Powinność współdziałania z organami ścigania została rozszerzona na operatorów (prywatnych i publicznych) oferujących powszechne usługi telekomunikacyjne w postaci nałożenia szczególnego obowiązku korzystania „ze wszystkich niezbędnych środków technicznych" w celu umożliwienia organom ścigania przechwytywania przekazów informacji w telekomunikacji, czyli korzystanie z podsłuchu oraz zapewnienie możliwości deszyfrowania treści (zasada nr 11) oraz udzielania informacji dotyczących połączeń realizowanych przez ich abonentów i umożliwiających identyfikację użytkowników (zasada nr 12).

Zasada nr 13 porusza zagadnienie gromadzenia, zabezpieczania i prezentowania dowodów elektronicznych. W szczególności zwraca uwagę na potrzebę dokonywania tych czynności w taki sposób, który najlepiej zapewnia i wyraża ich integralność i niepodważalną autentyczność, jak również zaleca usprawnienie procedur postępowania z dowo-

---

[163] *ang. „traffic data"*

[164] *należy zwrócić uwagę na kłócące się z przedstawioną wcześniej przez autora typizacją zakresu znaczeniowego pojęć „informacja" i „dane" – informacja jako efekt interpretacji danych; przyjęcie takiego założenie pozbawia sensu stwierdzenie „dane uzyskane w wyniku przechwycenia informacji";*

dami elektronicznymi tak, aby możliwe było ich wzajemne stosowanie w państwach członkowskich.

Problematykę dowodów elektronicznych w zakresie ich dostępności dla organów ścigania porusza zasada nr 14 stwierdzając konieczność ograniczenia ujemnych skutków stosowania technik kryptograficznych, jednakże bez ograniczania zgodnego z prawem stosowania tych technik, formułując jednocześnie postulat znalezienia kompromisu pomiędzy interesem wymiaru sprawiedliwości a potrzebami użytkowników kryptografii.

Zalecenie zwraca uwagę na konieczność prowadzenia regularnych ocen w zakresie zagrożeń związanych z rozwojem i stosowaniem technologii informatycznej w celu przygotowania środków przeciwdziałania zjawisku przestępczości komputerowej, będących na bieżąco z aktualnie panującymi trendami rozwoju. Dużą wagę przywiązuje się do gromadzenia i analizy danych dotyczących przestępstw popełnianych z wykorzystaniem komputera, w które to dane włączono również sposoby działania sprawców i aspekty techniczne (zasada nr 15).

Konieczność zapewnienia nie tylko mechanizmów prawnych, ale także infrastruktury technicznej i wyspecjalizowanego zaplecza ludzkiego znalazła oddźwięk w treści zasady nr 16, zalecającej rozważenie utworzenia specjalnych jednostek organizacyjnych, do zadań których należałoby prowadzenie dochodzeń w sprawach przestępstw, których zwalczanie wymaga specjalistycznej wiedzy w zakresie technik informatycznych. Tym samym postuluje prowadzenie szkoleń dla pracowników wymiaru sprawiedliwości w celu podnoszenia ich kwalifikacji zawodowych w tej dziedzinie.

Ostatnim zagadnieniem poruszonym w Zaleceniu jest problematyka współpracy międzynarodowej przy ściganiu przestępstw komputerowych, która nabiera szczególnego znaczenia, biorąc pod uwagę aspekt transgraniczności przestępczości komputerowej i zasadę terytorializmu obejmującą jej ściganie. W ostatnich dwu zasadach (17 i 18) zasugerowano nowe formy współpracy, takie jak transgraniczne przeszukanie i zajęcie danych, specjalne procedury przyspieszone oraz system oficerów łącznikowych.

Podsumowując, Zalecenie Nr (95) 13 objęło regulowaną materią szeroki zakres problematyki karnoprocesowej, związanej ze ściganiem przestępstw teleinformatycznych. Poruszono w nim zarówno kwestie dotyczące adaptacji instytucji przeszukania i zatrzymania do realiów przestępczości teleinformatycznej, korzystania ze środków technicznych przez organy ścigania w związku z prowadzonym postępowaniem, nałożenia obowiązku współdziałania z organami ścigania biegłych, świadków i operatorów telekomunikacyjnych. Uwzględniono w nim także, w zakresie proponowanych rozwiązań, problematykę gromadzenia i zabezpieczania dowodów przestępstw komputerowych oraz kwestie zwią-

zane z prowadzeniem badań nad zjawiskiem, zapewnienie organom ścigania zaplecza technicznego i merytorycznego, a także wskazano możliwe rozwiązania w zakresie usprawnienia współpracy międzynarodowej. Mając na uwadze powyższe można stwierdzić, iż Zalecenie Nr (95) 13 stanowiło kompleksowe przedstawienie sposobów mających usprawnić prowadzenie działań operacyjnych przez funkcjonariuszy organów ścigania w stosunku do sprawców przestępstw komputerowych.

4.4 Konwencja Rady Europy o Cyberprzestępczości – Convention on Cybercrime, Budapest 23.11.2001, European Treaty Series No. 185

Projekt konwencji został przyjęty przez Komitet Problemów Przestępczości Rady Europy 21 czerwca 2001 r. Konwencję podpisano 23 listopada 2001 r. w Budapeszcie. Ma ona stanowić ukoronowanie (i niejako kontynuację) prac Rady Europy w dziedzinie tworzenia międzynarodowych standardów normatywnych skierowanych przeciwko przestępczości komputerowej, których efektem były zalecenia z 1989 r. i 1995 r., opisane powyżej[165].

Działalność taka, zmierzająca w kierunku przyjęcia jednolitych rozwiązań prawnych w ustawodawstwie karnym wielu państw jest warunkiem niezbędnym skutecznej międzynarodowej współpracy w dziedzinie zwalczania przestępczości – zwłaszcza, mając na uwadze transgraniczny charakter Internetu, przestępczości komputerowej. Konsekwencje rozbieżności unormowań prawnokarnych pomiędzy państwami można było obserwować na przykładzie sprawy autorów wirusa „I love you", kiedy to niespełnienie warunku podwójnej karalności uniemożliwił postawienie im zarzutów[166]. Zrozumiałe jest więc podejmowanie inicjatyw zmierzających w kierunku likwidacji „prawnych rajów dla hackerów". Omawiana Konwencja stanowi kompleksowe przedstawienie rozwiązań na tym polu – do jej podstawowych założeń należy zwalczanie przestępczości teleinformatycznej i upowszechnienie przyjętych w jej tekście standardów prawnych. Tej drugiej koncepcji sprzyjać ma otwarty charakter Konwencji (co umożliwia przystąpienie do niej państw nie będących członkami Unii Europejskiej[167]) oraz pozostawienie znacznej liczby klauzul opcjonalnych, dających poszczególnym państwom – sygnatariuszom większe możliwości dostosowania zakresu kryminalizacji do obowiązującego porządku prawnego. Ponadto, w

---

[165] A. Adamski – Przestępczość w cyberprzestrzeni ..., op. cit., str. 9;
[166] A. Adamski – Rządowy projekt dostosowania polskiego kodeksu karnego do Konwencji Rady Europy o cyberprzestępczości. Materiały z konferencji Secure 2003; źródło : CERT Polska, http://www.cert.pl;
[167] do Konwencji przystąpiły cztery państwa nie będące członkami Rady Europy : Japonia, Kanada, RPA i Stany Zjednoczone A.P; źródło :
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=04/11/2005&CL=ENG

tym samym celu, Konwencja posługuje się standardami minimalnymi, dopuszczając możliwość częściowej rezygnacji z przyjętych w niej założeń[168].

Na dzień dzisiejszy (listopad 2005) Konwencję podpisało 31 państw, z czego ratyfikowało ją 11 z nich[169] - swoistą ciekawostką może wydawać się stanowienie większości wśród tych państw przez kraje relatywnie niedawno przyjęte do Wspólnoty[170].

Strukturę Konwencji stanowią trzy, stanowiące integralną całość, części – przepisy dotyczące prawa karnego materialnego, prawa karnego procesowego i uregulowań dotyczących współpracy międzynarodowej.

Konwencja , w materii prawa karnego materialnego, proponuje rozszerzenie listy przestępstw, o jakie państwa – sygnatariusze zobowiązani będą wzbogacić swoje ustawodawstwa karne. przewiduje także wprowadzenie karalności form stadialnych i zjawiskowych przestępstw konwencyjnych. Jednocześnie wprowadza nowy podział przestępstw, dzieląc zachowania naruszające prawo w cyberprzestrzeni na cztery podstawowe grupy :

1. Przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów (czyli, wg wiodącego w niniejszej pracy podziału, przestępstwa komputerowe *sensu stricte*); w tej kategorii typizowane są następujące zachowania :
    - art. 2 – nielegalny dostęp (hacking);
    - art. 3 – nielegalne przechwytywanie danych;
    - art. 4 – naruszenie integralności danych;
    - art. 5 – naruszenie integralności systemu;
    - art. 6 – niewłaściwe użycie urządzeń (kryminalizacja m. in. wytwarzania narzędzi hackerskich);
2. Przestępstwa komputerowe :
    - art. 7 – fałszerstwo komputerowe;
    - art. 8 – oszustwo komputerowe;

---

[168] *R. Koszut – Nowelizacja prawa karnego z 18.03.2004 r. w świetle wymagań Konwencji o Cyberprzestępczości,* [w:] *J. Kosiński (red.) – Przestępczość teleinformatyczna, str. 36, Szczytno 2004*

[169] *Albania, Bułgaria, Chorwacja, Cypr, Dania, Estonia, Węgry, Litwa, Macedonia, Rumunia i Słowenia; źródło : http://www.cybercrimelaw.net/tekster/international_agencys.html;*

[170] *wg innego źródła, na początku maja 2004 r. Konwencję podpisały 34 państwa, z czego ratyfikowało ją 5; por. R. Koszut – Nowelizacja prawa karnego z 18.03.2004 r. w świetle wymagań Konwencji o Cyberprzestępczości,* [w:] *J. Kosiński (red.) – Przestępczość teleinformatyczna, str. 35, Szczytno 2004; właściwy wydaje się być stan na 5 listopada 2005 podany wcześniej – por. : http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=04/11/2005&CL=ENG;*

3. Przestępstwa ze względu na charakter zawartych informacji :
    - art. 9 – przestępstwa związane z pornografią dziecięcą
4. Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych :
    - art. 10 – przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych;

Konwencja w art. 11 rozszerzyła również zakres odpowiedzialności karnej na stadium usiłowania (w odniesieniu do większości typizowanych przestępstw[171]), przewidując jednocześnie fakultatywność stosowania przepisu, oraz podżeganie i pomocnictwo w stosunku do przestępstw określonych w art. 2 – 10 Konwencji, które objęto wymogiem działania w zamiarze bezpośrednim[172]. Artykułem 12 Konwencja wprowadza odpowiedzialność karną osób prawnych za przestępstwa konwencyjne popełnione przez osoby fizyczne w „interesie" tych osób, przy czym odpowiedzialność karna osoby prawnej nie wyklucza odpowiedzialności sprawcy „wykonawczego", będącego osobą fizyczną.

Ponieważ Konwencja stała się podstawowym aktem europejskim normalizującym kryminalizację przestępczości teleinformatycznej, a także ze względu na omówienie przepisów zawartych w Kodeksie Karnym na tle Konwencji, omówię pokrótce charakterystykę przepisów zawartych w Tytule 1 Konwencji – „Przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów" (artykuły 2 – 6). Ponieważ korelacje odpowiednich przepisów polskiego Kodeksu Karnego z wzmiankowanymi przepisami zostaną omówione w rozdziale poświęconym kryminalizacji tych zachowań w polskim porządku prawnym, poniżej przedstawię jedynie krótką charakterystykę rozwiązań konwencyjnych.

Artykuł 2 [Nielegalny dostęp] obliguje strony do kryminalizacji zachowań, polegających na „umyślnym, bezprawnym[173] dostępie do całości lub części systemu informatycznego", tym samym w sposób zwięzły i jasny definiując niejako przestępstwo powszechnie określane mianem "hackingu". Fakultatywnym zagrożeniem sankcją karną objęto takie czynniki jak : popełnienie przestępstwa poprzez naruszenie zabezpieczeń, zamiar pozyskania danych informatycznych[174] lub inny nieuczciwy zamiar, popełnienie

---

[171] *czyny określone w art. 3 – 5, 7, 8, 9 ust. 1 lit. a i 9 ust. 1 lit. c;*
[172] *konstrukcja taka skutkuje wykluczeniem odpowiedzialności karnej dostawcy usług internetowych za wykorzystywanie tych usług przez inne podmioty w celu popełnienia wymienionych przestępstw – por. A. Adamski – Przestępczość w cyberprzestrzeni ..., op. cit., str. 59;*
[173] *wymóg umyślności i bezprawności dotyczy wszystkich przestępstw typizowanych w omawianym tytule, więc opuszczę go przy omawianiu kolejnych artykułów;*
[174] *mimo pozornego podobieństwa do istniejącego obecnie w Kodeksie Karnym zwrotu „uzyskanie informacji", sformułowanie użyte w tekście Konwencji odnosi się do zupełnie innego działania sprawcy; bardziej szczegółowo kwestia zostanie omówiona w rozdziale VI;*

przestępstwa w stosunku do systemu informatycznego połączonego z innym systemem informatycznym. Konstrukcja tego artykułu w swojej obligatoryjnej części jest niezwykle prosta i praktycznie nadaje się do implementacji do wewnętrznego porządku prawnego w swoim oryginalnym brzmieniu, jednocześnie będąc niezwykle elastyczna jako całość, pozostawiając państwom członkowskim duża swobodę w zakresie doboru czynników fakultatywnych[175].

W artykule 3 [Nielegalne przechwytywanie danych] Konwencja wprowadza karalność przechwytywania niepublicznych transmisji danych informatycznych, do, z, lub w ramach systemu informatycznego za pomocą urządzeń technicznych, z uwzględnieniem przechwytywania emisji elektromagnetycznych, pochodzących z systemu informatycznego, przekazującego takie dane. Fakultatywność karalności dotyczy przypadku popełnienia z nieuczciwym zamiarem lub w związku z systemem informatycznym połączonym z innym systemem informatycznym.

[Naruszenie integralności danych], stanowiące treść artykułu 4, jest kryminalizowane w postaci niszczenia, wykasowywania, uszkadzania, dokonywania zmian lub usuwania danych informatycznych. Ciekawą kwestią w przypadku tego przepisu jest użycie pozornie tożsamych sformułowań „wykasowuje" i „usuwa" – z tym, że wskazuje to na dalekowzroczność ustawodawcy, jako że określenie „wykasowuje" wskazuje na pewną czynność, która nie musi skutkować nieodwracalną utratą danych, natomiast „usuwa" pomija rodzaj czynności, jaki prowadzi do tego skutku, nacisk kładąc na jego nieodwracalność. Konwencja zezwala na zastrzeżenie przez strony warunku zaistnienia skutku w postaci poważnej szkody.

Artykuł 5 [Naruszenie integralności systemu] wprowadza kryminalizację poważnego zakłócania funkcjonowania systemu informatycznego poprzez wprowadzanie, transmisję, niszczenie, wykasowywanie, dokonywanie zmian lub usuwanie danych informatycznych bez uprawnienia[176]. Przepis obejmuje sankcją karną spowodowanie zakłóceń w działaniu systemów informatycznych lub całkowitą ich blokadę, będące najbardziej rozpowszechnioną formą zamachów godzących w bezpieczeństwo informacji. Przykładem czynu należącego do takiej kategorii jest atak typu *Denial of Service (DoS)*.

Najbardziej (chociaż bliższe prawdy jest określenie „jedynym") kontrowersyjnym przepisem tytułu 1 jest artykuł 6 [Niewłaściwe użycie urządzeń], który sprawił polskiemu

---

[175] poza oczywistym kryminalizowaniem innego czynu przestępnego przez art. 267 § 1 KK, rzuca się w oczy jednoczesne przyjęcie przez rodzimego ustawodawcę dwu pierwszych fakultatywnych przesłanek karalności, co ewidentnie osłabia skuteczność rzeczonego przepisu;

[176] podobna interakcja pojęć jak w artykule poprzednim i mająca takie samo znaczenie;

ustawodawcy, sądząc po efektach w postaci art. 269b KK, niemały problem[177]. Przepis ten obejmuje kryminalizacją dwojakiego rodzaju zachowania :

1. produkcję, sprzedaż, pozyskiwanie z zamiarem wykorzystania, importowanie, dystrybucję lub inne udostępnianie :
    - urządzenia (w tym programu komputerowego[178]), przeznaczonego lub przystosowanego **przede wszystkim** dla celów popełnienia przestępstwa z art. 2 -5 Konwencji;
    - hasła komputerowego, kodu dostępu lub podobnych danych, warunkujących dostępność całości lub części systemu informatycznego

z zamiarem wykorzystania dla celów popełnienia przestępstwa określonego w art. 2 – 5 Konwencji; oraz

2. posiadanie wyżej wymienionej jednostki z zamiarem wykorzystania w celu popełnienia przestępstwa wymienionego w art. 2 – 5 Konwencji; opcjonalnością w tym punkcie objęto zastrzeżenie w prawie krajowym wymogu posiadania większej ilości takich jednostek.

Powyższe unormowania określane są potocznie mianem „kryminalizacji narzędzi hackerskich", a praktycznie jest to próba kryminalizacji formy stadialnej przestępstwa, jaką jest przygotowanie („pozyskiwanie z zamiarem wykorzystania ..."). Objęcie karalnością wytwarzania i zbywania takich „narzędzi" wydaje się być uzasadnione, biorąc pod uwagę istnienie i rozwój wtórnego rynku, oferującego je do sprzedaży[179].

Na gruncie polskiego Kodeksu Karnego największe kontrowersje wzbudza ust. 2 art. 6 Konwencji – a to dzięki nieuwzględnieniu jego treści w redakcji analogicznego przepisu polskiej ustawy karnej. Rzeczony przepis praktycznie jest zaproszeniem dla wewnętrznego ustawodawcy do tworzenia kontratypów, jeśli zachowanie typizowane w ust. 1 art. 6 nie jest dokonywane w celu popełnienia któregokolwiek z przestępstw wymienio-

---

[177] dokładne omówienie art. 269b KK na tle Konwencji znajduje się w rozdziale V niniejszej pracy;

[178] uznanie przez Konwencję w tym kontekście programu komputerowego za urządzenie rzuca nowe światło na interpretację pojęcia „inne urządzenie specjalne" w treści art. 267 § 2 KK, co do którego wynikła rozbieżność poglądów dotycząca uznania komputera wyposażonego w oprogramowanie przystosowane do podsłuchu za takie urządzenie (A. Adamski), bądź też nie (W. Wójcik), z czego autor skłania się ku poglądowi nieuznawania komputera za takie urządzenie; szerzej na ten temat w szczegółowym omówieniu przepisu art. 267 § 2 w rozdziale V;

[179] wg raportu CERT Polska, na sprzedaż oferuje się prawie wszystko, co może służyć do przeprowadzenia ataku na systemy informatyczne – w 2002 roku cena za „0-day exploit" oscylowała wokół 500 USD, natomiast za abonament w wysokości 5000 USD rocznie uzyskiwało się prawo korzystania z dostępu do rozproszonej sieci tzw. „botnet" (w celu dalszego wykorzystania np. do ataku typu DDoS); M. Maj – Sieć zagrożeń w sieci Iinternet. Raport CERT Polska 2004, http://www.cert.pl;

nych w art. 2 – 5 Konwencji, „jak w przypadku dozwolonego testowania lub ochrony systemu informatycznego" – co stanowi wyraźne zalecenie dla legislatora[180].

W ust. 3 niniejszego przepisu Konwencja przewiduje możliwość zastrzeżenia przez strony niestosowania postanowień ust. 1 niniejszego artykułu, pod warunkiem, że zastrzeżenie to nie obejmuje sprzedaży, dystrybucji lub innego udostępniania jednostek takich jak hasła komputerowe, kody dostępu i podobne dane, warunkujące uzyskanie dostępu do całości lub części systemu komputerowego. Jak łatwo zauważyć, kryminalizacja grupy narzędzi, które można określić mianem „hackerskich" bądź „przestępczych", dokonana przez Konwencję jest bardzo elastyczna i dopuszcza, poza ściśle określonymi przypadkami, swobodne regulowanie zakresu przez wewnętrzne regulacje prawnokarne. Praktycznie, zachowania sprawcy zawarte w ust 1 są obligatoryjnie zagrożone karalnością w zakresie sprzedaży, dystrybucji i innego udostępniania haseł i kodów dostępu – w tym przypadku wyraźnie zauważalne jest szerokie pole widzenia ustawodawcy unijnego, zwłaszcza, jeśli chodzi o przypadek programów „podwójnego przeznaczenia", czego niestety rodzimy ustawodawca dostrzec nie zdołał[181].

W materii prawa karnego procesowego Konwencja określa rodzaje działań, jakie należy podjąć na szczeblu ustawodawstwa państwa członkowskich, aby wyposażyć organy procesowe w instrumenty, pozwalające na efektywne prowadzenie postępowań karnych w sprawach o popełnienie przestępstw związanych z technologią teleinformatyczną. Problematyka procesowa w materii szczegółowej zawarta jest w części II Konwencji (art. 16 – 21) następująco :

- Tytuł 2 – *Niezwłoczne zabezpieczanie przechowywanych danych* określa warunki zabezpieczenia danych przechowywanych w systemie informatycznym (art. 16) oraz zabezpieczenia i częściowego ujawnienia danych dotyczących ruchu (art. 17);
- Tytuł 3 – *Nakaz dostarczenia* zawiera przepisy dotyczące uprawnień właściwych organów do nakazania wskazanym podmiotom dostarczenia określonych danych informatycznych i informacji dotyczących abonentów (art. 18);

---

[180] jeden z głównych zarzutów autora niniejszej pracy do redakcji art. 269b KK, mającego w założeniu być implementacją art. 6 Konwencji na gruncie prawa polskiego, dotyczy właśnie całkowitego pominięcia kwestii możliwości – wręcz przez konwencję zalecanej – stworzenia odpowiednich kontratypów;

[181] aby nie stwarzać fałszywego wyobrażenia na temat wszechwiedzy ustawodawcy unijnego – po opublikowaniu projektu Konwencji nastąpiła fala protestów społeczności internetowej przeciw karalności tworzenia, udostępniania, używania etc. programów wymienionych w treści art. 6 Konwencji; protesty dotyczyły kwestii „podwójnego przeznaczenia" takich narzędzi i spowodowały wprowadzenie klauzuli w postaci ust. 2 do art. 6 Konwencji; por. A. Adamski – Przestępczość w cyberprzestrzeni ..., op. cit., str. 41-42;

- Tytuł 4 – *Przeszukanie i zajęcie przechowywanych danych informatycznych* dotyczy regulacji instytucji przeszukania i zajęcia w stosunku do danych przechowywanych w systemach informatycznych lub na nośniku służącym do przechowywania takich danych, a także rozszerzenia zakresu tych instytucji na inne systemy informatyczne (jeśli zajdzie uzasadniona konieczność takiego postępowania) oraz nadania właściwym organom uprawnień do zajęcia lub zabezpieczenia takich danych (art. 19);
- Tytuł 5 – *Gromadzenie danych informatycznych w czasie rzeczywistym* reguluje problematykę gromadzenia w czasie rzeczywistym danych związanych z ruchem (art. 20) i przejmowania danych związanego z ich treścią (art. 21).

W zakresie współpracy międzynarodowej, art. 23 Konwencji wprowadza zasady, na jakich współpraca ta powinna się opierać – ułatwiania współpracy i minimalizowania przeszkód, ścigania przestępstw zawartych w tekście Konwencji jak i wszystkich innych popełnionych z wykorzystaniem technologii teleinformatycznych (łącznie z przestępstwami „tradycyjnymi", gdy dowody ich popełnienia mają postać elektroniczną) oraz zgodności z postanowieniami części III niniejszej Konwencji oraz innych umów międzynarodowych dotyczących pomocy w sprawach karnych[182].

Podsumowując, Konwencja stanowi jak dotąd ukoronowanie działalności Rady Europy na polu walki z przestępczością teleinformatyczną. Zmierzając w kierunku wytyczonym przez regulacje Zaleceń Nr (89) 9 i (95) 13 jednocześnie znacznie rozszerza zakres ich unormowań. Na gruncie prawa karnego materialnego, poza wydłużeniem listy przestępstw komputerowych, postuluje nieuwzględnione dotychczas, wprowadzenie karalności form zjawiskowych i stadialnych tych czynów, a także wprowadza odpowiedzialność osób prawnych. W materii prawa karnego procesowego, poza rozszerzeniem dotychczasowych rozwiązań, określa zasady jurysdykcji transgranicznych przestępstw komputerowych i przesłanki ekstradycji sprawców[183]. Silny nacisk w Konwencji kładzie się na aspekt współpracy międzynarodowej w ściganiu tego rodzaju przestępstw (czego wyrazem jest m. in. otwarty charakter tej regulacji) – mając na uwadze charakter sieci, jaką jest Internet, jest to warunek *sine qua non* skutecznego przeciwdziałania zjawisku.

[182] *A. Adamski – Przestępczość w cyberprzestrzeni ..., op. cit., str. 105;*
[183] *A. Adamski – Przestępczość w cyberprzestrzeni ..., op. cit., str. 10;*

5. Rozdział V – *Przestępstwa komputerowe* w polskim Kodeksie Karnym z 1997 r.

Ustawa Kodeks Karny, uchwalona 6 czerwca 1997 roku zaczęła obowiązywać 1 września 1998 r. Wniosła ona do polskiego prawodawstwa karnego uregulowania dotychczas nieznane, ściśle związane z ochroną informacji w środowisku technologii komputerowej i automatycznego przetwarzania danych, bądź znacznie rozbudowane w stosunku do istniejących w trakcie obowiązywania ustawy karnej z 1969 r., która nie zawierała regulacji bezpośrednio związanych z technologią informatyczną (co nie oznacza, że nie obejmowała tych czynów – przynajmniej częściowo – karalnością). Za bezsprzeczny należy uznać fakt, że Kodeks Karny z 1997 r. uwzględnił powstawanie podwalin społeczeństwa informacyjnego, a co za tym idzie znaczenie, jakie w tych realiach posiada informacja. Uznanie wartości informacji obejmuje także potrzebę jej prawnokarnej ochrony, czego ustawodawca dał wyraz, umiejscawiając w treści Kodeksu należne przepisy.

5.1 Wprowadzenie;

Na potrzeby tego rozdziału będę się posługiwał podziałem „przestępstw komputerowych" na *sensu stricte* i *sensu largo*, gdzie wyznacznikiem podziału jest dobro prawne podlegające ochronie[184]. W rozdziale XXXIII Kodeksu Karnego z 1997 roku, zatytułowanym „przestępstwa przeciwko ochronie informacji" ochroną objęto informację, zapewniając jej dostępność, integralność i poufność. Ochrona tych atrybutów informacji – w aspekcie jej automatycznego przetwarzania - umieszczona jest w Kodeksie Karnym następująco[185] :

1. dostępność – formą zamachu może być sabotaż, wandalizm, zawirusowanie systemu, przeładowanie systemu danymi; przepisem kwalifikującym te czyny jest art. 269 § 1 KK, penalizujący uniemożliwienie automatycznego gromadzenia lub przekazywania informacji o szczególnym znaczeniu dla administracji rządowej;
2. integralność – może być naruszona poprzez włamanie do systemu, manipulacje danymi i oprogramowaniem, rekonfigurację systemu, wprowadzenie konia trojańskiego; sankcje karne zawiera art. 268 § 2KK, stanowiąc krymi-

[184] *jest to de facto podział na przestępstwa godzące bezpośrednio w informację (dane) i systemy służące do jej przetwarzania i przestępstwa tradycyjne, możliwe do popełnienia przy pomocy zaawansowanej technologii lub przez nią ułatwiane; podział „przestępstw komputerowych" stanowi treść rozdziału II;*
[185] *w brzmieniu kodeksu sprzed „cybernowelizacji" z marca 2004 r.;*

nalizację kasowania lub modyfikacji danych, utratę kontroli nad zarządzaną siecią komputerową;[186]

3. poufność – naruszana z pomocą podsłuchu lub włamania do systemu, poprzez przeglądanie chronionej informacji, kopiowanie plików lub baz danych przez osoby nieuprawnione; szkoda w postaci przechwycenia przesyłanej informacji, odszyfrowania haseł użytkowników, naruszenia tajemnicy korespondencji lub ochrony danych osobowych zagrożona jest karą przez art. 267 § 1 lub 2[187]

W związku z przyjęciem przez Sejm nowelizacji Kodeksu Karnego[188], zmianie uległa część przepisów dotychczas regulujących materię prawnokarnej ochrony informacji, jak również pojawiły się nowe – m. in. do przedmiotów podlegających ochronie dodano integralność systemów przetwarzających informację. Charakter tych zmian zostanie opisany poniżej właściwości danego przepisu sprzed „cybernowelizacji".

Ponadto część „przestępstw komputerowych" ujęta została pozakodeksowo w różnych ustawach szczególnych – regulacje te zostaną omówione bardzo pobieżnie (chciałbym jedynie zasygnalizować ich istnienie w porządku polskiego prawa karnego).

5.2 Przestępstwa komputerowe sensu stricte Rozdział XXXIII – Przestępstwa przeciwko ochronie informacji;

Zamieszczenie w odrębnym rozdziale ustawy karnej katalogu przestępstw przeciwko ochronie informacji, stanowiące usystematyzowanie norm prawnych chroniących informację, stanowi jedną z tez koncepcji „prawa karnego informacyjnego" U. Siebera, z jej fundamentalnym założeniem poddania dóbr niematerialnych (takich jak informacja) innemu reżimowi ochrony prawnej od ochrony, jakiej podlegają dobra materialne. Postulat ten znalazł odzwierciedlenie w polskiej ustawie karnej, która jest jedną z niewielu tego rodzaju[189]. Ponieważ przestępstwo z art. 267 § 1 będzie omawiane szerzej w rozdziale VI niniejszej pracy, pozwoliłem sobie nie uwzględniać go przy wyliczaniu czynów wymienionych w rozdziale XXXIII KK. Ponadto pominąłem również przepisy artykułów 265 i 266 KK (ujawnienie tajemnicy państwowej i służbowej), jako że nie mieszczą się one, na gruncie przesłanek koniecznych do popełnienia przestępstw z tych artykułów, w ramach

[186] *integralność jest atrybutem przysługującym zarówno informacji jak systemom służącym do jej przetwarzania (por. art. 4 i 5 Konwencji o Cyberprzestępczości); znalazło to także odbicie w Kodeksie Karnym po jego nowelizacji z dnia 18 marca 2004;*
[187] *A. Adamski – prawo karne ..., op. cit., str. 43;*

przestępstw przeciwko ochronie informacji magazynowanej, przesyłanej i przetwarzanej w formie zdigitalizowanej.

art. 267 § 2 – podsłuch komputerowy;

Przestępstwo z art. 267 § 2 popełnia ten, kto „w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym". Przepis ten nie miał odpowiednika w ustawie karnej z 1969 r.

Przedmiotem ochrony przestępstwa z tego artykułu jest poufność informacji (ochrona sfery życia prywatnego[190]), czyli prawo do wyłącznego dysponowania określoną informacją przez osobę do tego uprawnioną. Przesłankami karalności jest zakładanie lub posługiwanie się urządzeniami technicznymi w celu uzyskania zastrzeżonych rodzajów informacji. Wyliczenie sposobów przechwycenia informacji, do której sprawca nie jest upoważniony, nie ma charakteru *numerus clausus* ze względu na użycie zwrotu „inne urządzenia specjalne", co rozciąga karalność na wszelkie sposoby pozyskiwania przez sprawcę informacji dla niego nie przeznaczonych z wykorzystaniem urządzeń specjalnie do tego przystosowanych. W przeciwieństwie do czynu typizowanego w § 1 ustawodawca nie uzależnia karalności przechwycenia informacji od warunku „przełamania zabezpieczeń". Wynikająca z art. 267 § 1 zasada uzależniająca możliwość skorzystania z prawnej ochrony poufności informacji od jej zabezpieczenia dotyczy informacji przechowywanej w systemie komputerowym i nie ma zastosowania na gruncie danych przesyłanych lub wprowadzanych do systemu, ponieważ podstawową funkcją przepisu § 2 jest ochrona prywatności człowieka przed różnymi formami inwigilacji[191]. Przepis ten sankcjonuje również (poprzez zawarcie w nim zwrotu „inne urządzenie specjalne") inne, bardzo różnorodne formy ingerencji w ludzką prywatność, polegające na przechwytywaniu dźwięku, obrazu za pomocą urządzeń znajdujących się w lokalu lub też poza nim, w bliskiej lub dalszej odległości. Forma komunikacji za pomocą sieci komputerowych oferuje bardzo szeroki wachlarz możliwości naruszenia dyspozycji przepisu art. 267 § 2, np. przechwytywanie za pomocą „loggera" danych wprowadzanych do pamięci komputera za pomocą klawiatury, czy też rekonfiguracja komunikujących się ze sobą w sieci komputerów w taki sposób, żeby do danego komputera spływała kopia całej korespondencji elektronicznej danej sieci. Podsłuchu transmisji teleinformatycznej można dokonywać na wiele sposobów – np. monitorowanie ruchu w danej sieci za pomocą „sniffera" i przechwytywanie początkowej se-

---

[188] *ustawa z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks Karny, ustawy – Kodeks Postępowania Karnego oraz ustawy – Kodeks Wykroczeń (Dz. U. z 2004 r. Nr 69 poz. 626) zwaną dalej „cybernowelizacją KK";*
[189] *A. Adamski – Prawo karne ..., op. cit., str. 35-36;*
[190] *L. Gardocki – Prawo karne, wyd. C. H. Beck, str. 293;*
[191] *A. Adamski – Prawo karne .., op. cit., str. 56;*

kwencji bajtów każdej sesji, zawierającej „loginy" i „hasła" użytkowników, czy też stosowanie „spoofingu" w celu podszycia się pod użytkownika dysponującego dostępem w celu uzyskania dostępu do systemu (w tym przypadku jednak problem stanowi udowodnienie sprawcy działania w celu uzyskania informacji)[192]. Posługiwanie się komputerem jako „urządzeniem specjalnym" stanowi kwestię sporną[193]. Wśród innych metod zamachu na poufność informacji wymieniana jest także analiza promieniowania elektromagnetycznego, generowanego przez sprzęt komputerowy – jest to rodzaj podsłuchu bezinwazyjnego, przez co trudnego do wykrycia. Podsumowując, podsłuch komputerowy obejmuje trzy podstawowe grupy przypadków : przejmowanie danych z transmisji teleinformatycznych, przechwytywanie informacji wprowadzanych do komputera za pomocą klawiatury i analizę fal elektromagnetycznych emitowanych przez sprzęt komputerowy, co pozwala stwierdzić, że obejmuje zakresem penalizacji wszystkie znane w chwili obecnej techniki służące do stosowania podsłuchu komputerowego[194].

Art. 267 § 2 formułuje zakaz posługiwania się urządzeniami technicznymi w celu naruszenia poufności wszelkiej informacji nie przeznaczonej dla sprawcy, nie jest jednak zakazem bezwzględnym, albowiem istnieje grupa podmiotów, które po spełnieniu ściśle określonych warunków stają się podmiotami uprawnionymi do posługiwania się urządzeniami, o których mówi przepis (np. Szef Urzędu Ochrony Państwa, Minister Spraw Wewnętrznych i Administracji).

Przestępstwo określone w art. 267 § 2 jest przestępstwem umyślnym, możliwym do popełnienia tylko w zamiarze bezpośrednim.

Przepis nie uległ nowelizacji w marcu 2004 r. – art. 267 § 2 spełnia wszystkie wymogi stawiane przez art. 3 Konwencji, z wyjątkiem uregulowania kwestii norm uprawniających pracodawców do monitorowania przekazów informacji osób zatrudnionych w miejscu pracy[195] - w przypadku braku tej regulacji, wspomniane wyżej działanie pracodawcy będzie działaniem sprzecznym z art. 267 § 2.

art. 268 § 2 – naruszenie integralności komputerowego zapisu informacji;

Art. 268 nie miał odpowiednika pod rządami ustawy karnej z 1969 r. – został wprowadzony do Kodeksu Karnego z 1997 r. ze względu na wzrost znaczenia informacji

---

[192] A. Adamski – Prawo karne ..., op. cit., str. 57;

[193] A. Adamski uważa, że za urządzenie takie może uznać komputer, na którym zainstalowano oprogramowanie do przechwytywania informacji; odmiennie W. Wróbel, który odmawia tej cechy komputerowi wyposażonemu w taki program; A. Adamski – Prawo karne ..., op. cit., str. 59;

[194] A. Adamski – Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy, wyd. TNOiK Toruń 2001, str. 25;

[195] wymóg unormowania w prawie stron Konwencji takiego uprawnienia zgłosiło Zgromadzenie Parlamentarne Rady Europy – Opinia Zgromadzenia Parlamentarnego Rady Europy nr 226 z dnia 24 kwietnia 2004 r. [w:] A. Adamski – Przestępczość w cyberprzestrzeni, op. cit., str. 27;

w życiu codziennym, a co za tym idzie, coraz poważniejsze skutki, jakie niesie za sobą pogwałcenie integralności zapisu i systemów służących do przetwarzania informacji.

Integralność komputerowego zapisu informacji na gruncie Kodeksu Karnego otrzymuje ochronę na mocy art. 268 § 2, którego dyspozycja jest zależna od treści § 1 tegoż artykułu, chroniącego integralność zapisu informacji oraz jej dostępność (przez co należy rozumieć możliwość swobodnego korzystania z tej informacji przez osoby do tego uprawnione). Z treści art. 268 § 1 wynika, że odpowiedzialności karnej podlega ten, kto nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis[196] istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia[197] osobie uprawnionej zapoznanie się z nią. Przedmiotem ochrony jest „istotna informacja", przy czym mowa jest o informacji istotnej w znaczeniu obiektywnym (a nie subiektywnym), więc przy ocenie znaczenia należy uwzględniać uzasadniony interes dysponenta informacji, osoby uprawnionej do zapoznania się z jej treścią, a także cel, jakiemu służyła (miała służyć), ewentualnie, w przypadku danych osobowych, interes podmiotu, którego informacja dotyczy[198]. Przestępstwo ma charakter powszechny (jego podmiotem może być każdy, z wyjątkiem jednak podmiotów uprawnionych) Jak pisze A. Adamski, trudno znaleźć w prawie porównawczym przykład tak szerokiego ujęcia zakazu naruszenia integralności zapisu informacji, podając przykłady unormowań państw członkowskich, gdzie regulacja ta została zawężona do zapisu danych komputerowych, które ze względu na swoje właściwości pozostają poza regulacjami dotyczącymi przedmiotów materialnych, co było powodem zalecenia wszystkim państwom członkowskim kryminalizacji czynów polegających na „usunięciu, uszkodzeniu, uczynieniu niezdatnym do użytku lub zablokowaniu danych i programów komputerowych bez uprawnienia" przez Komitet Ministrów Rady Europy[199].

Taką funkcję ma pełnić dyspozycja § 2 omawianego artykułu dotycząca „zapisu na komputerowym nośniku informacji". Przepis ten definiuje przestępstwo materialne (skutkowe), do którego znamion należy skutek w postaci udaremnienia lub znacznego utrudnienia osobie uprawnionej zapoznania się z informacją (stawiając jednocześnie wymóg – poprzez związanie z § 1 – aby informacja ta była istotna), co świadczy, iż nacisk został w tym przypadku położony na ochronie dostępności informacji, niż na jej integralności. § 2 stanowi typ kwalifikowany przestępstwa określonego w § 1, co świadczy o uznaniu rodzaju nośnika informacji, a nie jej treści, za wyznacznik społecznej, w tym wy-

---

[196] przez niszczenie rozumie się „całkowite unicestwienie", uszkodzenie „dokonanie takiej zmiany, iż nie można zapisu wykorzystać we właściwy mu sposób", usuwanie „zabranie zapisu z miejsca, w którym się znajdował, z wyłączeniem jego uszkodzenia lub zniszczenia", zmienianie „nadanie – nawet w najmniejszym zakresie – treści odmiennej od właściwej" za : Komentarz do Kodeksu Karnego, red. Oktawia Górniok, str. 757, wyd. LexisNexis 2004;

[197] udaremnianie – „całkowita niemożność zapoznania się z zapisem"; utrudnianie – „ograniczona możliwość wykorzystania zapisu połączona ze znacznymi trudnościami w tym zakresie"; ibidem;

[198] A. Adamski – Prawo karne ..., op. cit., str. 65;

[199] ibidem

padku większej, szkodliwości czynu i co za tym idzie, o ustanowieniu przez ustawodawcę surowszej sankcji[200]. Może to budzić uzasadnione wątpliwości, zwłaszcza w erze lawinowych przemian technologicznych[201]. Chciałbym jednak zaznaczyć, iż wyższe zagrożenie karne w przypadku naruszenia integralności zapisu na komputerowym nośniku informacji nie stanowi kontrowersji – czyn taki wiąże się nierzadko z dokonaniem istotnych zmian w systemach informatycznych[202] i ze względu na skalę konsekwencji takich działań (czasem trudnych do przewidzenia nawet przez sprawcę[203] - przykładem może być „Cornell Worm" Roberta Morrisa), mających realne przełożenie na wartości pieniężne (koszty związane z usuwaniem skutków awarii, przywracania danych itp.) można mówić o znacznej szkodliwości społecznej, więc przewidziana ostrzejsza sankcja karna jest jak najbardziej na miejscu.

Kolejną nieścisłością, jaka pojawia się na gruncie omawianego przepisu jest posługiwanie się określeniem „komputerowy nośnik informacji". Pojęcie to nie zostało przez ustawodawcę zdefiniowane, nie posiada również ściśle określonego znaczenia w literaturze informatycznej, również w regulacjach prawnych można spotkać różniące się zakresem znaczeniowym definicje. Najbliższym znaczeniowo terminem jest „komputerowy nośnik danych"[204], którym w literaturze informatycznej określa się zazwyczaj nośniki magnetyczne (dyskietka, taśma[205], dysk twardy, kasetki ZIP czy JaZZ), optyczne (dyski CD-R, CD-RW, DVD i pochodne jedno- i wielokrotnego zapisu) i magnetooptyczne (dyski MO)[206]. A. Adamski, dokonując wykładni systemowej (analizując ustawę o rachunkowości, ustawę prawo bankowe i inne[207]) stwierdził, że pojęcie „komputerowy nośnik informacji", jakim posługuje się Kodeks Karny posiada stosunkowo wąski zakres, nie obejmujący np. urządzeń wyposażonych w pamięci półprzewodnikowe (np. drukarki)[208].

art. 269 § 1-2 – sabotaż komputerowy;

W raporcie Komitetu Ekspertów Rady Europy istotę sabotażu komputerowego określono jako sparaliżowanie działania lub zakłócenie funkcjonowania systemu komputerowego lub telekomunikacyjnego za pomocą „wprowadzenia, modyfikacji, wymazania lub usunięcia danych lub programów komputerowych lub innego oddziaływania na system

---

[200] udaremnienie osobie do tego uprawnionej zapoznanie się z „istotną" informacją, w wyniku wystąpienia przesłanek wymienionych w § 1 będzie zagrożone różnymi sankcjami karnymi w zależności od rodzaju nośnika, na jakim utrwalono ową informację (np. materiał filmowy na kasecie VHS i ten sam materiał na płycie VCD);
[201] A. Adamski – Prawo karne ..., op. cit., str. 67;
[202] instalacja specjalnego oprogramowania, zawirusowanie, rekonfiguracja systemu i inne – bardziej szczegółowy opis technik znajduje się w rozdziale II;
[203] np. instalacja robaka w sieci w celu wywołania określonego skutku, po nastąpieniu którego sprawca pozostawia program, który nadal wykonuje swoje funkcje;
[204] mając na uwadze różnicę pomiędzy pojęciami „informacji" i „danych";
[205] np. w streamerach;
[206] M. Molski, S. Opala – Elementarz bezpieczeństwa, op. cit., str. 138-141;
[207] patrz : A. Adamski – Prawo karne ..., op. cit., str. 67 przyp. 1;
[208] A. Adamski – Prawo karne ..., op. cit., str. 68;

komputerowy”[209]. Polski ustawodawca, jako jeden z nielicznych na świecie, wprowadził do ustawy karnej przepis przewidujący karalność sabotażu komputerowego, określając to działanie jako zakłócanie lub uniemożliwianie automatycznego gromadzenia lub przekazywania informacji o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji lub funkcjonowania administracji państwowej lub samorządowej bądź niszczenie, uszkadzanie, usuwanie lub zmiana zapisu takiej informacji na komputerowym nośniku (art. 269 § 1); § 2 tego artykułu wprowadza karalność alternatywnej postaci czynu opisanego w § 1, polegającej na niszczeniu bądź wymianie nośnika informacji lub urządzeń służących do automatycznego przetwarzania, gromadzenia lub przesyłania informacji, o których mowa w § 1.[210]

Przedmiotem ochrony tego przepisu jest integralność i dostępność gromadzonej i przekazywanej (przesyłanej)[211] elektronicznie informacji posiadającej szczególne znaczenie dla obronności kraju, bezpieczeństwa w komunikacji lub funkcjonowania administracji rządowej bądź samorządowej. Przestępstwa można dokonać godząc w zapis informacji (§ 1 – naruszenie integralności danych) lub w jej nośnik bądź urządzenie ją przetwarzające lub przekazujące (§ 2 – naruszenie integralności systemu służącego do przetwarzania danych). Przestępstwo sabotażu komputerowego (lub zakłócenia pracy systemu komputerowego[212]) możliwe jest do popełnienia za pomocą dwu podstawowych rodzajów działań – metodami fizycznymi (np. niszczenie połączeń, działanie polem magnetycznym czy podpalenie) oraz metodami logicznymi (np. ingerencja informatyczna, programy destrukcyjne, wirusy)[213].

Art. 269 § 1 typizuje przestępstwo posiadające alternatywne znamiona :

1. pierwsza grupa przesłanek popełnienia przestępstwa zawiera się w treści „kto, na komputerowym nośniku informacji, niszczy, uszkadza, usuwa lub zmienia zapis o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji lub funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej”. Opisywane przestępstwo ma charakter formalny (przestępstwo bezskutkowe – w przeciwieństwie do czynu typizowanego w art. 268 § 2[214] nie jest wymagane od sprawcy spowodowanie swoim działaniem skutku w postaci uniemożliwienia lub utrudnienia zapoznania się z informacją przez osobę uprawnioną; czyn ten

[209] *A. Adamski – Prawo karne ..., op. cit., str. 76;*
[210] *A. Adamski – Prawo karne ..., op. cit., str. 76-77;*
[211] *w treści przepisu art. 269 § 1 użyto sformułowania „przekazywanie”, natomiast § 2 tego artykułu posługuje się określeniem „przesyłania”; cybernowelizacja KK posługuje się w obu paragrafach pojęciem „przekazywanie”;*
[212] *W. Wiewiórowski – Profesjonalny haker ..., op. cit., pkt 4.8.3;*
[213] *ibidem;*
[214] *patrz opis powyżej;*

jest karalny ze względu na podjęte przez sprawcę czynności) i godzi w integralność zapisu informacji (integralność danych), przedmiotem wykonawczym natomiast jest „komputerowy nośnik informacji”[215].

2. drugą grupę stanowi określenie „zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich informacji”; przedmiotem ochrony jest dostępność informacji (będącą informacją o takim samym charakterze jak w pkt. 1), natomiast przedmiotem wykonawczym przestępstwa jest system teleinformatyczny, służący do gromadzenia i przekazywania tejże informacji (w związku z wyróżnieniem dwu rodzajów zamachów na dostępność informacji[216] można mówić o elemencie naruszenia integralności systemu służącego do przetwarzania danych).

§ 2 omawianego przepisu chroni integralność systemów komputerowych i teleinformatycznych. Przedmiotem wykonawczym czynu jest nośnik informacji bądź urządzenie służące do automatycznego przetwarzania, gromadzenia i przekazywania danych informatycznych (pojęcie wprowadzone „cybernowelizacją”). Działanie sprawcy, poprzez związanie z § 1 tego artykułu, może przybrać następujące formy :

1. niszczenie, uszkadzanie, usuwanie, zmiana danych informatycznych wskutek zniszczenia lub wymiany nośnika informacji;
2. zakłócenie lub uniemożliwienie automatycznego przetwarzania, gromadzenia i przekazywania danych informatycznych wskutek zniszczenia lub wymiany nośnika informacji;
3. niszczenie uszkadzanie, usuwanie, zmiana danych informatycznych wskutek zniszczenia lub uszkodzenia urządzenia służącego do uniemożliwienie automatycznego przetwarzania, gromadzenia i przekazywania takich danych;
4. zakłócenie lub uniemożliwienie automatycznego przetwarzania, gromadzenia i przekazywania danych informatycznych wskutek zniszczenia lub uszkodzenia urządzenia służącego do uniemożliwienie automatycznego przetwarzania, gromadzenia i przekazywania takich danych;

---

[215] *określenie to uznaje za chybione A. Adamski, formułując jednocześnie postulat de lege ferenda jego zmiany, por. A. Adamski – Prawo karne ..., op. cit., str. 68 przyp. 1; szersze dywagacje na temat tego pojęcia znajdują się w punkcie dotyczącym art. 268 KK;*

[216] *ataki destrukcyjne, powodujące zablokowanie działania systemu poprzez niszczenie lub modyfikację danych i ataki przez przeciążenie, paraliżujące działanie systemu przez wydanie mu poleceń w liczbie przekraczającej jego możliwości (ataki typu DoS lub DDoS); bardziej szczegółowy opis podstawowych technik przestępczych stanowi treść podpunktu 2.2 w rozdziale II;*

Nowelizacja KK z marca 2004 r. zmieniła brzmienie przepisu – o ile do czasu jej wejścia w życie mówiono o „zapisie informacji na komputerowym nośniku", o tyle nowelizacja wprowadziła na to miejsce określenie „danych informatycznych", którym posługuje się Konwencja (art. 1 ust. b). Ponadto na liście podmiotów, dla których chronione dane mają „szczególne znaczenie" dodano „instytucję państwową", natomiast wśród działań, jakie mogą ulec zakłóceniu lub uniemożliwieniu przez sprawcę uwzględniono „przetwarzanie danych".

Sprawcą przestępstwa określonego w art. 269 może być każdy (przestępstwo powszechne). Przepis art. 269 § 1 można uznać za kwalifikowaną odmianę czynu określonego w art. 268 § 2 ze względu na charakter chronionej informacji (lub danych informatycznych)[217].

Ustawa z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń[218] poza zmianą przepisów obowiązujących wprowadziła także kilka nowych regulacji. Celem tej ustawy było przystosowanie polskiego prawa do regulacji unijnych (w tym implementacji Konwencji o Cyberprzestępczości).

art. 268a § 1 – „sabotaż komputerowy"

Przepis ten stanowi kryminalizację czynu, polegającego na niszczeniu, uszkadzaniu, usuwaniu, zmianie lub utrudnieniu dostępu do danych informatycznych przez osobę do tego nieuprawnioną albo na zakłócaniu w istotnym stopniu lub uniemożliwianiu automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Przedmiotem ochrony jest więc dostępność danych informatycznych bądź integralność systemów służących do przetwarzania takich danych.

Podobnie jak art. 269 § 1, art. 268a § 1 typizuje czyn zabroniony posiadający alternatywne znamiona :

1. przesłanki zawierają się w treści „kto, nie będąc uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych". Przestępstwo ma charakter formalny – do jego wystąpienia wystarczające jest podjęcie przez sprawcę (przestępstwo powszechne – z wyłączeniem osób uprawnionych) wymienionych w dyspozycji działań. Przedmiotem ochrony jest dostępność danych informatycznych, natomiast przedmiotem

[217] *Komentarz do Kodeksu Karnego, red. Oktawia Górniok, str. 759, wyd. LexisNexis 2004;*
[218] *Dz. U. z 2004 r. Nr 69, poz. 626, zwana dalej „cybernowelizacją";*

wykonawczym może być nośnik tych danych lub system informatyczny, w którym są one gromadzone bądź przetwarzane.

2. alternatywnym czynem kryminalizowanym przez ten przepis jest „zakłócanie w istotnym stopniu lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych". Przestępstwo to również ma charakter formalny, jego przesłanki wypełnia podjęcie przez sprawcę wymienionych w dyspozycji działań. Przedmiotem wykonawczym (analogicznie do art. 269 § 1 w jego drugiej części) jest system służący do przetwarzania danych, natomiast przedmiot ochrony także stanowi dostępność informacji, ale – również per analogiam do art. 269 § 1 – można uznać, iż czyn przestępny typizowany w drugiej części przepisu także częściowo wypełnia znamiona zamachu godzącego w integralność systemów służących do przetwarzania danych.

§ 2 stanowi typ kwalifikowany przestępstwa typizowanego w § 1 ze względu na wyrządzenie znacznej szkody majątkowej.

Odnośnie tego artykułu, od chwili zgłoszenia go w projekcie zmiany ustawy – Kodeks Karny[219], zgłaszano różne zastrzeżenia[220]. Po pierwsze, mimo iż stanowić miał implementację art. 4 Konwencji, nie chroni bezpośrednio integralności danych, umiejscawiając środek ciężkości na zapewnieniu ich dostępności. „Z niejasnych powodów", jak pisze Adamski, przepis ukierunkowuje działania sprawcy jako atak na **dostęp** do danych informatycznych (krytycznym elementem tej konstrukcji staje się ścieżka dostępu do plików zawierających dane, a nie integralność czy też autentyczność danych zawartych w tych plikach)[221]. Ponadto, pomiędzy końcowymi fragmentami art. 268a[222] § 1 i 269a zachodzi superpozycja – art. 268a posługuje się pojęciem „w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie danych", art. 269a natomiast mówi „w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej", przy czym pojęcia te są niemal tożsame; praca „systemu komputerowego" i „sieci teleinformatycznej" (art. 269a) polega na „przetwarzaniu, gromadzeniu i

[219] *druk sejmowy nr 2031;*
[220] *ibidem;*
[221] *A. Adamski – Rządowy projekt dostosowania polskiego kodeksu karnego do Konwencji Rady Europy o cyberprzestępczości. Materiały z konferencji Secure 2003; źródło : CERT Polska, http://www.cert.pl;*
[222] *w projekcie ustawy (druk sejmowy nr 2031) był to art. 268 § 2, który miał zastąpić dotychczasowy, natomiast w trakcie prac legislacyjnych pozostawiono art. 268 w dotychczasowym brzmieniu, po nim natomiast dodano art. 268a , którym brzmienie § 1pozostawiono jak przewidziano w projekcie; A. Adamski w „Rządowym projekcie ..." posługuje się wersją z druku sejmowego nr 2031;*

przekazywaniu danych" (art. 268a § 1)[223], słuszne więc jest użycie, w stosunku do tej sytuacji, użycie pojęcia „chaos", jak również postulat jego uporządkowania[224].

Istotną dość ciekawostką, dotyczącą tego przepisu (w chwili gdy znajdował się w projekcie ustawy o zmianie ustawy – kodeks karny jako art. 268 § 2[225]) jest „Opinia o zgodności projektu ustawy o zmianie ustawy – kodeks karny z prawem Unii Europejskiej"[226] Urzędu Komitetu Integracji Europejskiej, gdzie w punkcie V czytamy „Art. 1 pkt. 7 projektowanej ustawy, dotyczący art. 268 § 2 Kodeksu karnego wdraża postanowienia art. 4 Konwencji", mimo, iż wspomniany artykuł Konwencji wyraźnie formułuje kryminalizację „umyślnego, bezprawnego niszczenia, wykasowywania, uszkadzania, dokonywania zmian lub usuwania danych informatycznych", czyli naruszenia integralności danych, którego to warunku, jak pisałem wyżej, artykuł ten nie spełnia.

art. 269a – sabotaż komputerowy

Przestępstwo określone w tym artykule popełnia ten, „kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie lub zmianę danych informatycznych w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej". Przedmiotem zamachu jest w tym przypadku niezakłócone funkcjonowanie „systemu komputerowego lub sieci teleinformatycznej" (czyli, dokonując interpretacji, systemy służące do gromadzenia i przetwarzania oraz przekazywania danych), a więc integralność systemów teleinformatycznych[227], przedmiotem wykonawczym zaś sam system (komputerowy lub teleinformatyczny). Przestępstwo ma charakter materialny, a jego skutkiem jest zakłócenie w istotnym stopniu pracy systemów komputerowych i sieci teleinformatycznych. Skutek następuje w wyniku działania sprawcy polegającym na „transmisji, niszczeniu, usuwaniu, uszkodzeniu lub zmianie danych informatycznych[228]", a więc na godzeniu w integralność danych, przy czym zamach na integralność danych jest w tym przypadku środkiem służącym do naruszenia integralności systemów teleinformatycznych i komputerowych. Przestępstwo ma charakter powszechny, z wyłączeniem osób uprawnionych do podejmowania działań wymienionych w dyspozycji. Swoistym novum jest pojawienie się w opisie strony przedmiotowej „transmisji danych", jako działania sprawcy prowadzącego do wystąpienia skutku.

---

[223] zgodnie z art. 1a Konwencji;
[224] A. Adamski – Rządowy projekt ..., op. cit., str. 6;
[225] art. 268 § 2 w projekcie ustawy i art. 268a § 1 ustawy o zmianie ustawy – kodeks karny są identycznie brzmiące;
[226] Sekr. Min. DH/2942/2003/DPE-agg, z dnia 10.09.2003; druk związany z drukiem sejmowym nr 2031, źródło : http://orka.sejm.gov.pl;
[227] znamienne jest posługiwanie się określeniem „szeroko pojęte dane informatyczne" przy opisie przedmiotu przestępstwa, przyjęte w niektórych publikacjach, por. Komentarz do Kodeksu Karnego, op. cit., str. 760, przy czym niekiedy wydaje się to niedopatrzeniem (komentarz do art. 268a § 1 – patrz opis artykułu powyżej – który posługuje się określeniem „zbiorczo określone dane informatyczne (baza danych)", co, na gruncie analizy przepisu, nie wydaje się być właściwe);
[228] wyjaśnienie pojęć stanowiących stronę przedmiotową przestępstwa zawiera opis przestępstwa z art. 268 § 2;

Przepis wprowadza karalność sabotażu komputerowego, zgodnie z art. 5 konwencji, czyli kryminalizuje naruszenie integralności systemu komputerowego.

art. 269b – kryminalizacja narzędzi "hackerskich"

Opisowi tego artykułu poświęcę nieco więcej uwagi ze względu na nowość, jaką wprowadza do Kodeksu Karnego, a także kontrowersje, jakie ta nowość ze sobą przyniosła.

Przepis ten wprowadza rozszerzenie kryminalizacji zamachów na bezpieczeństwo elektronicznie przetwarzanej informacji na stadium przygotowania przestępstwa i zgodnie z art. 6 Konwencji, wprowadza odpowiedzialność karną każdego, kto „wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 2, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej", czyli ustanawia karalność tworzenia, pozyskiwania, udostępniania lub zbywania „narzędzi", które „mogą być wykorzystane"[229] do zamachów na bezpieczeństwo danych i systemów informatycznych.[230].

Przestępstwo z art. 269b jest przestępstwem powszechnym[231] (co prawda do wypełnienia niektórych znamion wymienionych w treści wymagane są cechy indywidualne – wytworzenie urządzenia lub programu komputerowego wymaga od sprawcy posiadania umiejętności technicznych lub zdolności programowania – ponieważ jednak nie zostało to ujęte w dyspozycji przepisu, sygnalizuję jedynie istnienie tej kwestii), formalnym – do wypełnienia ustawowych znamion jego popełnienia wystarczające jest określone przepisem zachowanie sprawcy.

Zachowanie się sprawcy może polegać na wytwarzaniu, pozyskiwaniu, zbywaniu lub udostępnianiu (niezależnie od podmiotu, na którego rzecz odbywa się to działanie, jak również nie odgrywa żadnej roli cel, w jakim działanie to jest podejmowane[232]) przedmiotów czynu, określonych w pierwszej (urządzenia lub programy komputerowe) lub drugiej części przepisu (hasła komputerowe, kody dostępu lub inne dane). Strona podmiotowa obejmuje zarówno zamiar bezpośredni jak i ewentualny. Pominięto, na co zezwala art.

---

[229] zwrot „przystosowane do" w tekście przepisu nie wprowadza zakazu w stosunku do „narzędzi służących do", przewiduje natomiast możliwość popełnienia przy pomocy takiego narzędzia przestępstwa zagrożonego karą z jednego z wymienionych w tekście artykułów; jest to określenie dość nieostre i – choć będzie to daleka analogia – młotek, służący do wbijania gwoździ „jest przystosowany" do np. „spowodowania ciężkiego uszczerbku na zdrowiu";

[230] art. 6 Konwencji (w skrócie) wprowadza kryminalizację wytwarzania i zbywania narzędzi służących do popełnienia przestępstw wymienionych w art. 2- 5 Konwencji;

[231] biorąc pod uwagę znamiona przestępstwa wymienione w drugiej części omawianego przepisu formalny charakter wydaje się być chybiony z powodu braku zastrzeżenia uprawnień określonej grupy osób, o czym poniżej;

[232] w tym miejscu tkwi poważna skaza niniejszego przepisu, o czym poniżej;

6 pkt. 3 Konwencji, z kryminalizacji posiadania z zamiarem popełnienia przestępstwa urządzeń, programów i danych, o których wzmiankuje art. 269b.

§ 2 przewiduje obligatoryjne orzeczenie przepadku **przedmiotów** wymienionych w § 1, natomiast gdy nie stanowiły one własności sprawcy może przepadek orzec. Użycie zwrotu „przedmiot" w stosunku do urządzenia, wymienionego w § 1 nie budzi wątpliwości, które rodzą się w momencie odniesienia do programów komputerowych, a tym bardziej haseł komputerowych, kodów dostępu i osiągają kulminację, gdy docieramy do „innych danych". Mając w pamięci stwierdzenie Norberta Wienera, że „informacja jest informacją, a nie materią i nie energią", a także definicję informacji zawartą w Zaleceniu Rady OECD z dnia 26.11.1992 r. mówiącą, iż informacja „to znaczenie, jakie nadajemy danym przy pomocy konwencji odnoszących się do tych danych", można zaryzykować stwierdzenie, że otwiera się szerokie pole do dyskusji na temat interpretacji, co do której nie ma pewności, że zaowocuje skutkiem.

Ogólnie redakcji tego przepisu można wytknąć wiele potknięć, takich jak np. :

1. przynajmniej w drugiej części przepisu (chociaż z powodzeniem można ten zarzut odnieść również do części pierwszej) zabrakło stwierdzenia „kto, nie będąc do tego uprawnionym", a uprawnienia takie, choćby z racji pełnionej funkcji, powinni mieć administratorzy sieci w celu udostępnienia haseł osobom uprawnionym do dostępu lub wytwarzania programów do testowania zabezpieczeń ochranianej przez siebie sieci teleinformatycznej; generalny zakaz, zawarty w tym przepisie, poprzez braku uwzględnienia w nim kontratypu, jest „obosiecznym mieczem"; warto zaznaczyć, że Konwencja w art. 6 ust. 2 przewiduje tworzenie takiego kontratypu, a dokładniej stwierdza, iż nie należy interpretować artykułu w taki sposób, który mógłby stanowić o odpowiedzialności karnej osoby, który wypełniając wymienione znamiona czynu nie ma na celu popełnienia przestępstwa, lecz uprawnione testowanie lub ochronę systemu informatycznego.
2. kolejne zastrzeżenie łączy się z poprzednim, a raczej jest jego punktem wyjścia; koncepcja kryminalizacji „narzędzi hackerskich" jest uznawana za kontrowersyjną[233] głównie z powodu przyjęcia szerokiego zakresu „przedmiotów" objętych karalnością. Tak zwane „narzędzia hackerskie" to na ogół programy ogólnego (lub podwójnego) przeznaczenia, a przynajmniej posiadające na tyle rozbudowany katalog funkcji, iż trudno jednoznacznie zali-

[233] *A. Adamski – Rządowy projekt ..., op. cit., str. 7;*

czyć je do kategorii ściśle „hackerskiej[234]" lub, patrząc z drugiej strony, programy te mogą być wykorzystywane przez obie strony konfliktu administrator - przestępca[235], a na gruncie polskiej ustawy karnej wzbogaconej o ten przepis przewagę zdobywają ci ostatni, gdyż mając zamiar popełnienia przestępstwa np. z artykułów wymienionych w tym przepisie trudno sądzić, aby sankcja karna za wytwarzanie urządzeń mogących im to umożliwić powstrzymała ich od dokonania czynu, natomiast administratorom sieci wytrąca bardzo skuteczną broń z ręki;

3. przepis ogranicza zakres kryminalizacji czynności sprawcy do „narzędzi" przystosowanych do popełnienia ściśle wyliczonych w treści przestępstw, pomijając w tym wyliczeniu przestępstwo kryminalizowane w art. 267 § 1, dotyczące „nieuprawnionego zapoznania się z informacją w wyniku przełamania zabezpieczeń", czyli czynu określanego dotychczas „hackingiem"[236]

Na zakończenie dodam, że powyższe nieuwzględnienie art. 267 § 1 w liście przestępstw, do popełnienia których mogą służyć „narzędzia" wymienione w art. 269b jest elementem, który nie pozwala mówić o pełnej implementacji art. 6 Konwencji do polskiego porządku prawnego (art. 6 mówi o „narzędziach" służących[237] do popełnienia przestępstw z art. 2 – 5 Konwencji, której art. 2 nazywa się „nielegalny dostęp"). Można dywagować, czy w przypadku pozostawienia przepisu art. 267 § 1 KK w obecnym brzmieniu (nie obejmującym zakresem karalności przestępstwa konwencyjnego z art. 2) konieczne jest objęcie kryminalizacją wytwarzanie narzędzi służących do popełnienia przestępstwa z tego artykułu.

5.3 Przestępstwa komputerowe sensu largo w Kodeksie Karnym;

Poza rozdziałem XXXIII KK, w którym zawarto przepisy kryminalizujące tzw. „przestępstwa komputerowe" *sensu stricte* (czyli przestępstwa przeciwko ochronie informacji), w Kodeksie Karnym znalazły się także uregulowania, które, ze względu na sposób, w jaki zdefiniował je ustawodawca, można zaliczyć do grupy „przestępstw komputerowych". Pomimo funkcji ochronnej dotyczącej innych dóbr niż informacja, z treści tych przepisów dosłownie wynika, iż czyny przez nie penalizowane mogą zostać popełnione

[234] istnieje grupa programów, wykorzystywanych do ataków typu DoS czy DDoS, o których śmiało można powiedzieć, iż służą jedynie do wywołania efektu w postaci dysfunkcji systemu;
[235] słynne skanery portów takie jak NetBus czy Prosiak mogą służyć jednocześnie do skanowania wolnych portów w celu wykorzystania ich do włamania do systemu jak i wykrycia tych portów przez osobę odpowiedzialną za bezpieczeństwo systemu w celu ich zblokowania; sztandarowym jednak przykładem takiego programu jest kultowy już w chwili obecnej SATAN autorstwa Dana Farmera;
[236] przepis ten, pomimo wielokrotnego wytykania jego wad, nie doczekał się, pomimo potrzeby wynikającej z art. 2 Konwencji, nowelizacji;;

przy użyciu komputera, ich wspólną cechą jest więc odwoływanie się ich znamion do szeroko pojętej techniki komputerowej – są one „przestępstwami komputerowymi" ze względu na określony w ustawie sposób działania sprawcy, a nie ze względu na przedmiot zamachu[238].

W niniejszym podrozdziale pokrótce omówię wybrane przestępstwa z tej grupy w ich brzmieniu nadanym nowelą z 18 marca 2004 r.[239].

„Przestępstwa komputerowe" przeciw wiarygodności dokumentów zawarte w rozdziale XXXIV;

Wprowadzenie do Kodeksu Karnego przepisów realizujących zalecenie kryminalizacji fałszerstw komputerowych, zawartych w Rekomendacji Nr R(89)9[240], było możliwe dzięki zmianie prawnej definicji dokumentu, co nastąpiło w części ogólnej Kodeksu poprzez nadanie art. 115 § 14 brzmienia „dokumentem jest każdy przedmiot lub zapis na komputerowym nośniku informacji ...". Rozwiązanie to pozwoliło znacznie rozszerzyć katalog „przestępstw komputerowych" w polskim prawie karnym. Nowela do Kodeksu Karnego z 18 marca 2004 roku zmieniła brzmienie przepisu, którego treść brzmi obecnie „dokumentem jest każdy przedmiot lub inny zapisany nośnik informacji ..."[241].

art. 270 § 1 – fałszerstwo komputerowe

Przepis kryminalizuje zachowanie polegające na podrabianiu lub przerabianiu – w celu użycia za autentyczny – dokumentu lub używaniu takiego dokumentu jako autentycznego. Dyspozycję przepisu narusza każda ingerencja (podrobienie lub przerobienie) w treść dokumentu, dokonana w zamiarze bezpośrednim (w przypadku podrabiania lub przerabiania – w przypadku „używania jako autentycznego" w grę może również wchodzić *dolus eventualis*). Przedmiotem czynu jest dokument, przestępstwo ma charakter powszechny.

art. 276 – niszczenie lub ukrycie dokumentu

Czynem zabronionym przez ten artykuł jest „niszczenie, uszkadzanie, czynienie bezużytecznym, ukrywanie lub usuwanie dokumentu, którym sprawca nie ma prawa wyłącznie rozporządzać". W odniesieniu do dokumentu elektronicznego „niszczenie, uszka-

---

[237] posługuję się tutaj skrótem – listę tych narzędzi przedstawiłem wcześniej, podobnie jak ich charakter;
[238] A. Adamski – prawo karne ..., op. cit., str. 32;
[239] zmiany będą głównie dotyczyć interpretacji przepisu w związku z przyjęciem nowej definicji dokumentu;
[240] patrz Rozdział IV;
*[241] w projekcie nowelizacji zapis ten brzmiał „dokumentem jest każdy przedmiot, **w tym** zapisany nośnik informacji ..." i był tematem wielu negatywnych opinii, por. M. Płachta – Opinia w sprawie projektu ustawy o zmianie Kodeksu karnego, Kodeksu postępowania karnego oraz kodeksu wykroczeń (druk 2031), opinia zlecona, Biuro Ekspertyz i Analiz, Gdańsk 12.01.2004, w trakcie prac legislacyjnych nad projektem Senat RP zgłosił poprawkę do rzeczonego przepisu nadając mu obecne brzmienie (druk nr 2595 z dnia 4 marca 2004 r.), jednakże wciąż treść przepisu jest obiektem krytyki, por. A. Adamski – Rządowy projekt ..., op. cit., str. 3-4;*

dzanie, usuwanie" może być podjęte do nośnika, na którym ten dokument się znajduje. Biorąc pod uwagę łatwość reprodukcji dokumentu elektronicznego, całkowite jego zniszczenie może się okazać niemożliwe, np. w przypadku istnienia nieznanej lub wielkiej liczby kopii. Ponadto łatwość reprodukcji i modyfikacji (w stosunku do dokumentów tradycyjnych) staje się poważnym zagrożeniem w przypadku dokumentów, w stosunku do których obowiązują zwiększone rygory autentyczności – np. dokumenty będące dowodami w postępowaniu sądowym. Pozbawienie takiego dokumentu mocy dowodowej może polegać na pozbawieniu lub nienadaniu takiemu dokumentowi podpisu cyfrowego, jak też na nieautoryzowanej zmianie treści[242].

„Przestępstwa komputerowe" przeciwko mieniu zawarte w rozdziale XXXV KK;

Przedmiotem ochrony przepisów tego rozdziału jest mienie, rozumiane w interpretacji cywilistycznej jako „ własność i inne prawa majątkowe". Przedmiotem praw majątkowych mogą być dobra niematerialne, istniejące niezależnie od rzeczy, które mogą być nośnikami tych dóbr, służyć ich utrwaleniu lub korzystaniu z nich.

W rozdziale XXXV KK znajdują się cztery podstawowe typy przestępstw związanych z automatycznym przetwarzaniem informacji : nielegalne uzyskanie programu komputerowego (art. 278 § 2), paserstwo programu komputerowego (art. 293 § 1), a także dwa przestępstwa, które zostaną pokrótce przedstawione poniżej ze względu na fakt, iż nie miały odpowiednika w ustawie karnej z 1969 roku, czyli oszustwo telekomunikacyjne (art.. 285) i oszustwo komputerowe (art. 287).

art. 285 § 1– oszustwo telekomunikacyjne;

Odpowiedzialności karnej na mocy przepisu art. 285 § 1 podlega ten, kto „włączając się do urządzenia telekomunikacyjnego uruchamia na cudzy rachunek impulsy telefoniczne". Przez „włączenie się do urządzenia telekomunikacyjnego" należy rozumieć każdą ingerencję w integralność systemu telekomunikacyjnego, polegającą na uzyskaniu dostępu do funkcji realizowanych przez urządzenia składające się na ten system, przy jednoczesnej interpretacji „systemu telekomunikacyjnego" jako „zespołu urządzeń telekomunikacyjnych i zasad ich działania"[243].

Przestępstwo ma charakter powszechny i formalny – dokonanie następuje z chwilą podłączenia się przez sprawcę do urządzenia telekomunikacyjnego i uruchomienia

[242] *A. Adamski – Prawo karne ..., op. cit., str. 88-89;*
[243] *A. Adamski – Prawo karne ..., op. cit., str. 124;*

impulsów telefonicznych na cudzy rachunek. Czyn typizowany w art. 285 § 1 może zostać popełniony w obu formach zamiaru.

Zauważa się, że konstrukcja przepisu może być powodem jego szybkiego zdezaktualizowania, będącego konsekwencją użycia przez ustawodawcę ostrego znaczeniowo zwrotu „uruchamia na cudzy rachunek impulsy telefoniczne" i postępu technicznego. Pojęcie „impuls telefoniczny", którym posługuje się przepis, jest związane jest z techniką analogową, którą zastępuje się obecnie techniką cyfrową – pojęcie to traci zastosowanie w przypadku cyfrowych systemów telekomunikacyjnych, których działanie nie opiera się na zjawisku generowania impulsów elektrycznych zamienianych na sygnały dźwiękowe.

art. 287 – oszustwo komputerowe;

Oszustwa komputerowego może dopuścić się każdy (przestępstwo powszechne) – z oczywistym wyłączeniem, zawartym w treści przepisu, osób upoważnionych - kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia szkody innej osobie bez upoważnienia wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych[244]. Jest to przestępstwo formalne, umyślne, ukierunkowane na osiągnięcie określonego celu. Od tradycyjnego oszustwa czyn ten różni się przedmiotem wykonawczym – sprawca bezpośrednio oddziaływuje nie na ludzką psychikę, a na dane informatyczne i technologię służącą do ich przetwarzania.

Istotą przestępstwa określonego tym przepisem jest usiłowanie osiągnięcia korzyści majątkowej lub spowodowania szkody, co, wskutek stworzenia typu przestępstwa bezskutkowego, niewątpliwie upraszcza postępowanie dowodowe w procesie karnym. Przestępstwo uważa się za dokonane „w momencie wpłynięcia na automatyczne przetwarzanie danych, wprowadzenia nowego zapisu, tj. zanim nastąpiło powstanie zamierzonej szkody"[245].

Działanie sprawcy polegające na „wpływaniu" sprawcy na automatyczne przetwarzanie, gromadzenie, przekazywanie danych informatycznych należy interpretować jako ingerencję sprawcy w funkcjonowanie systemów przetwarzających dane, czyli naruszenie integralności tych systemów, natomiast „zmiana, usunięcie lub wprowadzenie nowego zapisu" jest działaniem godzącym zarówno w integralność jak i dostępność danych informatycznych.

---

[244] brzmienie nadane „cybernowelizacją"; dotychczas „wpływanie" dotyczyło informacji, a „wprowadzanie nowego zapisu" komputerowego nośnika informacji;

[245] K. Buchała – Reforma polskiego prawa karnego materialnego. Przestępstwa przeciwko ochronie informacji i oszustwo komputerowe, [w:] A. Adamski (red.) – Prawne aspekty ..., op. cit., str. 136-137;

W czasie, gdy rzeczony przepis powstawał, pojęcie oszustwa komputerowego oznaczało wykorzystywanie zaawansowanej technologii do dokonywania nadużyć finansowych, mogących mieścić się w trzech kategoriach :

- manipulacje komputerowe dokonywane „na wejściu" do komputera (manipulacja danymi wprowadzanymi do komputera, „input manipulation"); najczęściej sprawca działa z wnętrza sieci, w której dokonuje manipulacji (jest uprawnionym użytkownikiem); przykładem może być sprawa zastępcy dyrektora I oddziału ZUS-u w Warszawie, który wykorzystując instytucję „martwych dusz" uzyskiwał znaczne korzyści majątkowe[246];
- manipulowanie programem komputerowym („program manipulation") polega na odpowiedniej modyfikacji programu komputerowego, który w wyniku modyfikacji, polegającej na wyposażeniu go w dodatkowe funkcje, może wykonywać dodatkowe operacje, służące do dodkonywania nadużyć;
- manipulacja rezultatami przetwarzania danych (manipulacja „na wyjściu", „output manipulation") może polegać np. na wystawianiu podwójnych rachunków przy pomocy komputera;

„Przestępstwa komputerowe" przeciwko Rzeczypospolitej Polskiej zawarte w Rozdziale XVII KK;

art. 130 § 3 – szpiegostwo komputerowe;

Art. 130 KK kryminalizuje przestępstwo szpiegostwa, którego formę uprzywilejowaną przewiduje § 3. Jedną z czynności wykonawczych tego przestępstwa jest „wejście do systemu informatycznego w celu uzyskania wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej"[247].

Przedmiotem wykonawczym szpiegostwa są informacje, których przekazanie obcemu wywiadowi mogą wyrządzić szkodę RP. Indywidualnym przedmiotem ochrony są natomiast podstawy ustroju i suwerennego bytu Rzeczypospolitej Polskiej, określone w Konstytucji. Przy tak rozumianym przedmiocie ochrony nie można utożsamiać przepisu art. 130 ze szpiegostwem przemysłowym (w jego odmianie komputerowej), chociaż takie ujęcie szpiegostwa komputerowego znalazło się na „liście fakultatywnej" Zalecenia Nr

---

[246] J. Liszewski – Oszustwa popełniane z wykorzystaniem komputera w Polsce (dwa studia przypadków), [w:] A. Adamski (red.) – Prawne aspekty ..., op. cit., str. 54-56;

[247] tekst § 3 uległ zmianie w wyniku „cybernowelizacji"; poprzednia redakcja przepisu określała tą czynność wykonawczą jako „włączenie się do sieci komputerowej";

(89)9 Komitetu Ekspertów Rady Europy i zaistniało w ustawodawstwie karnym kilku krajów europejskich[248].

Uzyskanie wiadomości, o których mowa w § 2 nie jest warunkiem *sine qua non* postawienia sprawcy zarzutu z § 3 – przesłanką karalności staje się wejście do systemu informatycznego w celu ich uzyskania.

Określenie „wejście" zastąpiło używane przed nowelizacją „włączenie się", przy czym oba te pojęcia są tożsame w znaczeniu szerokości zakresu na gruncie omawianego przepisu, albowiem nie precyzują metody działania sprawcy, tylko desygnują stan faktyczny do którego działanie sprawcy prowadzi. Sprawca więc ponosi odpowiedzialność karną zarówno w przypadku złamania lub obejścia zabezpieczeń, wykorzystania hasła zdobytego podstępem, z wykorzystaniem lekkomyślności lub nieuwagi osoby uprawnionej[249]. Sprawcą „wejścia" do systemu może być zarówno „outsider", działający z zewnątrz sieci, jak i użytkownik działający wewnątrz niej, przekraczający swoje uprawnienia – praktycznie kwalifikacja obu tych przypadków jest identyczna, gdyż zarówno intruz z zewnątrz, jak i osoba działająca z „wnętrza", w wyniku podjętych czynności, znajdują się na terytorium, które powinno być dla nich niedostępne[250].

„Przestępstwa komputerowe" przeciwko bezpieczeństwu powszechnemu w Rozdziale XX KK;

art. 165 – sprowadzenie stanu powszechnego niebezpieczeństwa;

Art. 165 obejmuje zakresem karalności (§ 1 pkt 4) zachowanie, polegające na sprowadzeniu niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach na skutek zakłócania, uniemożliwiania lub wpływania w inny sposób na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych[251].

Czyn określony w art. 165 KK jest przestępstwem materialnym – jego dokonanie następuje wraz ze skutkiem, którym jest wywołanie przez sprawcę stanu konkretnego zagrożenia o charakterze powszechnym, czyli dotyczącym życia lub zdrowia większej (bliżej nieokreślonej) liczby osób lub mienia wielkiej wartości. Przez stan zagrożenia nale-

[248] *A. Adamski – Prawo karne ..., op. cit., str. 131;*
[249] *Ciekawym wydaje się fakt uwzględnienia tych przypadków w omawianym artykule i pominięcia ich w redakcji art. 267 § 1 KK;*
[250] *szerzej o tej problematyce w rozdziale VI poświęconym „hackingowi";*
[251] *przepis sprzed „cybernowelizacji" posługiwał się określeniem „informacja";*

ży rozumieć narastające w czasie niebezpieczeństwo, któremu w trakcie tego procesu można zapobiegać[252].

Indywidualnym przedmiotem ochrony przepisu jest bezpieczeństwo powszechne – do naruszenia tego dobra dochodzi wraz z wywołaniem niebezpieczeństwa (charakteryzującego się wyżej wymienionymi cechami), sprowadzonego poprzez oddziaływanie na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych może dotyczyć systemów teleinformatycznych wykonujących różnorakie zadanie, niekoniecznie związane z zapewnieniem bezpieczeństwa życia, zdrowia lub mienia obywateli[253] - np. system sterujący pracą elektrowni nuklearnej.

5.4 Porównanie polskich przepisów dotyczących przestępczości komputerowej sensu stricte z rozwiązaniami przyjętymi w Konwencji Rady Europy o Cyberprzestępczości

Jak już wspominałem poprzednio, polski ustawodawca, wprowadzając do treści Kodeksu Karnego rozdział XXXIII „Przestępstwa przeciwko ochronie informacji" uczynił pierwszy krok w kierunku kryminalizacji zachowań godzących w bezpieczeństwo zdigitalizowanych danych. Poniżej postaram się pokrótce przedstawić, jak rozwiązania krajowe realizują postulaty bądź zalecenia Rady Europy. Zakresem treści tego rozdziału obejmę przepisy umiejscowione w rozdziale XXXIII Kodeksu Karnego, skupiając się głównie na analizie spełnienia przez nie postanowień Konwencji o Cyberprzestępczości, jako najświeższego aktu Rady Europy.

Normalizacja przepisów regulujących materię przestępstw popełnianych z zastosowaniem zawansowanych technologii zarówno wśród państw członkowskich Wspólnoty jak i krajów pozostających poza strukturami, była warunkiem niezbędnym wprowadzenia realnej karalności sprawców tych czynów.

Mając na uwadze, że Konwencja Budapeszteńska jest obecnie podstawowym aktem normatywnym służącym do walki z cyberprzestępczością, a także czekającą Rzeczpospolitą jej ratyfikację, chciałbym przedstawić, w jakim stopniu polskie przepisy prawnokarne realizują zawarte w niej wytyczne. Odniosę się tutaj do artykułów 3 – 6 Konwencji, zawartych w tytule I rozdziału II, czyli dotyczących przestępstw „przeciwko pouf-

[252] *A. Adamski – Prawo karne ..., op. cit., str. 135;*
[253] *A. Adamski – Prawo karne ..., op. cit., str. 135;*

ności, integralności i dostępności danych informatycznych i systemów". Celowo pomijam art. 2 Konwencji, którego relacje z art. 267 § 1 omówiłem w poprzednim rozdziale.

Można śmiało stwierdzić, że jedynym w pełni zaimplementowanym do krajowego porządku prawnego przepisem Konwencji jest art. 5, odzwierciedlony w Kodeksie Karnym w art. 269a, dotyczącym naruszenia integralności systemu, a wprowadzonym ustawą z 18 marca 2004 r. Nie ujmując nic polskiemu ustawodawcy, można uznać, iż jest to spowodowane niemal dosłownym powtórzeniem redakcji analogicznego przepisu Konwencji.

Również nakaz kryminalizacji nielegalnego przechwytywania danych (art. 3 Konwencji) doczekał się rozsądnego rozwiązania w postaci przepisu § 2 art. 267 KK (określanym jako przepis kryminalizujący podsłuch komputerowy[254]). Przepis ten, nie będąc nowelizowany od wejścia w życie Kodeksu Karnego z 1997 r., niemal całkowicie spełnia wymogi konwencyjnego ujęcia tego przestępstwa. Materią nieuregulowaną przez powyższy przepis jest, zgłoszony przez Zgromadzenie Parlamentarne Rady Europy wymóg zawarcia w regulacjach prawnych regulacji dotyczących uprawnień pracodawcy do monitorowania przepływu informacji osób zatrudnionych w miejscu pracy. Wymóg ten został zawarty w Opinii Zgromadzenia Parlamentarnego Rady Europy Nr 226 z dnia 24 kwietnia 2004 r., nie mógł więc zostać uwzględniony w treści „Cybernowelizacji" KK.

Implementacja art. 4 Konwencji, dotyczącego naruszenia integralności danych, jest już bardziej problematyczna. Do chwili wejścia w życie „Cybernowelizacji" Kodeksu Karnego za przepis kryminalizujący ten czyn uchodził art. 268 § 2, któremu jednak można było zarzucić (na tle ujęcia omawianego przestępstwa przez Konwencję), iż chronił nie tyle integralność danych, co dostęp do nich przez osobę do tego uprawnioną, tak więc działanie sprawcy, wypełniające znamiona czynu typizowanego w przepisie, o ile nie skutkowały „udaremnieniem lub znacznym utrudnieniem" zapoznania się z informacja, nie podlegały karalności na podstawie tego artykułu. Drugą kwestią było wprowadzenie wymogu „istotności" informacji, do której dostęp miał być utrudniony lub udaremniony, znacznie zawężający możliwość stosowania przepisu. Ustawą z dnia 18 marca 2004 r. do Kodeksu Karnego wprowadzono art. 268a, którego § 1 miał w założeniu implementować postanowienie art. 4 Konwencji, czego jednak w sposób zadowalający nie czyni, kładąc nacisk na ochronę dostępu do rzeczonych danych, a nie ich *stricte* integralność, w związku z czym nie można mówić o pełnym wdrożeniu postanowień Konwencji w tej materii przez polskiego ustawodawcę. Swoistą ciekawostką jest fakt, iż redakcja art. 269 KK, z pominięciem zawartego w jego treści wymogu „szczególnego znaczenia" danych, w pełni postanowienia Konwencji spełnia.

[254] *A. Adamski – Prawo karne ..., op. cit., str. 55;*

Przepisem, którego redakcji można wytknąć najwięcej potknięć, jest art. 269b KK, mającego wdrażać art. 6 Konwencji, mówiący o „niewłaściwym użyciu urządzeń". Zarzuty te dotyczą przede wszystkim ujęcia problematyki przez ustawodawcę. Przepisowi tego artykułu, jako mającego spełnić wymogi postanowień Konwencji, można postawić dwa główne zarzuty :

1. nieuwzględnienie przepisu art. 267 § 1 KK na liście przestępstw, do popełnienia których miałyby być przystosowane programy komputerowe i urządzenia, których „wytwarzanie, zbywanie, pozyskiwanie lub udostępnianie" jest na mocy tego przepisu karalne. Zarzut niniejszy nie jest kategoryczny – wspomniałem przy omawianiu art. 269b, iż art. 6 Konwencji wprowadza karalność wytwarzania narzędzi, przystosowanych bądź przeznaczonych do popełnienia przestępstw z art. 2 – 5 Konwencji, przy czym art. 267 § 1 KK w żadnym stopniu nie spełnia wymogów art. 2 (o czym poniżej), więc uwzględnienie przestępstwa z tego artykułu, jako nie mieszczącego się w ramach przestępstw konwencyjnych, w redakcji art. 269b można uznać za uzasadnione. Z drugiej strony problemem staje się ciągłe postrzeganie art. 267 § 1 KK jako przepisu kryminalizującego „hacking", o którym mówi art. 2 Konwencji.
2. pominięcie wskazanego przez europejskiego ustawodawcę wyłączenia stosowania karalności na podstawie zawartego w ust. 2 tego artykułu, stwierdzającego, że przepisu niniejszego artykułu nie należy stosować, jeśli działanie, określone w ust. 1, nie jest dokonywane w celu popełnienia przestępstwa, wymienionego w art. 2 – 5, tak jak w przypadku dozwolonego testowania lub ochrony systemu informatycznego.

Art. 2 Konwencji, kryminalizujący czyn polegający na uzyskaniu nielegalnego dostępu do systemu informatycznego, nie posiada odpowiednika na gruncie polskiej ustawy karnej[255].

Podsumowując, nie można mówić o pełnej implementacji postanowień Konwencji o Cyberprzestępczości do polskiego porządku prawa karnego. Uwzględnienia nie doczekał się art. 2, natomiast regulacje art. 4 i 6 zostały przez polskiego ustawodawcę wprowadzone do Kodeksu Karnego w sposób nie odpowiadający całkowicie zamysłom europejskiego legislatora.

---

[255] omówienie art. 267 § 1 jako przepisu mającego realizować postanowienia art. 2 Konwencji znajduje się w rozdziale poświęconym przestępstwu „hackingu";

6. Rozdział VI – Nieuprawnione uzyskanie informacji („hacking”) w ujęciu art. 267 § 1 Kodeksu Karnego z 1997 r.

Nawiązując do niejasności terminologicznych chciałbym zauważyć, iż wielu autorów, nawet po dość dogłębnym rozważeniu kwestii terminologii popełnia błąd, używając pojęcia „hacker” mimo, iż z wcześniejszych rozważań wynika (poza kwestią, iż nie ma w Kodeksie Karnym przestępstwa „hackingu”), że „hacking” to „nieuprawniony dostęp do systemu komputerowego” – w dalszych rozważaniach następuje ocena art. 267 § 1 jako przepisu penalizującego ten czyn, nie powinna więc nikogo dziwić powszechnie negatywna ocena jako że przepis ten ochrania przed całkowicie odmiennym zagrożeniem.

Główną kontrowersją dotyczącą przestępstwa „hackingu” jest pytanie, w jakim stopniu kryminalizować zjawisko uzyskania dostępu do systemu komputerowego i danych w nim przechowywanych przez osobę nieuprawnioną – czyli jakie dobro prawne chronić i przed jakimi zamachami na nie, stanowi to bowiem punkt wyjścia prac legislacyjnych.

6.1 Wprowadzenie;

Podstawową zmianą, jaka zaszła po wejściu w życie Kodeksu Karnego z 1997 r. w stosunku do analogicznego przepisu Kodeksu Karnego z 1969 r.[256] jest zmiana dobra, podlegającego na mocy tego przepisu ochronie. Dobrem prawnie chronionym w art. 172 sKK była tajemnica korespondencji, natomiast w art. 267 KK z 1997 r. środek ciężkości został przesunięty w stronę ochrony informacji, głównie w aspekcie jej poufności, w związku z czym można twierdzić, że przepis art. 267 w całości chroni poufność informacji – z tym, że § 1 zakresem ochrony obejmuje informację przechowywaną na nośniku, warunkując popełnienie przestępstwa od przełamania zabezpieczeń[257].

6.2 Charakterystyka przepisu;

„Art. 267 § 1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie

[256] *Ustawa z dnia 19 kwietnia 1969 r. – Kodeks Karny (Dz. U. z 1969 r. Nr 13 poz. 94 z późn. zm.) dalej jako sKK;*
[257] *patrz opis czynu z art. 267 § 2;*

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2."

Przepis powyższy jest dostosowaną, poprzez użycie nowej terminologii, do współczesnych realiów wersją art. 172 sKK, który chronił tajemnicę korespondencji. Rozwiązanie przyjęte w Kodeksie Karnym z 1997 r. zapewnia jednak słabszą ochronę poufności informacji, niż czynił to jego poprzednik, albowiem stanowi, że naruszenie poufności informacji (będącą dobrem prawnie chronionym przez ten przepis) ma miejsce w chwili uzyskania przez sprawcę „informacji dla niego nie przeznaczonej", gdzie przyjmuje się że pojęcie „uzyskanie informacji" oznacza zapoznanie się z jej treścią[258] (autor przyjmuje tą interpretację jako punkt wyjścia do dalszych rozważań, natomiast kwestia sporów doktrynalnych zostanie omówiona w dalszej części niniejszego rozdziału), co pod rządami ustawy karnej z 1969 r. nie było warunkiem *sine qua non* popełnienia przestępstwa z art. 172, o czym zadecydował wzgląd czysto pragmatyczny na możliwość udowodnienia sprawcy popełnienia czynu naruszenia tajemnicy korespondencji. W związku z powyższym działanie sprawcy („otwarcie zamkniętego pisma", „podłączenie się do przewodu służącego do przekazywania informacji", „ przełamanie elektronicznych, magnetycznych albo innych szczególnych zabezpieczeń") nie stanowi kryterium naruszenia poufności informacji, lecz charakteryzują metodę, jaką posłużył się sprawca w celu uzyskania informacji, do której nie był uprawniony. W konsekwencji sprawcy należy udowodnić, że „zamknięte pismo" otworzył i przeczytał bez zgody osoby do tego uprawnionej, podczas gdy do czasu wejścia w życie Kodeksu Karnego z 1997 r. przedmiotem dowodu był sam fakt otwarcia takiego pisma.

Kwestia położenia nacisku na konieczność „uzyskania" przez sprawcę informacji dla niego zastrzeżonej w treści przepisu art. 267 § 1 KK niewątpliwie osłabia jego funkcję, natomiast przyjęcie takiej wykładni pojęcia „uzyskuje", jaką prezentuje autor niniejszej pracy praktycznie tworzy martwy przepis. Co do zwrotu „uzyskuje" istnieje niezgodność poglądów w doktrynie – wg innego rozumienia pojęcia przesłanka „uzyskania" jest spełniona w chwili przejęcia przez sprawcę fizycznego władztwa nad „nośnikiem zapisu informacji" bądź skopiowania zapisu informacji i do realizacji znamion przestępstwa nie jest konieczne zapoznanie się przez sprawcę z treścią informacji, co więcej – nie jest konieczne, by sprawca miał realną możliwość zrozumienia treści informacji[259]. Taka wykładnia

---

[258] *S. Glaser i A. Mogilnicki interpretując przestępstwo naruszenia korespondencji na gruncie art. 253 § 1 KK z 1932 r. stwierdzają, że przez podstepne „uzyskanie" wiadomości telefonicznej lub telegraficznej rozumie się „zapoznanie się z treścią danej wiadomości", cyt. za Glaser i Mogilnicki – Kodeks Karny. Komentarz, Kraków 1934, str. 831 [w:] A. Adamski – Prawo karne ..., op. cit., str. 46;*

[259] *W. Wróbel – Komentarz do art. 267 kodeksu karnego* [w:] *A. Zoll (red.), G. Bogdan, K. Buchała, Z. Ćwiąkalski, M. Dąbrowska-Kardas, P. Kardas, J. Majewski, M. Rodzynkiewicz, M. Szewczyk, W. Wróbel – Kodeks karny. Część szczególna. Komentarz do art. 177-277. Tom II, Zakamycze 1999;*

przepisu, choć niewątpliwie będąca bardziej utylitarna z punktu widzenia postępowania karnoprocesowego[260], nie wydaje mi się właściwa z kilku powodów.

Przede wszystkim po raz kolejny podniosę kwestię rozróżnienia pojęć „informacji" i „danych" – w skrócie dane to substrat procesu interpretacji, którego wynikiem jest informacja. Jednocześnie trzeba mieć na uwadze, że te same dane, w zależności od konwencji ich dotyczących i towarzyszących okoliczności mogą być różnorako interpretowane, a co może skutkować uzyskaniem różnych informacji. Kwestią posiadającą jednak największe znaczenie jest brak możliwości stosowania tych pojęć zamiennie – dane na przykład można, w przeciwieństwie do informacji, zniszczyć lub ukraść, nie można natomiast, w przypadku ich cyfrowego magazynowania, się z nimi zapoznać[261]. Omawiany tekst nie posługuje się co prawda pojęciem „danych" a „zapisem informacji", jednakże w kontekście omawianej wypowiedzi oba pojęcia mają (w tym przypadku) ten sam zakres znaczeniowy. Przy takim rozumieniu pojęć powstają następujące wątpliwości :

1. sprawca kopiujący zapis informacji na „nośniku komputerowym" kopiuje dane – jeśli nie otworzy np. skopiowanych plików, a jedynie będzie w posiadaniu ich kopii, nie dojdzie do procesu interpretacji tychże danych, a więc sprawca nie zapozna się z informacją; w tym kontekście nie jest dla mnie jasne wypełnienie znamion przestępstwa z omawianego artykułu, a to z powodu specyficznych cech danych przetwarzanych elektronicznie – w przypadku kopiowania zapisu informacji przez ręczne przepisanie pisma sprawca podświadomie zapoznaje z treścią, co w przypadku kopiowania danych cyfrowych nie zachodzi;
2. całkowicie chybiony wydaje mi się pogląd, głoszący wypełnienie znamion przestępstwa przez skopiowanie zapisu informacji ma nośniku komputerowym przez sprawcę, który nie ma realnej możliwości zrozumienia treści informacji (dyskusyjne, aczkolwiek nie pozbawione sensu jest takie ujęcie w przypadku przejęcia władztwa nad nośnikiem zapisu informacji w przypadku uniemożliwienia uprawnionemu dysponentowi zapoznania się z ową informacją);

---

[260] autor pracy doszedł do podobnych wniosków, co A. Marek, stwierdzający, iż „wystarczy uzyskać w sposób określony w tym przepisie nieprzeznaczoną dla sprawcy informację – bez wymagania jej percepcji [...]. Przy innej interpretacji udowodnienie dokonania tego przestępstwa byłoby często niemożliwe"; por. : A. Marek – Kodeks karny. Komentarz. Dom Wydawniczy ABC, 2005, wyd. II;

[261] każdy plik przechowywany na np. twardym dysku komputera ma postać pliku binarnego – plik taki można naturalnie odczytać, korzystając z wiedzy matematycznej i znajomości tablic ASCII, ale to już jest proces interpretacji, więc zapoznajemy się z informacją, nie danymi;

Według autorów komentarza, przepis art. 267 § 1 chroni „szeroko rozumiane prawo do dysponowania informacją[262]" i w tym kontekście skopiowanie zapisu informacji może zostać uznane za wypełnienie znamion przestępstwa (dysponowanie bez zgody dysponenta), ale jedynie w przypadku, gdy uznamy pojęcia „informacji" i „zapisu informacji" za tożsame. Autor pracy uznaje rozdzielność zakresu obu pojęć zgodnie z rekomendacją OECD, w związku z czym przychyla się do poglądu uznającego „uzyskanie" informacji za „zapoznanie się z jej treścią", pomimo niewątpliwych ujemnych konsekwencji na polu dowodowym (autor wyraża pogląd, iż dokonywanie tak dalekiej wykładni przepisu w celu uczynienia go funkcjonalnym mija się z celem – martwy przepis należy nowelizować, aby mógł spełniać należne mu funkcje).

W Kodeksie Karnym przepis dotyczący ochrony tajemnicy korespondencji jednocześnie kryminalizuje przestępstwo „hackingu"[263]. Jak to określił A. Adamski „stosunek polskiego ustawodawcy do zjawiska 'hackingu' określić można jako umiarkowanie liberalny", dodając, iż należy przypuszczać, ze nie jest to postawa w pełni zamierzona[264]. Treść przepisu warunkuje postawienie zarzutu popełnienia czynu z art. 267 § 1 w wyniku „przełamania zabezpieczeń" – w związku z tym uzyskanie dostępu do systemu, który nie jest zabezpieczony nie mieści się w ramach opisywanego przepisu. Warto dodać, że niektóre powszechnie używane systemy operacyjne nie spełniają podstawowych wymogów bezpieczeństwa, o czym informują sami ich twórcy[265]. Przepis art. 267 § 1 można interpretować dwojako :

1. Złamanie zabezpieczenia w postaci hasła wiąże się niekiedy z zaznajomieniem się przez „hackera" z jego treścią – w tym przypadku sprawca swoim działaniem wyczerpuje ustawowe znamiona czynu z analizowanego przepisu[266]. W tym przypadku nie jest konieczne użycie „zcrackowanego" hasła i penetracji systemu – karalna staje się czynność przygotowawcza, czyli uzyskanie informacji warunkującej wejście do systemu, poprzez nieuprawnione uzyskanie informacji, jaką jest treść hasła, a nie uzyskanie – dzięki tejże informacji – dostępu (nieuprawnionego) do systemu komputerowego;

---

[262] nieco inaczej A. Marek, ujmując za przedmiot ochrony „prywatność i tajemnicę komunikowania się"; por. : A. Marek – Kodeks karny. Komentarz. Dom Wydawniczy ABC, 2005, wyd. II;

[263] rozumianego jako nieuprawnione zapoznanie się z informacją w wyniku przełamania zabezpieczeń – podnosiłem już tą kwestię, uważam natomiast, iż jest ona na tyle istotna, że należy się jej ponowna wzmianka – ogólnie za „hacking" uważa się czyn polegający na uzyskaniu nieuprawnionego dostępu do systemu komputerowego, przy czym przesłanką dodatkową może być wymóg przełamania zabezpieczeń, natomiast przepis art. 267 § 1 chroniąc tajemnicę korespondencji wprowadza definicję czynu, który ze „stricte hackingiem" ma niewiele wspólnego (patrz art. 2 Konwencji);

[264] A. Adamski – Hacking a nowy kodeks karny; tekst opublikowany w „Informatyce" nr 9/1998 str. 9-12, źródło : http://www.law.uni.torun.pl/KOMP-LEX/I9-98.html

[265] „Zawsze stawialiśmy sprawę jasno. Windows 95 ani Windows 98 nie są systemami, których można używać w środowisku, gdzie ktoś może czyhać na bezpieczeństwo." Paul Leach (Microsoft) 29 października 1998 r. [w:] M. Molski, S. Opala – Elementarz ..., op. cit., str. 153;

[266] często jednak złamanie hasła odbywa się w sposób zautomatyzowany i „hacker" nie poznaje treści hasła, a jest jedynie informowany o uzyskaniu dostępu;

2. Alternatywną interpretacją przepisu jest jego wykładnia gramatyczna, zgodnie z którą „hacker" ponosi odpowiedzialność karną za zapoznanie się z treścią informacji przechowywanej w systemie komputerowym, nie będącą dla niego przeznaczoną, w przypadku uzyskania dostępu do niej w wyniku przełamania zabezpieczeń; w tym kontekście można mówić o „kradzieży informacji"[267] (chociaż bardziej na miejscu jest określenie „kradzież z włamaniem"); pomimo poprawności powyższej wykładni, w praktyce może ona być mało użyteczną, a to z powodu :

    - niejako narzucenia „hackerowi" zamiaru pozyskania informacji, co niekiedy nie ma odniesienia do stanu faktycznego – np. w przypadku, gdy celem włamania jest wykorzystanie przez sprawcę potencjału obliczeniowego „hackowanego" systemu (tzw. „kradzież czasu pracy komputera")[268]; problematyczny również w tym momencie wydaje się być fakt postawienia zarzutu (z powyższego artykułu KK) „hackerowi", który włamał się do systemu w celu dalszego użycia go jako komputera „zombie" (w przypadku ataku DoS/DDoS);
    - trudności, jakie napotka udowodnienie sprawcy faktu, że informację uzyskał (czyli zapoznał się z nią); nawet przyjmując, iż w logach systemowych pozostaje zapis o aktywności użytkowników, nie nastręcza większych trudności dezaktywacja tej funkcji bądź usunięcie fragmentu logu, dotyczącego działań podjętych przez określonego użytkownika;

W stosunku do przyjętych powszechnie standardów kryminalizacji „hackingu", kładących nacisk na ochronę systemów komputerowych przed dostępem do nich osób do tego nieuprawnionych ze względu na bezpieczeństwo tych systemów i ich integralność, bardziej odpowiadająca ich założeniom wydaje się być pierwsza z powyższych interpretacji, druga natomiast nawiązuje raczej do konstrukcji kradzieży z włamaniem, niż do naru-

---

[267] *W. Wróbel – Przestępstwa przeciwko ochronie informacji, Rzeczpospolita Nr 206 (3550) z dnia 3 września 1993 r. [w:] A. Adamski – Prawo karne ..., op. cit., str. 47;*

[268] *wg. brytyjskich ekspertów ds. bezpieczeństwa systemów komputerowych, 95 % przypadków „hackingu" ma na celu wykazanie nieskuteczności zabezpieczeń, a pozostałe 5 % to ataki mające na celu pozyskanie informacji; Security – Return of the Hack, Computing z dnia 30 kwietnia 1998 r., str. 56 [w:] A. Adamski – Prawo karne ..., op. cit., str. 48 przyp. 1;*

szenia miru domowego (*per analogiam* do integralności i nienaruszalności systemu komputerowego)[269].

Przestępstwo typizowane w przepisie art. 267 § 1 jest przestępstwem materialnym, którego karalnym skutkiem jest zapoznanie się przez sprawcę z treścią informacji będącą dla niego zastrzeżoną. Jak pisałem wcześniej, dobrem chronionym przez ten przepis jest poufność informacji (w tym przypadku przechowywanej w systemie komputerowym), co odbiega od powszechnie przyjmowanych, w stosunku do czynów określanych mianem „hackingu", norm. Przestępstwo to jest przestępstwem powszechnym, z oczywistym wyłączeniem osób posiadających uprawnienia do zapoznania się z informacją („kto bez uprawnienia uzyskuje informację ..."), lub będących jej adresatami. Przedmiotem czynu jest informacja dla sprawcy nie przeznaczona, czyli sprawca nie jest jej adresatem (brak wyraźnego wskazania na sprawcę jako na adresata informacji, brak również jakichkolwiek przesłanek uzasadniających twierdzenie, iż sprawca tym adresatem jest – nawet w wypadku braku wyraźnego wskazania adresata). Przy uzyskaniu przez sprawcę informacji dla niego nie przeznaczonej konieczny jest brak uprawnień do ich uzyskania – przewidziany jest więc kontratyp uzyskania informacji przez osobę nie będącą jej adresatem, natomiast posiadającą uprawnienia do zapoznania się z nią (np. działania operacyjne Policji, przeprowadzone na podstawie i zgodnie z przepisami szczególnymi, regulującymi tą materię). Sposoby uzyskania informacji przez sprawcę zostały ujęte w formie listy zamkniętej jako :

1. otwarcie zamkniętego pisma – w każdy możliwy technicznie sposób;
2. podłączenie się do przewodu służącego do przekazywania informacji (w tym przypadku konieczne jest przedsięwzięcie przez sprawcę działań technicznych, czyli eliminuje kryminalizację podsłuchania rozmowy telefonicznej przez osobę stojącą obok rozmawiającego);
3. przełamanie elektronicznych, magnetycznych lub innych szczególnych zabezpieczeń (co niekiedy wymaga od sprawcy podjęcia skomplikowanych czynności); w tym przypadku posłużono się listą otwartą, co sprawia wrażenie perspektywicznego ujęcia problematyki;

Podjęcie wyżej wymienionych działań, nie uwieńczonych zapoznaniem się z informacją nie przeznaczoną dla sprawcy jest usiłowaniem[270]. Strona podmiotowa prze-

[269] *A. Adamski – Prawo karne ..., op. cit. str. 48;*

stępstwa polega na umyślności – przyjmuje się, że zamiar ewentualny nie może wystąpić[271]. Skutek nie występuje także w przypadku skopiowania przez sprawcę pliku z danymi, z którymi nie zdążył, czy też nie miał zamiaru, się zapoznać.

Podstawą zakazu formułowanego w art. 267 § 1 jest założenie, że prawo powinno chronić wyłącznie te kategorie informacji, które zostały przez dysponenta zabezpieczone, co ma być wyrazem woli zastrzeżenia ich do własnej wyłącznej dyspozycji. Zabezpieczenia te powinny spełniać rolę realnej przeszkody[272] w zapoznaniu się z informacją przez osoby do tego nieuprawnione. O zaistnieniu przestępstwa określonego przez art. 267 § 1 decyduje nie fakt uzyskania zastrzeżonej informacji, co sposób jej uzyskania. W przypadku uzyskania tej informacji bez przełamywania zabezpieczeń, nie można mówić o popełnieniu przestępstwa (np. w przypadku posłużenia się przez sprawcę technikami opisanymi poniżej), a w przypadku wykorzystania „dziury" w systemie nie można sprawcy nawet postawić zarzutu usiłowania[273].

6.3 art. 267 § 1 a metody działań przestępczych

Jak wspomniałem w rozdziale poświęconym podziałom przestępstw komputerowych i metodom działań przestępczych i rozdziale dotyczącym „hackingu", *modus faciendi* „hackerów" obejmuje bardzo szeroki wachlarz sposobów działania, nie wspominając już o motywach postępowania. Postaram się przedstawić kilka z nich pod kątem możliwości postawienia sprawcy zarzutu popełnienia przestępstwa z omawianego artykułu, przy czym pamiętać należy, iż „hackerzy" mogą nie tyle poszukiwać informacji, ile próbować swoich sił w przełamywaniu zabezpieczeń, a także stosować metody dające im możliwość infiltracji systemu bez przełamywania jego zabezpieczeń – głównie takie metody (a dokładnie kilka z nich) chciałbym bliżej przedstawić.

Podstęp – jest to bardziej zbiór metod (zasadzających się na manipulacji), niż sam sposób i posiada kilka (co najmniej) desygnatów, z których przedstawię dwa :

- „social engineering" czyli „inżynieria społeczna" jest oddziaływaniem nie na system komputerowy, a na człowieka, który go obsługuje (najczęściej to jest właśnie najsłabsze ogniwo zabezpieczenia systemu przed atakiem); „hacker" wprowadza w błąd, co do swojej tożsamości, za pomocą telefonu, „fake maila", czy też osobiście, dysponenta poszukiwanej przez siebie informacji – podając się za uprawnionego użytkownika uzyskuje hasła do-

[270] *Kodeks Karny. Komentarz, op. cit., str. 755;*
[271] *ibidem;*
[272] *„realna przeszkoda" w tym przypadku oznacza przeszkodę, w stosunku do której należy podjąć bezpośrednie oddziaływanie w celu jej przełamania;*
[273] *A. Adamski – prawo karne ..., op. cit., str. 53;*

stępu, w związku z czym kodeksowe „przełamanie zabezpieczeń" staje się zbędne – „hacker" uzyskuje dostęp do systemu na prawach legalnego użytkownika sieci, co, wobec braku wypełnienia znamion, uniemożliwia postawienie zarzutu z art. 267 § 1. Wszystkie „podręczniki" traktujące o „inżynierii społecznej" podkreślają konieczność dokładnego poznania obowiązujących w danym miejscu regulacji (często wymienia się „trashing", czyli przeszukiwanie śmieci pochodzących z danej firmy, jako skuteczny sposób poznania jej struktury, organizacji i panujących zasad) zwyczajów swojej ofiary. W ten sposób sprawca doprowadza do sytuacji, w której nie tyle „aktywnie uzyskuje" potrzebną mu informację, jaką jest przykładowo hasło dostępu do systemu, co jest mu ona oferowana. Inną kwestią jest wspomniany już „świadomy użytkownik"[274]

- IP spoofing – metoda zasadzająca się na manipulacji systemem komputerowym, szczególnie zaś elementem filtrującym przychodzące pakiety pod kątem adresu IP ich nadawcy; działanie sprawcy polega na zmianie w nagłówku pakietu TCP adresu IP nadawcy i zmyleniu filtra, który uznaje je za pakiety pochodzące z wnętrza sieci, a nie za intruza, co pozwala „hackerowi" ominąć procedurę weryfikacji użytkownika przy „wejściu do sieci"; sprawca nie „przełamuje" zabezpieczeń i nie tyle je omija, co jest „wpuszczany" do sieci, co nie wypełnia znamion przestępstwa, tak więc, analogicznie do przykładu powyżej, art. 267 § 1 nie znajduje w tej sytuacji zastosowania;

Przy okazji omawiania „IP spofingu" zwrócę uwagę na fakt powodujący bezkarność stosowania tej techniki. Godna rozważenia w tym punkcie wydaje się być kwestia statusu pakietu protokołu TCP. Zmiana adresu IP nadawcy w jego nagłówku, z oryginalnego na spreparowany (na czym technika ta polega) nosi teoretycznie znamiona powszechnego przestępstwa fałszerstwa. Niestety, wśród przedmiotów wykonawczych tego przestępstwa nie znajdzie się pakietu przesyłanych danych (niezależnie od rodzaju[275]), a w związku z obecną redakcją przepisu § 14 art. 115 KK nie można uznać go za dokument, pomimo bezsprzecznego posiadania atrybutu „nośnika danych" – pakiety danych płynące światłowodem są formą zapisu informacji, nie mając żadnego podłoża i będąc samoistnymi jej nośnikami[276],

---

[274] najsłynniejszy „socjotechnik", Kevin Mitnick stwierdził „wydajecie miliardy dolarów na „firewalle", systemy biometryczne i inne techniki zabezpieczeń, po czym pozwalacie, aby wasz pracownik zapisał hasło na kartce i przykleił do monitora", co w pełni oddaje realia bezpieczeństwa teleinformatycznego;
[275] TCP, UDP itp.;
[276] A. Adamski – Rządowy projekt ..., op. cit. str. 4;

Wykorzystanie przez sprawcę luki systemowej bądź „dziury" w oprogramowaniu w celu uzyskania dostępu do systemu pozostaje poza zakresem karalności na gruncie Kodeksu Karnego, jeśli działanie sprawcy ograniczyło się jedynie do „wejścia" do systemu. W takim bowiem przypadku nie może być mowy o przełamaniu zabezpieczeń, nawet jeśli zostały one zainstalowane w atakowanym systemie[277]. Ponadto sprawca w tym przypadku nie podlega sankcji nawet w przypadku „uzyskania" informacji, do czego nie był upoważniony. Inną kwestią jest uzyskanie nieuprawnionego dostępu przez włamywacza w wyniku przełamania zabezpieczeń, pomimo istniejących w systemie niezałatanych luk – w przypadku, kiedy działanie sprawcy nie ograniczy się do uzyskania dostępu, a wypełni wszystkie znamiona przestępstwa, sprawca będzie ponosił odpowiedzialność karną z art. 267 § 1 KK.

Kolejną kwestią, którą poruszyłem we wcześniejszej części pracy, jest motyw działania hackerów. Korzystając z wyżej wymienionych technik (lub też wielu innych, o których nie wspomniałem) mogą uzyskiwać wejście do systemu, aby wykorzystać go do innego celu – zaatakowany komputer spełnia tym samym jedynie funkcję narzędzia wykonawczego (jak ma to miejsce w przypadku ataku typu DDoS).

Opisane powyżej metody działań odnoszą się do ataków pochodzących z zewnątrz atakowanej sieci. Rzecz ma się nieco inaczej w przypadku ataku z wewnątrz. W związku z tym chciałbym przedstawić dwa przypadki, które nawet jeśli nie zdarzają się na porządku dziennym, to występują niewątpliwie dość często, a mianowicie „przekroczenie" uprawnień przez pracownika oraz działania administratora sieci w ramach zakresu (lub poza) obowiązków.

Cyberprzestrzeń jest środowiskiem charakteryzującym się dużą częstotliwością interakcji międzyludzkich, co może być powodem wielu konfliktów interesów (pomiędzy użytkownikami) jak i występowania zachowań, uznawanych przez administratorów sieci za dysfunkcjonalne[278]. Zrozumiałe jest więc, iż na użytek administrowanej przez siebie sieci administrator tworzy regulamin korzystania z niej. Niewątpliwie siecią, która przysparza administratorowi najmniej problemów jest sieć oparta na schemacie „administrator może wszystko, użytkownik nic", gdzie istnieją tylko takie dwa rodzaje kont. Rozbudowane sieci informatyczne charakteryzują się jednak skomplikowaną strukturą wewnętrzną i gradacją uprawnień posiadanych przez użytkowników poszczególnych rodzajów kont.

---

[277] na gruncie np. włoskiego kodeksu karnego byłoby to działanie podlegające karalności;
[278] A. Adamski – Prawna reglamentacja zachowań użytkowników i administratorów sieci komputerowych, materiały seminarium Secure 97; źródło : http://www.law.uni.torun.pl/KOMP-LEX/zegrze97.html

Niezwykle częstym przypadkiem są próby uzyskania przez użytkowników posiadających w sieci mniejsze uprawnienia dostępu do zasobów systemu dla nich normalnie niedostępnych – najczęściej poprzez uzyskanie hasła swojego zwierzchnika. Niezależnie od motywów kierujących sprawcą, kwestia ewentualnego postawienia mu zarzutu z art. 267 § 1 zależy od sposobu uzyskania dostępu. Najprostsze wydaje się posłużenie „inżynierią społeczną" i zdobycie hasła wprost od administratora systemu, lub też użyć jednej z metod podstępu. Życie jednak bywa bardziej niewiarygodne niż fikcja i niekiedy wystarczy sprawdzić, czy dany pracownik, mający większe uprawnienia nie zapisał hasła dostępu np. na karteczce i nie przykleił do monitora[279]. Zapoznanie się w tym przypadku z „informacją dla sprawcy nie przeznaczoną", jakim jest treść hasła nie wypełnia znamion „przełamania zabezpieczeń" – co więcej nie można nawet mówić o ich ominięciu. Najciekawsze są konsekwencje, jakie ten przypadek niesie ze sobą. Otóż pracownik poruszając się po zastrzeżonych normalnie dla siebie rewirach systemu może swobodnie zapoznawać się z przechowywanymi tam informacjami, nadal nie wypełniając znamion czynu typizowanego przez art. 267 § 1, może je również kopiować, a przesyłając je dalej nie wypełnia również znamion § 3 wspomnianego artykułu. Dopóki działanie sprawcy polega na wymienionych wyżej zachowaniach, pozostaje on faktycznie bezkarny (wyjątkiem mogą być okoliczności pozwalające na postawienie sprawcy zarzutu z art. 130 § 3).

Drugim przypadkiem, jaki chciałbym pokrótce omówić, jest działalność administratora systemu, która niekiedy stawia go na granicy prawa, a nawet poza nią. Postulat „świadomego użytkownika" dotyczy również osób zarządzających siecią, tyle że w większym stopniu i nieco innym zakresie. Jak zauważył A. Adamski w cytowanym wyżej wykładzie, uprawnienia administratora systemu bardzo często mogą stawiać go „po drugiej stronie barykady"[280]. Kwestią, jaką poruszę jest prawo użytkownika sieci komputerowej do poufności prywatnych danych przechowywanych w systemie komputerowym będącym elementem składowym sieci. Administrator posiada największe uprawnienia użytkownika sieci, co determinuje wgląd w każde inne konto, należące do tej sieci – abstrahując od problemu, czy wolno mu przeglądać prywatne pliki innych użytkowników[281], możliwości ich przeglądania ma de facto nieograniczone. Administrator, logując się na swoje konto („administrator, superuser") często nie ma nawet możliwości „ominąć" zabezpieczeń użytkowników ani nawet zapoznać się treścią ich haseł – ma bezpośredni wgląd we wszystkie

[279] *patrz uwagi w podrozdziale 2.3;*
[280] *referat ten opierał się jeszcze na przepisach Kodeksu Karnego z 1969 roku i stąd uwagi że prawo polskie nie dysponuje mechanizmami penalizacji różnego typu zachowań, nie ma to jednak wpływu na niniejsze rozważania;*
[281] *kwestia otwartą do dyskusji jest problem, czy użytkownik może posiadać na np. służbowym komputerze prywatne pliki, a jeśli nie, to czy zakaz taki może zostać wprowadzony regulaminem danej sieci i czy taki regulamin, którego autorem jest administrator może udzielić mu zezwolenia na kasowanie plików, które np. uważa za potencjalnych nosicieli wirusów i czy postępowanie takie, na podstawie regulaminu zwalnia go od odpowiedzialności karnej na podstawie np. art. 268 KK ?*

dane na wszystkich kontach. Jak widać art. 267 § 1 całkowicie nie ma tu zastosowania, jedynie można rozważać kwestię postawienia zarzutu z art. 266 § 1.

6.4 ocena końcowa art. 267 § 1 KK;

Wzmiankowane na początku rozdziału określenie stosunku polskiego ustawodawcy do „hackingu" jako umiarkowanie liberalnego ma, na podstawie powyższych rozważań, realne uzasadnienie w stanie faktycznym i na powstałe pytanie, czy stosunek ten ma charakter zamierzony trzeba udzielić odpowiedzi – niestety negatywnej. Przepisowi art. 267 § 1 można wytknąć wiele potknięć, których nie można uznać za celowe działanie ustawodawcy.

Ocena końcowa przepisu art. 267 § 1 powinna przebiegać dwutorowo : jako przepisu chroniącego poufność informacji oraz przepisu kryminalizującego zjawisko „hackingu". Ze zrozumiałych względów uwagę skupię na drugiej z wymienionych kwestii.

Za podstawowy, a praktycznie jedyny liczący się w tej pracy argument ocenny przepisu art. 267 § 1 należy uznać fakt, że nie kryminalizuje „hackingu" i jakkolwiek można dalej rozpatrywać, w jakim stopniu zapewnia ochronę poufności informacji (co, jak wynika z redakcji, jest podstawowym jego celem), to jako przepis „anty-hackerski" nie posiada żadnego praktycznie znaczenia. Pomimo braku jakiejkolwiek ustawowej definicji „hackingu", to na podstawie analizy przepisów Konwencji można stwierdzić, że za działanie takie uchodzi „uzyskanie umyślnego, bezprawnego dostępu do całości lub części systemu informatycznego", czyli zamach na integralność i niezakłócone działanie systemów przetwarzania informacji.

Niewątpliwą wadą przepisu, rozumianego jako regulację chroniącą poufność informacji, jest uzależnienie odpowiedzialności karnej za czyn typizowany w art. 267 § 1 od przełamania przez sprawcę zabezpieczeń, które stoją na straży informacji – przyjęcie takiego rozwiązania osłabia funkcję ochronną przepisu, rozumianego jako ochronę poufności informacji. Kolejną, wiążącą się z poprzednią, jest wymóg zapoznania się przez sprawcę z informacją, co może powodować komplikacje dowodowe. Ogólnie rzecz ujmując, przepis ten, konstytuując przestępstwo materialne, „obarczony" jest koniecznością spełnienia przez sprawcę dodatkowych przesłanek, co w sumie owocuje – w kontekście coraz to nowych metod działań sprawców, ich motywów i celów – przynajmniej częściową niemożnością zastosowania sankcji karnej.

W tym miejscu chciałbym jeszcze zawrzeć refleksję nad przesłanką „przełamania zabezpieczeń" egzystującą w treści omawianego przepisu. Z jednej strony trudno się nie zgodzić z powyższą argumentacją, mówiącą o wyrażeniu woli przez dysponenta po-

przez wprowadzenie zabezpieczeń, z drugiej zaś powstaje pytanie, dlaczego niezabezpieczony system informatyczny ma pozostać bez ochrony prawnej. Ostatecznie „wejście" do niechronionego systemu również jest działaniem co najmniej nieetycznym. Poza tym modele ochrony prawnokarnej, wprowadzone przez niektóre kraje europejskie, pomimo zawarcia wymogu zabezpieczenia systemów teleinformatycznych lub danych przechowywanych w takich systemach, wśród znamion przestępstwa „hackingu" nie uwzględniają konieczności ich przełamywania. W to miejsce wprowadzają jedynie wymóg wyrażenia przez podmioty uprawnione wyraźnego zastrzeżenia dysponowania dostępem do systemów lub danych. Elementem decydującym jest więc wola dysponenta dobrem ukierunkowana na jego zabezpieczenie, nie zaś jakość tych zabezpieczeń, czy też ich przełamanie. Jak zauważył P. Waglowski „patrząc na problem okiem prawnika - gdy ktoś ukradnie portmonetkę z mieszkania, do którego drzwi nie były zamknięte - będzie to nadal kradzież. Doświadczenie podpowiada nam jednak, że drzwi warto zamykać."[282] Na gruncie prawa karnego w tym przypadku karalność czynu zależeć będzie nie od tego, czy drzwi były zamknięte, czy otwarte, lecz od faktu, czy zainstalowano w nich zamki. W regulacjach prawnych problematyka ta znalazła oddźwięk w różnych schematach kryminalizacji „hackingu".

Na gruncie Kodeksu Karnego z 1932 r.[283] tajemnica korespondencji chroniona była przepisem art. 253 § 1, wprowadzającym karalność nieuprawnionego [1] otwarcia zamkniętego pisma dla sprawcy nie przeznaczonego, [2] przywłaszczenia lub niszczenia cudzej korespondencji, nim adresat się z nią zapoznał, [3] przyłączania się do przewodu, służącego do podawania wiadomości, [4] podstępnego uzyskania nie przeznaczonej dla sprawcy wiadomości telefonicznej lub telegraficznej. Warto zauważyć, przekładając redakcję tego przepisu na dzisiejsze realia, że chroni poufność informacji w szerszym zakresie, niż czyni to obecnie art. 267 § 1 KK. Przykładowo, wprowadzenie karalności podstępnego uzyskania wiadomości obecnie zaowocowałoby objęciem sankcją karną wykorzystanie przez sprawcę metod socjotechnicznych („*social engineering*") oraz manipulację systemem („*IPspoofing*"). Przepis chroni poufność zabezpieczonej informacji („zamknięte pismo") szerzej, niż czyni to jego odpowiednik z 1997 r., nie wprowadza bowiem wymogu „uzyskania informacji" – do zaistnienia przestępstwa wystarcza sam fakt otwarcia pisma dla sprawcy nie przeznaczonego (przeczytanie otwartego pisma pozostaje poza zakresem karalności, w sferze działań nieetycznych). Mając na uwadze jednoczesną kryminalizację podsłuchu („podłączenie się do przewodu") można stwierdzić, iż na ówczesne realia był to przepis uniwersalny, który także w dniu dzisiejszym nie stracił całkowicie skuteczności.

[282] *P. Waglowski – Nadchodzi czas wielkiej kwarantanny, http://www.vagla.pl/felietony/felieton_062.htm;*
[283] *Rozporządzenie Prezydenta Rzeczypospolitej z dnia 11 lipca 1932 r. – Kodeks Karny (Dz. U. z dnia 15 lipca 1932 r.);*

6.5 art. 267 § 1 KK na tle Konwencji o Cyberprzestępczości

Analizując konstrukcję przepisu art. 267 § 1 i porównując ją do brzmienia art. 2 Konwencji nie sposób nie zauważyć, że przepisy te traktują o dwu różnych zachowaniach przestępczych. W związku z tym porównywanie ich nie ma większego sensu, a omówienie, w jakim stopniu art. 267 § 1 KK spełnia postanowienia art. 2 Konwencji zamyka się w jednym słowie : „żadnym". Ponadto zrozumiałe zdziwienie budzi fakt, iż w tym stanie rzeczy ustawodawca nie zdecydował się na nowelizację omawianego przepisu, zwłaszcza na gruncie „cybernowelizacji" KK, tym bardziej, iż karalność „nieuprawnionego dostępu" nie pojawiła się dopiero na gruncie Konwencji, a w różnych ujęciach egzystowała w raporcie OECD i Zaleceniu Nr (89) 9.

Art. 2 Konwencji („Nielegalny dostęp") przewiduje kryminalizację „umyślnego, bezprawnego dostępu do całości lub części systemu informatycznego", jednocześnie przewidując alternatywne wprowadzenie dodatkowych przesłanek w postaci konieczności naruszenia zabezpieczeń, zamiaru pozyskania danych informatycznych lub innego nieuczciwego zamiaru lub popełnienia przestępstwa w stosunku do systemu, który jest połączony z innym systemem informatycznym. Już tytuł przepisu wskazuje jego treść i można uznać, iż jest to przepis kryminalizujący czyn zwany „hackingiem".

Konstrukcja art. 267 § 1 środek ciężkości kładzie na „uzyskaniu informacji", do czego sprawca nie był uprawniony, co jest – jak pisałem wcześniej – uwspółcześnioną wersją przepisu chroniącego tajemnicę korespondencji. Dodatkowo wprowadzono przesłankę przełamania zabezpieczeń, znacznie osłabiającą skuteczność przepisu. W myśl tego artykułu sprawca ponosi odpowiedzialność karną za uzyskanie konwencyjnego „nielegalnego dostępu" tylko wówczas, gdy uzyska informację (która nie jest dla niego przeznaczona) w wyniku przełamania zabezpieczeń, przy czym sam fakt uzyskania owego dostępu nie jest w tym przypadku istotny. „Nielegalny dostęp", o którym mówi Konwencja, traktowany jest domyślnie, jako środek prowadzący do celu, jakim jest uzyskanie informacji i nie podlega karalności.

Konwencja, za pomocą art. 2, chroni nienaruszalność systemów informatycznych, Kodeks Karny przepisem art. 267 § 1 poufność danych, które m. in. mogą być przechowywane w takich systemach – w związku z tym wniosek że oba przepisy chronią różne dobra prawne nasuwa się sam. Jak zauważyłem poprzednio, ciekawostką jest, iż oba przepisy uważa się za kryminalizujące „hacking", nawet jeśli nie zdefiniowano tego pojęcia (w jego pejoratywnym znaczeniu). Podsumowując, zachowanie przestępcze polegające

na uzyskaniu nieuprawnionego dostępu do systemów informatycznych[284] nie podlega w chwili obecnej karalności na gruncie przepisów Kodeksu Karnego jako samoistne przestępstwo.

6.6 Art. 267 § 1 na tle wybranych rozwiązań legislacyjnych państw europejskich;

Poniżej przedstawię przykładowe charakterystyki przepisów karnych dotyczących przestępstwa „hackingu" w państwach europejskich. Aby zaprezentować w szerokim zakresie możliwe rozwiązania, nawiązałem do podziału dokonanego przez M. Möhrenschlagera na trzy główne sposoby kryminalizacji zjawiska[285], a więc na ujęcie wąskie, szerokie i mieszane.

„Hacking" w ujęciu „wąskim" - Dania

Ten schemat karalności „hackingu" uznaje za przedmiot ochrony bezpieczeństwo i poufność informacji przechowywanych w komputerze oraz danych przesyłanych pomiędzy systemami. Zagrożenie sankcją karną dotyczy nieuprawnionego dostępu do informacji (danych).

Rozwiązanie takie zostało przyjęte w Danii w ustawie karnej z 1985 r. w § 263 (2), który to przepis nie zmienił brzmienia w treści dyspozycji po nowelizacji ustawy, uchwalonej 19 maja 2004 r. Przepis ten chroni wyłączność dostępu do informacji (danych) przez osoby do tego uprawnione.

„Hacking" w ujęciu szerokim – przepisy niektórych stanów USA

W tym przypadku ochroną zostaje objęta nienaruszalność systemu i dane komputerowe. Odpowiedzialność karna przewidziana jest w przypadku uzyskania dostępu do systemu przez osobę do tego nieuprawnioną, przy czym nie ma znaczenia, czy uzyskanie dostępu nastąpiło w wyniku przełamania przez sprawcę zabezpieczeń, chroniących dany system.

Rozwiązanie takie zostało przyjęte przez niektóre ustawodawstwa stanowe USA.[286].

„Hacking" w ujęciu mieszanym – Wielka Brytania

---

[284] *a takie ujęcie uznaje za standard prawa europejskiego decyzja ramowa COM (2002) 173 final* [w:] *A. Adamski – Rządowy projekt ..., op. cit., str 3;*

[285] *M. Möhrenschlager – Hacking ? To criminalise or not ? Sugestions for the legislator [w:] A. Adamski (red.) – Prawne aspekty .., op. cit., str. 161 – 181;*

[286] *A. Adamski – Prawo karne ..., op. cit., str. 45 [za:] M. Möhrenschlager : Hacking. Criminalise or not.Suggestions for the legislator [w:] A. Adamski – Prawne aspekty ..., op. cit., 180 – 182;*

Wybierając ten sposób ustawodawca uznaje za przedmiot ochrony dane i programy komputerowe, przewidując karalność za każdą próbę uzyskania nieuprawnionego dostępu do nich.

Karalność „hackingu" wedle tego schematu wprowadzono w Wielkiej Brytanii ustawą o nadużyciach komputerowych (Computer Misuse Act) z 1990 r. Stwierdza ona, w art. 1 ust. 1, iż odpowiedzialności karnej podlega ten, kto :

a) Powoduje uruchomienie jakiejkolwiek funkcji komputera w zamiarze uzyskania dostępu do znajdujących się w nim programów lub danych;

b) Do uzyskania takiego dostępu nie jest uprawniony;

c) W chwili, w które powoduje uruchomienie funkcji komputera wie o tym, że nie jest osobą do tego uprawnioną.

W związku z takim przyjęciem kryminalizacji, karalne staje się samo wejście w interakcję z systemem komputerowym przez osobę do tego nieuprawnioną[287]. Działaniem sprawcy jest „uruchomienie jakiejkolwiek funkcji komputera w zamiarze uzyskania dostępu" – prawo angielskie wymaga jedynie próby zalogowania się w systemie przez sprawcę, która to próba zostanie przez atakowany system odrzucona, aby można było sprawcy postawić zarzut popełnienia przestępstwa. Jednoczesnym wymogiem jest jednak brak uprawnień sprawcy do takich działań, czego ma on świadomość w chwili podjęcia próby logowania się.

Przedmiotem ochrony, w myśl art. 1 ust. 1 ustawy, są dane i programy komputerowe znajdujące się w komputerze. Zaliczenie brytyjskiej ustawy do grupy schematów „mieszanych" wynika z faktu uznania każdej nieuprawnionej próby wejścia do systemu za obiektywny warunek karalności. Strona podmiotowa polega na działaniu w zamiarze bezpośrednim.

Brytyjski model kryminalizacji „*hackingu*" został określony przez M. Möhrenschlagera jako trzeci samoistny schemat podejścia ustawodawcy do problemu[288], natomiast w interpretacji A. Adamskiego stanowi on szczególną formę modelu „wąskiego", którym charakteryzują się ustawodawstwa niektórych państw skandynawskich[289] (przypadek Danii opisano powyżej).

W porównaniu z brzmieniem art. 267 § 1 przepis ustawy angielskiej upraszcza postępowanie sądowe – udowodnienie sprawcy zamiaru uzyskania dostępu do informacji,

[287] *A. Adamski – Prawo karne ..., op. cit., str 54;*
[288] *M. Möhrenschlager – Hacking : criminalize or not ? op. cit. [w:] A. Adamski – Prawne aspekty .., op. cit., , str. 181;*
[289] *A. Adamski – Prawo karne ..., op. cit., str. 45;*

a nie – jak w przypadku polskiego Kodeksu Karnego zamiaru uzyskania informacji – jest zadaniem dużo prostszym. Wystarczy niekiedy przedstawienie wydruku z logów systemowych atakowanego komputera, z których wynikać będzie podjęcie przez sprawcę prób logowania do systemu. Różnica w przedmiocie podlegającym dowodzeniu jest więc bardzo istotna – polska ustawa karna zawęża karalność do uzyskania informacji, stawiając jednocześnie wymóg przełamania zabezpieczeń, czego nie można uznać za element usprawniający postępowanie w takiej sprawie.

Włochy

Art. 615b włoskiej ustawy karnej przestępstwo hackingu konstytuuje jako „nieuprawnione uzyskanie dostępu do systemu informatycznego lub telekomunikacyjnego, chronionego przy pomocy zabezpieczeń”[290]. Konstrukcja przepisu jest niezwykle prosta i w sposobie ujęcia działania przestępczego nawiązuje do przestępstwa naruszenia miru domowego (co jest spotykane także w innych europejskich kodeksach karnych)[291]. Cechą charakterystyczną tego sposobu ujęcia „hackingu” jest poniesienie odpowiedzialności karnej przez sprawcę za uzyskanie nieuprawnionego dostępu do chronionego systemu niezależnie od faktu przełamania zabezpieczeń – przesłanką karalności jest „wejście” do systemu, który w zamyśle jego właściciela miał być chroniony, w tym wypadku więc nie uwalnia od odpowiedzialności karnej wykorzystanie luki w oprogramowaniu i ominięcie zabezpieczeń. Wydaje się również, że do stwierdzenia popełnienia przestępstwa nie jest konieczna świadomość sprawcy co do istnienia zabezpieczeń w penetrowanym systemie. Przepis włoskiej ustawy karnej za przedmiot ochrony uznaje wyłączny dostęp do systemu przez osoby do tego uprawnione, można więc uznać, iż kryminalizuje „hacking” w czystej postaci.

Niemcy

Art. 202a niemieckiego kodeksu karnego (wg A. Adamskiego przepis o najbardziej zbliżonej konstrukcji do art. 267 § 1 KK[292]) za „hacking” uznaje „nieuprawnione uzyskanie dla siebie lub innej osoby[293] danych nie przeznaczonych dla niego i wyraźnie chronionych przed nieuprawnionym dostępem”. W porównaniu z modelem włoskim taka konstrukcja przepisu zapewnia słabszą ochronę, nie kryminalizując uzyskania nieuprawnionego dostępu do systemu, tylko nieuprawnione uzyskanie danych. Do zaistnienia przestępstwa konieczny jest brak uprawnień sprawcy do uzyskania danych oraz wola dysponenta zastrzeżenia ich do własnego, wyłącznego użytku wyrażona zabezpieczeniem. Ustawodawca nie wprowadza natomiast wymogu „uzyskania w wyniku przełamania za-

[290] *A. Adamski – Prawo karne ..., op. cit., str. 49;*
[291] *ibidem;*
[292] *A. Adamski – Prawo karne ..., op. cit., str. 49;*
[293] *w ten sposób przepis ten zawiera w sobie dyspozycję § 1 i 3 art. 267 KK;*

bezpieczeń". Podobnie jak w modelu włoskim sprawcy wystarczy udowodnić uzyskanie danych nie będących dla niego przeznaczonych, znajdujących się w systemie posiadającym zabezpieczenia chroniące przed nieuprawnionym dostępem, tak więc wykorzystanie np. luki systemowej nie wyłącza odpowiedzialności karnej. W porównaniu do analogicznego przepisu Kodeksu Karnego zapewnia szerszą ochronę danych.

Dokonując porównania powyższych przepisów z art. 267 § 1 KK nie sposób dojść do tego samego wniosku, jaki nasuwał się podczas analizy art. 2 Konwencji, a mianowicie, że wprowadzają one karalność różnych zachowań przestępczych i chronią przed odmiennymi zagrożeniami. Uogólniając, przepisy wymienionych państw europejskich wprowadzają sankcję karną za czyn będący uzyskaniem dostępu do systemu / danych bez uprawnienia. Występujący w nich wymóg zabezpieczenia przed takim dostępem nie osłabia ich skuteczności, jako że przełamanie przez sprawcę podjętych środków bezpieczeństwa nie jest traktowane jako przesłanka karalności.

7. Rozdział VII – Tendencje rozwojowe w zakresie problematyki „przestępczości komputerowej”

Rozwój „przestępczości komputerowej” jest uzależniony od rozwoju technologii. W miarę, jak techniki teleinformatyczne znajdują zastosowanie w kolejnych dziedzinach życia, wraz z nimi pojawiają się nowe formy zachowań niezgodnych z porządkiem prawnym. Drugi kierunek, w jakim zjawisko takiej przestępczości może się rozwijać, jest związany z ogólnym przeobrażeniem świata i skorelowanymi z tym zmianami świadomości społecznej. Czołowym przykładem jest kwestia „cyberterroryzmu”, będącego zjawiskiem niosącym ze sobą tym większe zagrożenie, im większa jest ingerencja teleinformatyki w życie codzienne.

7.1 Kierunki rozwoju „przestępczości komputerowej”

Zjawisko „przestępczości komputerowej” charakteryzuje się obecnie dwoma podstawowymi kierunkami rozwoju. Pierwszym z nich jest stała automatyzacja działań przestępczych, drugim zaś skracanie się czasokresu pomiędzy odkryciem słabości systemowej, a reakcją środowiska przestępczego. Są to dwie relatywnie stałe tendencje, jako że w związku z niezwykle szybkim ewoluowaniem metod przestępczego działania, z każdym rokiem trendy rozwoju ulegają poważnej zmianie. Trzecią kwestią, wynikająca z dwu poprzednich, jest zwiększająca się skala pojedynczego ataku i związanych z tym strat materialnych. Chciałbym zaznaczyć, iż wyznaczenie trendów rozwoju przestępczości omawianego rodzaju przedstawia wiele trudności i jest możliwe praktycznie tylko za pomocą analizy incydentów naruszających bezpieczeństwo teleinformatyczne zgłoszonych do zespołów reagujących na takie zdarzenia (np. CERT NASK). Niezmienną tendencją jest wzrost liczby takich zgłoszeń, trzeba jednak zwrócić uwagę, iż ten stan rzeczy może posiadać dwie równorzędne przyczyny : faktyczny rozwój zjawiska i zwiększenie się świadomości poszkodowanych, zarówno o byciu ofiarą, jak i możliwości zgłoszenia tego faktu.

Na podstawie prowadzonych przez siebie statystyk, istniejący od 1996 zespół CERT NASK, w corocznych raportach przedstawia podsumowanie mijającego roku i możliwe typy zagrożeń na lata następne. W 2000 roku do najczęściej występujących incydentów zaliczono ataki : [1] na systemy poczty elektronicznej, [2] polegające na skanowaniu poszczególnych komputerów bądź sieci, [3] na serwery WWW i [4] zmierzające do blokady systemu. Jednocześnie stwierdzono brak większych zmian w topologii występujących incydentów na przestrzeni lat (tj. od roku 1996)[294]. W 2001 r. stwierdzono utrzymanie się

[294] *CERT Polska – Raport 2000. Przypadki naruszające bezpieczeństwo teleinformatyczne; źródło : http://www.cert.pl;*

wzrostu liczby skanowania komputerów i sieci, głownie dzięki monitorowaniu tych zagrożeń i używania systemów detekcji. Stwierdzono wówczas po raz pierwszy (na podstawie obserwacji rozprzestrzeniania się wirusów sieciowych) istnienie trendu, rozwijającego się do dnia dzisiejszego, mianowicie automatyzację procesu przeprowadzania ataków, jego przyczyn i towarzyszących mu okoliczności takich jak : [1] wykorzystywanie automatycznych narzędzi, zarówno w fazie przygotowania ataku (pisanie wirusów) jak i jego przeprowadzania (skanowanie, włamania za pomocą rootkit'ów), [2] istnienie w atakach znanych, lecz nie załatanych słabości, wykorzystywanych przez te narzędzia. Z powyższym łączy się relatywnie niski poziom wiedzy sprawcy incydentu (zasygnalizowano istnienie kategorii sprawców określanych jako „*script kiddies*")[295].

W roku następnym stwierdzono drastyczne zaciemnienie istniejących w sieci relacji – jednoczesny wzrost odsetka użytkowników dysponujących dużą wiedzą dotyczącą bezpieczeństwa IT i wykazujących się ignorancją w tej materii, trudności w ustaleniu rzeczywistego sprawcy ataku (coraz częściej spotykano się z sytuacją, iż potencjalny sprawca był *de facto* jedną z ofiar – sytuacje takie najczęściej zdarzają się w przypadku „zombies", wykorzystywanych do ataków DoS/DDoS). Jednocześnie utrzymała się tendencja wykorzystywania luk w konfiguracji systemów. Stwierdzono również wzrost liczby coraz bardziej rozległych incydentów[296]. W 2003 roku zaobserwowano dwa główne kierunki rozwoju – utrzymanie się skanowania sieci oraz pojawienie się poważnej dystrybucji nielegalnych treści (przede wszystkim „dziecięcej pornografii"), która, pomimo podejmowanych przeciwdziałań, nadal się rozwija w szybkim tempie. Ponadto incydenty zaczęły charakteryzować się coraz większym stopniem skomplikowania i rozbudowania[297].

W roku ubiegłym utrzymała się tendencja zwyżkowa w kierunku automatyzacji procesu przeprowadzania ataków sieciowych oraz tworzenia całych sieci zagrożeń (wspomniane juz włamywanie się do systemów w celu przejęcia nad nimi kontroli, połączenia w tzw. „*botnet'y*" i wykorzystania do ataku DDOS), Utrzymanie wzrostowego trendu w zgłaszaniu incydentów przypisuje się zarówno większej liczbie przeprowadzanych ataków, jak i ciągłym rozwojem Sieci i wzrostem świadomości użytkowników względem kwestii bezpieczeństwa[298]. Do zespołu CERT zgłaszano coraz więcej poważnych incydentów. Sprawcy należący do kategorii „*script kiddie*s" ustąpili miejsca, pod względem stanowienia zagrożenia, wykwalifikowanym profesjonalistom Do głównych trendów roku 2004 specjaliści z branży bezpieczeństwa teleinformatycznego zaliczają poniższe trzy :

---

[295] CERT Polska – Raport 2001. Przypadki naruszające bezpieczeństwo teleinformatyczne; źródło : http://www.cert.pl;
[296] CERT Polska – Raport 2002. Przypadki naruszające bezpieczeństwo teleinformatyczne; źródło : http://www.cert.pl;
[297] CERT Polska – Raport 2003. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2003; źródło : http://www.cert.pl
[298] przykładowo czas od wydania uaktualnienia na lukę do załatania połowy podatnych systemów uległ skróceniu z 30 (rok 2003) do 21 dni (2004), cyt. za S. Górniak – Obecne trendy w zagrożeniach sieciowych, źródło : http://www.cert.pl

1. ataki zautomatyzowane – tą kategorię zdominowały ataki przeprowadzane za pomocą wirusów i robaków, pomiędzy którymi toczy się walka o pierwszeństwo w statystykach :

   - przykładem działalności wirusów był „MyDoom", rozprzestrzeniający się jako wykonywalny załącznik mailowy i za pomocą sieci p2p, zaprogramowany przez autora na wykonanie ataku DDoS na witrynę www.sco.com, który, pomimo przygotowań firmy SCO i bezpłatnej dystrybucji oprogramowania przeciw wirusowi, zakończył się sukcesem[299]; innym spektakularnym wydarzeniem był „pojedynek" pomiędzy wirusami „Beagle" i „Netsky", rozprowadzanymi za pomocą poczty elektronicznej, z czego na szczególną uwagę zasługuje drugi z wymienionych – przede wszystkim nie zakładał „backdoor'ów" i nie rozsyłał spamu, poza tym likwidował „backdoor'y" założone przez „MyDoom" i „Beagle"[300];

   - w kategorii zagrożeń powodowanych przez robaki specjaliści zwracają uwagę na niezwykle szybkie tempo wykorzystywania przez nie ogłoszonych luk i wcześniejsze przygotowywanie algorytmów infekcji; najbardziej znanymi robakami zeszłego roku był „Sasser" (pojawił się w tydzień po opublikowaniu istnienia luki, którą wykorzystywał, a w przeciągu kilku dni zaobserwowano jego siedem odmian), „Dabber", charakteryzujący się wykorzystywaniem błędu w kodzie „Sassera" (robak – pasożyt, atakujący wyłącznie systemy zainfekowane „Sasser'em") oraz „Witty", który pojawił się w rekordowym czasie 48 godzin od opublikowaniu luki systemowej, zaatakował przede wszystkim grupy komputerów służące do ochrony bezpieczeństwa, a dzięki nowej metodzie infekcji dość szybko się rozprzestrzeniał[301];

2. ataki na „*honeypot'y*", będące przynętami dla „hackerów" są stosunkowo nową kategorią incydentów, stanowiących swoisty „pojedynek" administratora z „hackerem"; celem postawienia „*honeypot'a*" może być próba zwabienia „hackera" do wnętrza tak spreparowanej sieci, poznanie drogi, jaką przemierza np. robak w infekowanym systemie i wypracowanie automatycznych metod przeciwdziałania; ze strony „hackera" atak na „*honeypot'a*" to przede wszystkim wykrycie go i pozbawienie funkcjonalności logowania – duże

[299] *po zablokowaniu witryny www.sco.com pozbawiono wirusa celu zmieniając wpis w serwerach DNS na www2.sco.com; cyt. za S. Górniak – Obecne trendy ..., op. cit.;*
[300] *po ogłoszeniu kolejnej wersji (w sumie było ich ok. 30-stu) twórca „Netsky" poinformował o zaprzestaniu tworzenia kolejnych wersji, jednocześnie opublikował kod źródłowy wirusa;*
[301] *w przeciągu 45 minut stwierdzono zarażenie ok. 12 tysięcy komputerów;*

znaczenie ma w tym maskowanie przez intruza sposobu działania w celu uniemożliwienia poznania jego metody i identyfikacji jego samego;

3. przeglądarki internetowe – rok 2004 był, zwłaszcza dla Internet Explorera Microsoftu, czarnym rokiem; szerzej o lukach odkrytych w przeglądarkach pisałem w rozdziale II, w tym punkcie poruszę jedynie kwestię zarówno rekordowej liczby błędów tego produktu, jak i stworzenie potencjalnie dużego zagrożenia dzięki zintegrowaniu tej przeglądarki z powłoką systemową i klientami poczty;[302]

Dokonując przeglądu przez pojawiające się co roku typy zagrożeń można stwierdzić istnienie kilku kategorii incydentów, które zmieniają co prawda charakter, wciąż jednak są wymieniane w raportach dotyczących bezpieczeństwa Sieci. Podobnie jest z panującymi w tej materii trendami – prym wiedzie automatyzacja przeprowadzania ataków i ich rozległy charakter, a co za tym idzie, zwiększenie się wymiaru strat przez nie powodowanych. Duże znaczenie ma również skrócenie czasu reakcji przestępczego podziemia na ujawnione błędy w oprogramowaniu. Pozwala to przewidywać, przynajmniej częściowo, kierunki dalszego rozwoju „przestępczości komputerowej" – na dzień dzisiejszy jest to np. pojawienie się „0-day exploit'ów" i narzędzi je wykorzystujących.

7.2 Cyberterroryzm – zjawisko i jego konsekwencje

Cyberterroryzm stał się ostatnio określeniem bardzo modnym i dość często wykorzystywanym, jednakże nie sposób nie odnieść wrażenia, iż każdy posługujący się tym zwrotem ma na myśli coś zupełnie innego. Jest to – jak „hacking"' – pojęcie powszechnie znane i używane, a jednocześnie niezdefiniowane i dlatego też postanowiłem poświęcić temu zjawisku więcej uwagi. Czym jest więc cyberterroryzm ?

Zacząć należałoby od pojęcia „terroryzmu", które charakteryzuje się szerokim zakresem, o czym świadczyć może powstanie ponad 100 definicji tego zjawiska. Na potrzeby wprowadzenia do pojęcia „cyberterroryzmu" będę się posługiwał definicją ustawową[303], wg której przestępstwo o charakterze terrorystycznym to „czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat popełniony w celu : [1] poważnego zastraszenia wielu osób, [2] zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej

[302] *S. Górniak – Obecne trendy ..., op. cit;*
[303] *art. 155 § 20 KK;*

do podjęcia lub zaniechania określonych czynności, [3] wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu."

Próbując zdefiniować pojęcie „cyberterroryzmu" natrafia się na ten sam problem, co w przypadku np. kradzieży dokonanej za pomocą komputera – czy czyn polegający na przełamaniu zabezpieczeń systemu informatycznego instytucji, przykładowo banku, i przelaniu pieniędzy zgromadzonych na tamtejszych kontach będzie kradzieżą z włamaniem dokonaną za pomocą zaawansowanej technologii (komputer spełniałby więc rolę narzędzia, podobnie jak wytrych czy łom), czy też będzie to przestępstwo „naruszenia integralności danych informatycznych" ?[304]

W realiach „społeczeństwa informacyjnego", gdzie informacja stała się niejako podwaliną nowej formacji społeczno-ekonomicznej, teoretycznie każdy zamach na nią można uznać za akt terrorystyczny. Powstaje pytanie, czy każdy zamach na każdą informację ? Wydaje się właściwym wprowadzenie zawężenie zakresu pojęcia poprzez używanie zwrotów „istotna informacja", „spowodowanie niebezpieczeństwa powszechnego" itp. Usunięcie bądź modyfikacja danych w systemie informatycznym banku powoduje straty w wielkich rozmiarach finansowych, trudno jednak uznać taki zamach za akt terrorystyczny, natomiast ten sam czyn skierowany przeciw systemom informatycznym np. lotniska spełniłby przesłanki działania terrorystycznego. Pozostaje też kwestia umyślności – czyn o charakterze terrorystycznym wydaje się być możliwym do popełnienia tylko i wyłącznie w zamiarze bezpośrednim.

Problematykę „cyberterroryzmu" i próby definiowania zjawiska podejmowano niejednokrotnie. Wynikiem jednej z nich, dokonanej poprzez podział zachowań przestępczych w odniesieniu do zaawansowanej technologii, aktem „cyberterrorystycznym" będzie zachowanie nie należące do grupy czynów „hackerskich" (pojmowanych jako uzyskiwanie nieuprawnionego dostępu i wyszukiwaniu słabości systemowych, nie wzbudzające społecznego strachu ani nie powodujące wielkich szkód) ani do kategorii działań wykorzystujących wiedzę sprawcy do osiągnięcia korzyści materialnych. Trzecią kategorią zachowań, w której zawierają się akty „cyberterroryzmu", aczkolwiek jej nie wypełniają całkowicie, są ataki mające na celu spowodowanie jak największych szkód (jako przykład wymienia się ataki DoS na witryny CNN czy eBay, a także działalność „Code Red")[305].

Wg innej koncepcji „cyberterroryzm" to „celowe ataki albo groźby ataków skierowane przeciw komputerom, sieciom i przechowywanym w nich informacjom w celu zastraszenia rządów i społeczeństw czy też wymuszenia na nich jakichś politycznych lub

[304] *Abstrahuję w tych rozważaniach od kodeksowych kwalifikacji czynów;*
[305] *J. Böttler – Threats posed by Cyber Terror and Possible Responses of the United Nations;*

społecznych działań". Jednocześnie ataki te powinny być wymierzone przeciw osobom lub własności, albo powinny powodować szkody wywołujące strach (przykładowo mogą to być ataki powodujące katastrofy lotnicze, skażenie wody, powodujące poważne straty ekonomiczne lub ataki na krytyczne infrastruktury)[306].

Można zauważyć ostatnio rozwój tendencji nazywania cyberterroryzmem każdego działania niezgodnego z prawem a dotyczącego zaawansowanej technologii. Przyjęta w Wielkiej Brytanii ustawa Akt o Terroryzmie wprowadza pojęcie „cyberterrorysty", którym to mianem określa praktycznie wszystkich „złych hackerów"[307] – konsekwencje takich unormowań są łatwe do przewidzenia. Każde przestępstwo popełnione z wykorzystaniem zaawansowanej technologii lub przeciw niej może zostać uznane za działanie o charakterze terrorystycznym - samo określenie sprawcy tym mianem nie ma oczywiście większego znaczenia, rzecz rozbija się o wymiar sankcji karnej.

Świat uległ przeobrażeniu po 11 września 2001 r. – społeczności zdały sobie sprawę, że zagrożenie terroryzmem nie ogranicza się do wybranych kilku punktów na kuli ziemskiej, lecz obejmuje cały świat. Międzynarodowa współpraca w materii walki z terroryzmem osiągnęła niespotykane dotąd rozmiary – niestety, niekiedy zgodnie z sentencją „cel uświęca środki". W Stanach Zjednoczonych ponownie, tym razem za społeczną aprobatą, FBI uruchomiło projekt „Carnivore", mający na celu inwigilację poczty elektronicznej, przy jednoczesnej społecznej akceptacji wprowadzenia zakazu stosowania silnej kryptografii. Społeczeństwa zaakceptowały również funkcjonowanie systemu „Echelon", którego istnienie oficjalnie uznano niewiele wcześniej po przeprowadzeniu wieloletnich śledztw[308]. Dzięki medialnemu nagłośnieniu zagrożenia, terroryści osiągnęli jeden ze swoich podstawowych celów, a mianowicie wystąpienie stanu społecznego poczucia zagrożenia, który zaowocował dobrowolnym zrzeczeniem się przez społeczeństwo przysługujących im podstawowych praw na rzecz ochrony ze strony państwa. Zjawiska te zachodzą w warunkach relatywnie słabej znajomości realiów technologii teleinformatycznej[309], dlatego też przedstawienie pewnych faktów w odpowiednim świetle może skutkować działaniami, których konsekwencji społeczeństwa nie są w stanie przewidzieć, a które są trwałe. Prawo tworzone spontanicznie w odpowiedzi na konkretne wydarzenia, zwłaszcza spektakularne, z reguły nie jest „dobrym" prawem – szczególnie dla społeczeństwa, które się go domagało.

---

[306] D. E. Denning – Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, 2000; http://www.cs.georgtown.edu/~denning/infosec/cyberterror.html [w:] *J. Böttler – Threats posed by Cyber Terror ..., op. cit.;*

[307] Wyjaśnienie pojęcia znajduje się w rozdziale poświęconym „hackerom";

[308] Obu systemom – ze względu na ich specyfikę – poświęcę więcej uwagi poniżej;

[309] W rozdziale poświęconym przestępczości komputerowej i „hackerom" pisałem o społecznej świadomości realiów „cyberprzestępczości";

Nie chciałbym, aby powyższe wywody sprawiały wrażenie bagatelizowania przez autora niniejszej pracy problematyki „cyberterroryzmu" – problem istnieje i autor uważa, że jest na tyle poważny, iż zasługuje na bardziej racjonalne podejście do kryminalizacji zjawiska niż uleganie krótkoterminowej ogólnospołecznej histerii. Znaczne podwyższenie wymiaru kary za „przestępstwa komputerowe" w Stanach Zjednoczonych na podstawie „Anti-Terrorism Act" można uznać za posunięcie mające odstraszać potencjalnych sprawców od popełniania czynów przestępnych[310], trudno natomiast zrozumieć zaliczenie wszystkich czynów naruszających integralność, dostępność i poufność danych i systemów informatycznych za akty terrorystyczne – nastolatek kradnący pieniądze z bankomatu jest niewątpliwie złodziejem, trudno natomiast uznać go za terrorystę. W ostatecznym rozrachunku regulacje prawne stają przed trybunałem opinii publicznej, która, pozostając pod wpływem mediów, wydaje werdykt pod naciskiem chwili.

Aby przybliżyć szczególny charakter zjawiska, który określa się mianem „cyberterroryzmu" podam przykład incydentu, jaki miał miejsce 22 października 2002 r. Tego dnia miał miejsce największy, skomasowany atak typu DDoS[311] na podstawową infrastrukturę tworzącą Internet. Zaatakowano w ten sposób 13 serwerów obsługujących system domenowy (DNS[312]) najwyższego poziomu (root level servers[313]) – był to pierwszy w historii atak na wszystkie serwery. W wyniku tego ataku, wg doniesień, przestało funkcjonować 4 lub 5 zaatakowanych maszyn, jednakże pozostałe przejęły ich funkcje i konsekwencje tego incydentu pozostały niezauważone dla szerszej rzeszy użytkowników Sieci. Gdyby jednak dysfunkcja dotknęła wszystkie, przestałby działać Internet[314]. Jest to przykład obrazujący specyfikę uderzeń „cyberterrorystycznych" – był to jeden z najbardziej spektakularnych ataków tego typu – ale tylko dla wtajemniczonych. Dla zwykłego użytkownika Sieci fakt ten przeminął bez echa, natomiast dla tej stosunkowo nielicznej garstki wtajemniczonych był on porównywalny, lub wręcz poważniejszy, od ataku na WTC 11 września. Ażeby to zrozumieć wystarczy sobie wyobrazić konsekwencje unieruchomienia Internetu na choćby 12 godzin.

Wydarzeniem, które można umiejscowić na pograniczu zakresu „cyberterroryzmu" i „hacktyvismu" była swoista wojna pomiędzy „hackerami" pro-izraelskimi i pro-palestyńskimi. Po porwaniu 3 izraelskich żołnierzy przez Palestyńczyków, przez „hackerów" izraelskich został przeprowadzony atak typu DoS na witryny internetowe Autonomii

---

[310] choć jednym z odwiecznych i wciąż poruszanych sporów doktrynalnych jest kwestia wpływu zaostrzenia sankcji karnej na zmniejszenie ilości popełnianych przestępstw;
[311] Distributed Denial of Service – dokładniejszy opis tej techniki znajduje się w rozdziale poświęconym sposobom działań przestępczyh;
[312] Domain Name System – System Nazw Domenowych;
[313] Główne serwery nazw; serwery DNS na poziomie globalnym, które przechowują adresy serwerów nazw dla domen najwyższego poziomu (a więc .com, .edu, itp. oraz domen krajowych -.pl, .nl itp.)
[314] P. Waglowski – Wirtualny terror; http://www.vagla.pl/felietony/felieton_040.htm

Palestyńskiej, co w odpowiedzi spowodowało zmasowane ataki „hackerów" Palestyńskich na strony Parlamentu Izraelskiego, Ministerstwa Spraw Zagranicznych, Banku Izraelskiego i giełdy w Tel – Awiwie[315]. Na podstawie tych wydarzeń można dojść do wniosku, iż sprawcami części incydentów, mających charakter „cyberterrorystyczny", mogą być „hackerzy" kierujący się swoimi przekonaniami politycznymi bądź religijnymi. Tym samym zjawisko „hacktyvismu" może być postrzegane jako poważne źródło zagrożeń.

7.3 Tendencje zmian przepisów karnych regulujących materię „przestępczości komputerowej" w Polsce i na świecie

Zapoznawszy się ze specyfiką „cyberprzestępczości", a także kierunkami jej rozwoju łatwo można stwierdzić, iż stanowi kategorię czynów przestępczych charakteryzujących się niezwykle dynamiczną ewolucją. Ta cecha stawia przed prawodawcą trudny do rozwiązania problem stworzenia regulacji prawnych, będących na tyle uniwersalnymi, iż nie będzie zachodzić potrzeba ich wielokrotnej nowelizacji.

Zapoznając się z treścią projektów ustaw o zmianie ustawy – Kodeks Karny, odnosi się wrażenie, że przepisy dotyczące ochrony informacji znajdują się na szarym końcu zainteresowań legislatorów. Wśród licznych projektów nowelizacji Kodeksu Karnego, przepisy mające na celu ochronę informacji zostały uwzględnione w dwu. Mając na uwadze brak implementacji art. 2 Konwencji o Cyberprzestępczości oraz powszechny pogląd głoszący potrzebę nowelizacji art. 267 § 1 KK, jako przepisu mającego w teorii kryminalizować to przestępstwo konwencyjne, przedstawię pokrótce projekty, zawierające odpowiednie regulacje.

W poselskim „Projekcie Kodeksu Karnego z 2002 r.[316]", będącym właściwie projektem nowego Kodeksu Karnego, przestępstwa przeciwko ochronie informacji umiejscowiono w rozdziale XXXV i w stosunku do obecnie obowiązującej regulacji jest to najpoważniejsza zmiana. *De facto* zmianie uległa jedynie numeracja przepisów – np. dotychczasowy przepis art. 267 § 1 w omawianym projekcie to art. 271 § 1, który niczym nie różni się od poprzednika, podobnie jak pozostałe regulacje tego rozdziału. Ciekawostką jest nieuwzględnienie w treści projektu postanowień Konwencji o Cyberprzestępczości (otwartej do podpisu 23 listopada 2001 r.), pomimo datowania niniejszego druku na dzień 3 marca 2002 r. – przepisy projektowanego rozdziału XXXV są kopią rozdziału XXXIII KK w brzmieniu sprzed „Cybernowelizacji". Inną ciekawą kwestią jest brak odniesienia się autorów do projektowanych przez siebie rozwiązań w uzasadnieniu omawianego projektu

[315] *J. Böttler – Threats posed by Cyber Terror ..., op. cit.;*
[316] *druk sejmowy nr 387; źródło – http://www.sejm.gov.pl;*

– wzmianki doczekał się jedynie przepis dotyczący ochrony tajemnicy państwowej i służbowej.

Innym projektem, zawierającym przepisy dotyczące ochrony informacji, jest prezydencki projekt ustawy o zmianie ustawy – Kodeks Karny z dnia 20 grudnia 2001 r.[317]. Niniejszy projekt wprowadza istotną zmianę art. 267 § 1, polegającą na zmianie chronionego przepisem dobra prawnego z poufności informacji na uprawniony dostęp do niej („kto bez uprawnienia uzyskuje dostęp do informacji dla niego nie przeznaczonej ...”). Karalnością objęte jest więc uzyskanie nieuprawnionego dostępu do informacji. Jednocześnie pozostawiono wymóg popełnienia przestępstwa w wyniku przełamania zabezpieczeń, dodając jednakże alternatywną przesłankę karalności w postaci „ominięcia zabezpieczeń”, co eliminuje kolejny mankament przepisu. Taka redakcja przepisu pozwala na postawienie zarzutu sprawcy posługującego się metodami socjotechnicznymi (lub metodami polegającymi na stosowaniu podstępu) lub wykorzystującym istniejące w systemie luki. Zmiana charakteru czynu przestępnego kryminalizowanego znowelizowanym przepisem art. 267 § 1 KK wydaje się obejmować karalnością przestępstwo „hackingu” – gdyby w redakcji przepisu dodano zwrot „lub systemu służącego do przechowywania danych”, można byłoby mówić o implementacji przestępstwa konwencyjnego z art. 2, traktującego o uzyskaniu nieuprawnionego dostępu do systemu informatycznego. Innym elementem, wprowadzającym pewną elastyczność do przepisów chroniących informację, jest proponowana zmiana zwrotu „zapis na komputerowym nośniku informacji” w redakcji art. 268 § 2 KK na „dane informatyczne”.

Jak można zauważyć, przepisy chroniące informację doczekały się wzmianki w dwu, na kilkanaście, projektach nowelizacji ustawy karnej, z czego zmiany w tych przepisach przewiduje zaledwie jeden. Fakt ten świadczy dobitnie o małym zainteresowaniu problematyką ze strony ustawodawcy, co w dobie tworzenia w Polsce podstaw społeczeństwa informacyjnego jest niezrozumiałe

7.4 Przyszłościowe tendencje zwalczania „przestępczości komputerowej”

Niewątpliwie zapobieganie popełnianiu przestępstw w zarodku jest najbardziej skuteczną metodą – i taka też jest przyczyna powstania i funkcjonowania systemów takich jak „Carnivore” bądź „Echelon”. Niestety problem w tej materii leży gdzie indziej, a mianowicie w stwierdzeniu „odpowiedzialności karnej podlega ten tylko, kto popełnia **czyn** za-

[317] *druk sejmowy nr 181; źródło – http://www.sejm.gov.pl;*

broniony pod groźbą kary …", którym, na szczęście społeczeństwa polskiego, posługuje się rodzimy Kodeks Karny, ustalając tym samym podstawowe granice odpowiedzialności karnej. Trudno jest autorowi niniejszej pracy wyobrazić sobie postawienie zarzutu – na jakiejkolwiek podstawie – za wysłanie e-maila, w którego treści zawierałby się zamiar popełnienia przestępstwa. Jeśli taka sytuacja miałaby miejsce, dzięki przechwyceniu owej wiadomości przez jeden z systemów inwigilacyjnych, oznaczałoby to koniec stosowania jakichkolwiek zasad. Największym zagrożeniem dla podstawowych praw człowieka, związanych z jego wolnościami jest fakt nieznajomości realiów ogólnoświatowej inwigilacji – w Stanach Zjednoczonych fakt działania systemu „Carnivore" był, pomimo podejmowania prób nagłaśniania, powszechnie nieznany, natomiast po 11 września 2001 roku społeczeństwo zaakceptowało jego funkcjonowanie, mając nadzieję, iż zabezpieczy się w ten sposób przed kolejną tragedią, nie zastanowiwszy się, że systemy tego typu pracują nieustannie dokonując selekcji przechwytywanych informacji. Smutek wzbudza również inny fakt – Parlament Europejski nie reagował na doniesienia o istnieniu ogólnoświatowego systemu szpiegowskiego, w którym notabene uczestniczy jedno z państw członkowskich Unii Europejskiej (Wielka Brytania), pomimo, iż pierwsze poważne prywatne dziennikarskie śledztwo datuje się na 1988 rok. Reakcję tego organu udało się uzyskać dopiero po doniesieniach jakoby system „Echelon" służył obecnie szpiegostwu gospodarczemu na rzecz amerykańskich przedsiębiorstw co m. in. było bezpośrednim powodem przegrania przetargu na dostawę samolotów do Arabii Saudyjskiej przez Airbus'a na rzecz Boeinga. Wynika więc jasno, że o ile nie przymyka się oczu na wymierne straty finansowe europejskich koncernów w walce z ich amerykańskimi konkurentami, o tyle pogwałcenie prywatności obywateli państw członkowskich nikomu snu z powiek nie spędza.

Zakończenie

Środowisko, w jakim zachodzą zjawiska przestępczości komputerowej, charakteryzuje się brakiem stałości – podlega procesowi dynamicznego rozwoju, co, naturalną koleją rzeczy, determinuje również rozwój samej przestępczości, zarówno w kategorii metod działania jak i celów i rozmiarów ataku, a także skutków. Regulacje prawne pozostają w tyle, nie są w stanie dotrzymać kroku technologii. Piszę : technologii, bo rozwój przestępczości komputerowej jako zjawiska jest ściśle związany z rozwojem technologicznym, będący dla niej środowiskiem, w jakim istnieje. Rozwój technologii w obecnych czasach jest lawinowy – powstają nowe instytucje, dla których trzeba tworzyć nowe regulacje – definicje, podziały, schematy. Nie wystarcza – na gruncie prawa karnego - kryminalizowanie zjawisk, jakie już wystąpiły, lecz należy szukać rozwiązań wybiegających w przyszłość, pozostających jednocześnie w korelacji z obowiązującymi normami innych gałęzi prawa. Prawo karne spełnia w systemie prawnym rolę posiłkową – nie ustanawia norm współżycia społecznego, a wprowadza sankcje za nieprzestrzeganie norm ustanowionych przez inne dziedziny.

Patrząc na problemy ze zdefiniowaniem niektórych zachowań i na eksperymenty, jakie się obecnie prowadzi nietrudno zauważyć, że kierunek, polegający na dostosowywaniu prawa do zaistniałych już stanów faktycznych nie jest metodą całkowicie skuteczną. W sytuacji, gdy naukowcy w bardzo zaawansowanym stopniu prowadzą prace nad pamięciami białkowymi, trudno przypuszczać, że bezproblemowo uda się zawrzeć w ustawodawstwie karnym kryminalizację ataków na informacje zapisaną na takim „nośniku". Rozwój technologii wdziera się obecnie na tereny dotychczas dla niej niedostępne i łączy (lub podejmuje próby) elementy rzeczywistości do tej pory biegunowo odległe. Postulat tworzenia rozwiązań prawnych niejako „na wyrost" wydaje się być w pełni uzasadniony.

Polskie prawo karne, pomimo podejmowanych w ostatnim czasie prób dostosowania jego rozwiązań do rewolucyjnie zmieniających się realiów, pozostaje niestety w tyle nie tylko za ewoluującymi metodami działań przestępczych, lecz również za rozwiązaniami prawnokarnymi innych państw. Najlepszym przykładem takiego stanu rzeczy jest niepełna implementacja postanowień Konwencji o Cyberprzestępczości, pomimo zawartych w jej treści wyraźnych wskazań co do sposobu uregulowania materii „przestępczości komputerowej" w ustawodawstwie karnym. Jest to o tyle zastanawiające, iż Polska zajmuje drugie (po Korei Płd.) miejsce na liście państw, z których pochodzi najwięcej ataków komputerowych.

Przestępczość komputerowa podlega tym samym prawom, co każdy inny rodzaj przestępczości – i najlepszym sposobem ograniczenia tego zjawiska jest edukacja dotycząca samej podstawy egzystencji ludzkiej i społecznej – pojęcia dobra i zła.. Sam fakt posługiwania się przez sprawcę klawiaturą a nie łomem czy też wytrychem nie jest przesłanką potwierdzającą twierdzenie o szczególnej szkodliwości zjawiska „przestępczości komputerowej" – kwestia zasadza się na problemie środowiska, w którym zjawisko zachodzi i środowiska, w jakim obecnie żyjemy. Tworząc podwaliny systemu społeczno-gospodarczego opartego na informacji zrozumiałe jest dążenie do zapewnienia tejże informacji jak najlepszej ochrony – funkcjonowanie systemu społeczno-ekonomicznego opartego na zapisie zerojedynkowym jest od tego uzależnione, dlatego też każdy zamach na urządzenie służące do przetwarzania danych może zostać odebrane nie jako zamach na urządzenie a jako zamach na strukturę społeczną – czyli atak terrorystyczny. Tworząc regulacje prawnokarne należy pamiętać nie tylko o tym, aby były one na tyle uniwersalne, by znajdowały zastosowanie pomimo nieustannie zmieniających się realiów, lecz także by zachowania, objęte zakresem karalnościKierunek rozwoju cywilizacyjnego, jaki przyjęły obecnie społeczeństwa, w coraz większym stopniu uniezależnia się od czynnika ludzkiego, dlatego też szczególną uwagę trzeba zwrócić na kwestię edukacji – nie tylko dotyczącą stosowania technologii i korzystania z udogodnień, jakie niewątpliwie niesie ze sobą jej powszechne stosowanie. Przede wszystkim należy położyć nacisk na aspekt etyczny, na ustaleniu i utrzymaniu coraz bardziej zacierającej się granicy pomiędzy „dobrem" a „złem" – zwłaszcza w realiach systemu, w którym rola elementu ludzkiego jest coraz mniejsza. Występujące we współczesnym świecie podziały i towarzyszące temu konflikty przybierają w ostatnich latach coraz bardziej radykalne formy i coraz częściej przenoszone są na wirtualną płaszczyznę. Należy o tym pamiętać tworząc normy społecznego współżycia i prowadząc edukację przyszłych pokoleń.

Bibliografia

monografie

A. Adamski – Prawo karne komputerowe, Warszawa 2000;

A. Adamski (red.) – Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Materiały z konferencji naukowej, TNOiK, Toruń 1994;

A. Adamski – Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy, wyd. TNOiK Toruń 2001;

D. Doroziński – „Hakerzy. Technoanarchiści cyberprzestrzeni.", wyd. Helion 2001;

B. Fischer – Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne. Kantor wydawniczy „Zakamycze" 2000;

L. Gardocki – Prawo karne, wyd. C. H. Beck, Warszawa, 2001;

O. Górniok (red.) – Komentarz do Kodeksu Karnego, wyd. Lexis Nexis 2004;

J. Kosiński (red.) – Przestępczość teleinformatyczna. Materiały seminaryjne Szczytno 2004;

A. Marek – Kodeks karny. Komentarz. Dom Wydawniczy ABC, 2005, wyd. II;

M. Molski, S. Opala – Elementarz bezpieczeństwa systemów informatycznych, wyd. Mikom, Warszawa 2002;

D. Parker – Crime by Computer, New York 1976;

A. Płaza – Przestępstwa komputerowe, Rzeszów 2000;

C. Stroll – The Cuckoo's Egg; Tracking a Spy through the Maze of Computer Espionage, New York 1989;

M. Świtała – Wirusy komputerowe. analiza prawnokarna, Poznań 2001;

A. Zoll (red.), G. Bogdan, K. Buchała, Z. Ćwiąkalski, M. Dąbrowska-Kardas, P. Kardas, J. Majewski, M. Rodzynkiewicz, M. Szewczyk, W. Wróbel – Kodeks karny. Część szczególna. Komentarz do art. 177-277. Tom II, Zakamycze 1999;

akty prawne

Recommendation of the Council of the OECD concerning Guidelines for the Security of Informations Systems OECD/GD (92) 10 Paris, 1992;

Council of Europe, Computer-Related Crime : Recommendation No. R(89)9 on computer-related crime and final report of the European Committee of Crime problems, Strasbourg 1989;

Problems of Criminal Procedural Law Connected with Information Technology. Recommendation No. R(95) 13 adopted by the Committee of Ministers of the Council of Europe on 11 September 1995 and explanatory memorandum, Council of Europe Publishing, 1996;

Council of Europe – Convention on Cybercrime, Budapest 23.11.2001 r.; European Treaty Series No. 185;

Ustawa z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks Karny, ustawy – Kodeks Postępowania Karnego oraz ustawy – Kodeks Wykroczeń (Dz. U. z 2004 r. Nr 69 poz. 626);

druk sejmowy nr 2031 i druki związane; źródło – http://www.sejm.gov.pl;

Poselski „Projekt Kodeksu Karnego z 2002 r." druk sejmowy nr 387; źródło – http://www.sejm.gov.pl;

Prezydencki projekt ustawy o zmianie ustawy – Kodeks Karny z dnia 20 grudnia 2001 r. druk sejmowy nr 181; źródło – http://www.sejm.gov.pl;

Rozporządzenie Prezydenta Rzeczypospolitej z dnia 11 lipca 1932 r. – Kodeks Karny (Dz. U. z 1932 r. Nr 60 poz. 571 z późn. zm.);

Ustawa z dnia 6 czerwca 1997 r. – Kodeks Karny (Dz. U. z 1997 r., Nr 88 poz. 553 z późn. zm.);

Ustawa z dnia 19 kwietnia 1969 r. – Kodeks Karny (Dz. U. z 1969 r. Nr 13 poz. 94 z późn. zm.);

źródła encyklopedyczne

Wielka Encyklopedia PWN, Warszawa 2002;

Słownik Języka Polskiego, PWN, Warszawa 1978;

W. Kopaliński – Słownik Wyrazów Obcych i zwrotów obcojęzycznych, wyd. XVII, Warszawa 1979;

A. Marciniak, M. Jankowski – Słownik informatyczny angielsko – polski, PWN 1991;

J. Stanisławski – Wielki słownik angielsko-polski. Wiedza Powszechna 1975;

artykuły i opracowania

A. Adamski – Rządowy projekt dostosowania polskiego kodeksu karnego do Konwencji Rady Europy o cyberprzestępczości. Materiały z konferencji Secure 2003; źródło : CERT Polska, http://www.cert.pl;

A. Adamski – Prawna reglamentacja zachowań użytkowników i administratorów sieci komputerowych, materiały seminarium Secure 97; źródło : http://www.law.uni.torun.pl/KOMP-LEX/zegrze97.html

A. Adamski – Hacking a nowy kodeks karny; „Informatyka" nr 9/1998 str. 9-12, źródło : http://www.law.uni.torun.pl/KOMP-LEX/I9-98.html

J. Böttler – Threats posed by Cyber Terror and Possible Responses of the United Nations;

CERT Polska – Raport 2000. Przypadki naruszające bezpieczeństwo teleinformatyczne; źródło : http://www.cert.pl;

CERT Polska – Raport 2001. Przypadki naruszające bezpieczeństwo teleinformatyczne; źródło : http://www.cert.pl;

CERT Polska – Raport 2002. Przypadki naruszające bezpieczeństwo teleinformatyczne; źródło : http://www.cert.pl;

CERT Polska – Raport 2003. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2003; źródło : http://www.cert.pl

CERT Polska, Raport 2004 – Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w 2004 roku; źródło : CERT Polska, http://www.cert.pl;

D. E. Denning – Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, 2000; http://www.cs.georgtown.edu/~denning/infosec/cyberterror.html

S. Górniak – Robaki sieciowe – historia i studium przypadku; materiały konferencji Secure 2003 ; http://www.cert.pl;

S. Górniak – Obecne trendy w zagrożeniach sieciowych, źródło : http://www.cert.pl

K. J. Jakubski – Przestępczość komputerowa – zarys problematyki. Prokuratura i Prawo, nr 12/96, str. 34;

P. Kościelniak – Nikt nie jest bezpieczny; Rzeczpospolita z dnia 8 maja 1997 r.;.

P. Kościelniak, M. Kopyt – „Sieć apokalipsy". Elektroniczne przestępstwa; Rzeczpospolita z dnia 6 listopada 1997 r.

M. Maj – Sieć zagrożeń w sieci Internet. Raport CERT Polska 2004; http://www.cert.pl

M. Maj, P. Jaroszewski – „Bezpieczeństwo przeglądarek internetowych"; źródło : CERT Polska, http://www.cert.pl;

M. Maj – Bezpieczeństwo systemów; materiały konferencji Secure 2000; źródło : http://www.cert.pl;

M. Maj – Metoda szacowania strat powstałych w wyniku ataków komputerowych, materiały konferencji Secure 2002; źródło : CERT Polska, http://www.cert.pl;

Ministerstwo Łączności – ePolska. Plan działania na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001 – 2006 z dnia 14 czerwca 2001 r

M. Płachta – Opinia w sprawie projektu ustawy o zmianie Kodeksu karnego, Kodeksu postępowania karnego oraz kodeksu wykroczeń (druk 2031), opinia zlecona, Biuro Ekspertyz i Analiz, Gdańsk 12.01.2004

J. Siwek – Cele sił zbrojnych – zdolność reagowania na incydenty komputerowe; materiały konferencji Secure 2003; źródło : CERT Polska, http://www.cert.pl;

U. Sieber – Przestępczość komputerowa, a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka, Przegląd Policyjny, Nr 3(39)/95;

P. Waglowski – Spam ofensywny seksualnie;

J. Wierzbołowski, referat na konferencji naukowej „Integracja europejska wobec wyzwań ery informacyjnej (proindustrialnej)" zorganizowanej przez Centralny Urząd Planowania oraz Instytut Rozwoju i Studiów Strategicznych;

W. Wiewiórowski – Profesjonalny haker. Paradoks odpowiedzialności karnej za czyny związane z ochroną danych i systemów komputerowych. Materiały z konferencji naukowej „Bezpieczeństwo sieci komputerowych a hacking. Internetki V, Lublin, 4-5 marca 2005", wyd. UMCS, Lublin 2005

W. Wróbel – Przestępstwa przeciwko ochronie informacji, Rzeczpospolita Nr 206 (3550) z dnia 3 września 1993 r.

„Łapią hakerów z Warez City" – Gazeta Wyborcza, nr 198. 4712 z dnia 24 sierpnia 2004 r.;

źródła internetowe

„1999 Report on Cyberstalking : A new challenge for law enforcement and industries", http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

S. Gibson – Distributed Reflection Denial of Service. Description and analysis of a potent, increasingly prevalent, and worrisome Internet attack; http://grc.com/dos/drdos.htm;

Hobbes' Internet Timeline – the definitive ARPAnet & Internet history v5.6; http://www.zakon.org/robert/internet/timeline/

Kerberos – Zagrożenia bezpieczeństwa i przedmioty ochrony w systemie informatycznym. Modele bezpieczeństwa; źródło : http://kerberos.w.pl;

B. Szewczyk – Przestępstwa internetowe; http://stud.wsi.edu.pl/~dratewka/crime/przestepczosc.htm;

P. Waglowski – Aby spać mógł ktoś; http://www.vagla.pl/felietony/felieton_050.htm;

P. Waglowski – And justice for all dot com; http://www.vagla.pl/felietony/felieton_001.htm;

P. Waglowski – Nadchodzi czas wielkiej kwarantanny; źródło : http://www.vagla.pl/felietony/felieton_062.htm

P. Waglowski – Wirtualny terror; http://www.vagla.pl/felietony/felieton_040.htm

The Internet Worm of 1988; http://world.std.com/~franl/worm.html

http://gicek.tripod.com/

http://hacking.pl/articles.php?id=56

http://www.biznesnet.pl/pp/16066/Aresztowany-za-spam-na-komunikatory

adresy WWW

http://www.vagla.pl;
http://www.cert.pl;
http://kerberos.w.pl;
http://www.sejm.gov.pl;
http://www.ws-webstyle.com/cms.php/en/netopedia/;
http://www.cybercrimelaw.net/tekster/international_agencys.html;
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=04/11/2005&CL=ENG;
http://hacking.pl;
http://hack.pl;