DAWID WACHAŁOWICZ

Internet jako źródło zagrożeń bezpieczeństwa i porządku publicznego

Pod koniec lat pięćdziesiątych Departament Obrony Stanów Zjednoczonych Ameryki Północnej powołał do życia agencję ARPA[1], która w roku 1967, we współpracy z ośrodkami akademickimi, rozpoczęła prace nad projektem zdecentralizowanej sieci komputerowej. Głównym celem prac było stworzenie sieci połączeń, która nie będzie posiadała swoistego centrum, a jej głównym atutem będzie możliwość zachowania działania, nawet w przypadku uszkodzenia znaczącej części infrastruktury technicznej. Tak powstała wojskowo-akademicka sieć ARPANET, którą można uznać za protoplastę obecnego Internetu.

Obecnie Internet jest jednym z najważniejszych mediów. Wykształcenie się oraz stały rozwój społeczeństwa informacyjnego, zapoczątkowały poważne zmiany w zakresie wymiany informacji, a także świadczenia komercyjnych usług. Internet jest największą siecią komputerową o globalnym zasięgu, która stworzyła możliwości szybkiego dostępu do informacji, zasobów rozrywkowych, usług komercyjnych; bankowości elektronicznej, handlu online, platform aukcyjnych itp. W związku z rozwojem technologii teleinformacyjnej tworzone są nowe miejsca pracy, świadczone nowe usługi, dostęp do materiałów naukowych stał się zdecydowanie bardziej powszechny niż dawniej.

Pomimo wielu zalet Internetu, stanowi on również poważne źródło zagrożeń dla bezpieczeństwa i porządku publicznego. Łatwość dostępu do sieci oraz częściowa anonimowość, jaką oferuje

[1] Ang. Advanced Research Project Agency – Agencja Zaawansowanych Projektów Badawczych.

Internet, bywają bardzo często wykorzystywane przez przestępców i to właśnie one są motorem napędzającym ich działania.

Obecnie można zauważyć tendencję do zamiennego stosowania pojęć „przestępstw internetowych" i „przestępstw komputerowych". Jednym z zadań niniejszej pracy jest wprowadzenie pewnego rozgraniczenia pomiędzy te dwie formy przestępczości. O ile przestępstwa internetowe zawierają się rodzajowo w grupie przestępstw komputerowych, ponieważ aby zaistniały musi dojść do nadużyć za pośrednictwem lub w stosunku do elektronicznych systemów przetwarzania informacji; o tyle przestępstwa komputerowe są grupą szerszą, ponieważ do ich zaistnienie nie jest wymagany dostęp do sieci teleinformatycznej. Na potrzeby niniejszej pracy pod pojęciem cyberprzestępczości należy rozumieć, zarówno przestępstwa komputerowe jak i ich węższą rodzajową grupę – przestępstwa internetowe. Założenie to wynika z braku legalnej definicji na gruncie polskiego prawa pojęć takich jak przestępczość komputerowa, przestępczość internetowa oraz cyberprzestępczość.

Pomimo istniejącego od kilkudziesięciu lat problemu związanego z tym szczególnym rodzajem przestępczości, do dzisiaj nie powstała jego uniwersalna, normatywna definicja. Na gruncie polskich ustaw, w tym ustawy szczególnej jaką jest Kodeks karny z 1997 roku, nie występuje legalna definicja pojęć, takich jak „przestępczość komputerowa", „przestępczość internetowa" czy stosowana zamiennie do dwóch ww. cyberprzestępczość, a jedynie katalog czynów zabronionych zaliczanych do tego rodzaju przestępstw. Zdefiniowania tego problematycznego pojęcia podejmują się zarówno kryminolodzy, teoretycy i analitycy problemu, jak również wiele organizacji i instytucji.

W ocenie autora głównym problemem unormowania pojęcia jest niezwykle szybki rozwój technologii informacyjnej. Próba stworzenia katalogu przestępstw określanych jako „przestępstwa komputerowe" wymaga stałej ich aktualizacji w oparciu o analizę nowych form przestępczych, które pojawiają się równocześnie z rozwojem zarówno infrastruktury technicznej, jak i rozwojem

możliwości programistycznych. Nowe rozwiązania i usługi świadczone drogą internetową niosą za sobą ryzyko modyfikacji i ekspansji działań przestępczych. Z drugiej strony należy zaznaczyć, że próba zawarcia pojęcia „przestępstw komputerowych" w sztywnej i ogólnej konstrukcji zdaniowej może skutkować próbą modyfikacji działań przestępczych w taki sposób, aby nie nosiły znamion czynu zabronionego określonego w normie. Kolejnym problemem związanym ze stworzeniem jednolitej definicji pojęcia jest międzynarodowy charakter cyberprzestępczości. Należy dążyć do stworzenia zunifikowanego, wyczerpującego, normatywnego zdefiniowania pojęcia, które obowiązywało będzie na arenie międzynarodowej, aby w sposób skuteczny ścigać sprawców przestępstw komputerowych.

Na potrzeby pracy, pojęcia „przestępczości i przestępstw komputerowych" zostały określone jako zjawisko dotyczące nadużyć za pośrednictwem lub w stosunku do elektronicznych systemów przetwarzania informacji, w których te systemy są jednym ze środków umożliwiających popełnienie czynu zabronionego lub są przedmiotem zamachu. Jest to podstawowy podział przestępstw komputerowych: na przestępstwa komputerowe *sensu stricte* i *largo*.

Cyberprzestępcy posiadają obecnie potężny arsenał środków i rozwiązań technicznych oraz programistycznych, które ze znaczną skutecznością stosują przy dokonywaniu zarówno najprostszych włamań komputerowych, jak i poważnych przestępstw. Należy do nich zaliczyć w szczególności złośliwe oprogramowanie: wirusy komputerowe, konie trojańskie, rootkity, tylne wejścia, bomby logiczne, spyware, robaki sieciowe, exploity, ataki Atak DDoS[2], botnety. Przestępcy osiągają swoje cele również poprzez wykorzystywanie technik zawierających metody bazujące na inżynierii społecznej takich jak phishing czy pharming.

Modyfikacja, wzajemne nakładanie się i krzyżowanie sposobów działań sprawców, uniemożliwiają stworzenie jednorodnej i klasycznej metodologii. Rzadko zdarza się, aby sprawcy posługi-

[2] Ang. Distributed Denial of Service – rozproszona odmowa usług.

wali się jedynie określoną techniką działań. Cyberprzestępcy wykorzystują w swoim procederze różne konfiguracje i kolejności stosowanych środków i sposobów.

Niska świadomość zagrożeń cyberprzestępczością, a także często jedynie podstawowy zakres wiedzy informatycznej użytkowników Internetu, doprowadzają do sytuacji, w których osoby poszkodowane są nieświadome, że stały się ofiarami przestępstw komputerowych. Problemem w dokładnym przedstawieniu poziomu przestępczości internetowej, w poszczególnych obszarach, jest również fakt, iż wielu użytkowników sieci nie zgłasza tego rodzaju przestępstw odpowiednim organom, uważając że wykrycie sprawcy nie jest możliwe.

Według danych opublikowanych przez Europejski Urząd Policji z cyberprzestępczością zetknęło się w 2012 roku prawie 400 mln osób[3]. Wyższy wskaźnik, bo aż 556 mln dorosłych użytkowników Internetu (w tym 7,2 mln Polaków) dotkniętych przestępczością internetową, przedstawia Norton Cybercrime Report 2012. Według raportu, cyberprzestępczość wymierzona w konsumentów, wygenerowała koszty bezpośrednie rzędu 110 mld dolarów (w Polsce 4,8 mld zł)[4]. Faktyczna liczba przestępstw komputerowych oraz poziom strat przez nie spowodowanych, są niezwykle trudne do oszacowania.

Oszustwa komputerowe są obecnie najpowszechniejszym rodzajem przestępstw internetowych. W większości przypadków, głównym obszarem działalności cyberprzestępców dokonujących oszustw są platformy aukcyjne, sklepy internetowe, systemy bankowości online, a nawet systemy społecznościowe takie jak np. Facebook, Twitter. Obecnie niektóre rodzaje złośliwego oprogramowania, takie jak np. aplikacja „Zeus", która za pośrednictwem komputera instaluje się również na telefonie komórkowym, w trakcie wymiany informacji między komputerem a telefonem, posia-

[3] Http://di.com.pl/news/46940,0,Rok_2012_byl_pelen_....html, [Online], 2012 [dostęp: 8 marca 2013].

[4] Http://www.symantec.com/pl/pl/about/news/release/20120925_, [Online], 2013 [dostęp: 9 marca 2013].

dają możliwość przechwytywania i dalszego przekazywania treści SMSów autoryzujących, wysyłanych np. z systemów bankowych[5].

W zakresie oszustw internetowych warto również zwrócić uwagę na poważny problem jakim jest scamming. Zjawisko to polega na wzbudzeniu zaufania ofiary, w celu wyłudzenia korzyści finansowych. Proceder przestępczy w tym przypadku bazuje na wykorzystywaniu emocji takich jak np. chciwość czy empatia. Scenariuszy scammingu jest wiele. Oszustwa te dotyczą piramid finansowych, fałszywych loterii i konkursów, ofert i poradników przedstawiających sposoby na szybkie wzbogacenie się. Szczególnym rodzajem scammingu jest tzw. „nigeryjski szwindel", w przypadku którego drogą mailową wysyłane są do potencjalnych ofiar wiadomości zawierające prośbę o pomoc, w zamian za znaczne korzyści materialne.

Cyberkradzieże również stanowią stale rozwijający się obszar przestępczości internetowej. Różnica między cyberoszustwem, a cyberkradzieżą polega na tym, że w przypadku oszustwa, wprowadzony w błąd poszkodowany dobrowolnie i świadomie przekazuje sprawcy środki finansowe lub majątkowe. Do kradzież komputerowych dokonywanych za pośrednictwem Internetu należy zaliczyć: malwersacje, nieuprawnione przywłaszczenie, szpiegostwo przemysłowe, plagiat oraz piractwo komputerowe[6]. Nie ulega wątpliwości, że obecnie w obszarze cyberkradzieży, najpowszechniejszą grupę przestępstw stanowią te, dotyczące piractwa komputerowego.

Programy komputerowe, utwory muzyczne, produkcje filmowe, a także inne pliki stanowiące własność intelektualną, chronione prawem autorskim rozpowszechniane są za pośrednictwem sieci P2P[7] oraz serwisów i forów internetowych typu warez. O skali zjawiska w tym przypadku może świadczyć fakt ogromnej

[5] Http://webhosting.pl/Trojan.ZeuS.dla.Androida.powraca.i.udaje.program.antywirusowy, [Online], 2012 [dostęp: 9 marca 2013].

[6] B. Hołyst, J. Pomykała, dz. cyt., s. 18.

[7] Ang. Peer-to-Peer – schemat komunikacji sieciowej, który zapewnia wszystkim połączonym w sieci komputerom te same uprawnienia.

popularności stron warezowych. Według badań zleconych przez Business Software Alliance, ilość samego tylko nielegalnego oprogramowania w Polsce wynosi aż 53%, a jego wartość 618 mln dolarów. Należy zaznaczyć, że „crackerzy" łamiący zabezpieczenia poszczególnych programów, często umieszczają w ich kodzie „tylne wejścia" lub rozpowszechniają je z innym rodzajem złośliwego oprogramowania, w rezultacie czego osoby pobierające i korzystające z pirackich wersji oprogramowania komputerowego narażają własny system na infekcję.

Poważny problem związany z ogólnodostępnymi zasobami internetowymi stanowią obraźliwe i nielegalne treści. Znacząca liczba incydentów, zaliczanych do tego obszaru, dotyczyła rozsyłania niechcianej korespondencji mailowej – spamu[8]. W internetowych zasobach można spotkać treści pochwalające przemoc, nawołujące do nienawiści, treści o charakterze rasistowskim, ksenofobicznym, antysemickim, pornograficznym (twarda pornografia lub pornografia dostępna bez ostrzeżenia o wymogach pełnoletniości), a także treści o charakterze pedofilskim[9]. Strony internetowe zawierające tego rodzaju zakazane treści, z reguły umieszczane są na serwerach zlokalizowanych w państwach, których system prawny nie penalizuje publikowania takich informacji.

Znaczącym obszarem cyberprzestępczości są włamania do komputerów osobistych, serwerów i stron internetowych, mające na celu skasowanie, zmianę lub skopiowanie określonych treści, a także ataki typu DoS, których celem jest zablokowanie określonej usługi sieciowej, a więc przestępstwa komputerowe sensu stricte. W ostatnich latach można zauważyć tendencję do wykorzystywania różnych form „hackingu" w przestępczym procederze, jako formy obywatelskiego nieposłuszeństwa i sprzeciwu wobec działań administracji publicznej. W 2012 roku bardzo duża ilość ataków na serwery rządowe, spowodowana była sprzeciwem internetowej społeczności w stosunku do planowanego podpisa-

[8] CERT Polska, Raport Roczny CERT Polska 2011, s. 26.

[9] Kwestię tę omawia się w podrozdziale 2.2.

nia przez Polskę umowy ACTA[10]. Ataki DDoS doprowadziły do niestabilnego działania stron służb bezpieczeństwa takich jak Policja i ABW[11]. W wyniku włamań została zmieniona zawartość strony internetowej m.in. Kancelarii Prezesa Rady Ministrów[12]. Ofiarą ataku padł również prywatny laptop wiceministra cyfryzacji Igora Ostrowskiego[13]. „Hackerzy" zadeklarowali się, że w przypadku podpisania przez Polskę umowy ACTA, opublikują rzekomo posiadane hasła do rządowych skrzynek elektronicznych oraz fragmenty innych baz danych. Powołany 1 lutego 2008 r. Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL[14], w odniesieniu do znacznej liczby ataków „hackerskich", bardzo dokładnie zbadał poziom bezpieczeństwa 30 stron w domenie gov.pl[15]. Jak wynika z raportu za pierwszy kwartał 2012, stwierdzono 454 błędy, z których 74 powodowały bardzo wysoki poziom zagrożenia

Znaczna część wyłudzeń i oszustw internetowych dotyczy spraw, w których ofiarą są osoby małoletnie. Sprawcy wykorzystują ich niską świadomość społeczną, łatwowierność oraz otwartość na nowe kontakty. Najpoważniejszą jednak formą przestępstw internetowych w stosunku do osób małoletnich, jest dziecięca pornografia oraz nawiązywanie przez pedofilów za pośrednictwem Internetu kontaktów z małoletnimi. Według szacunków, w zasobach internetowych znajduje się ponad milion zdjęć i filmów z pornografią dziecięcą. Statystycznie co rok pojawia się 50

[10] Ang. Anti-Counterfeiting Trade Agreement – Umowa handlowa dotycząca zwalczania obrotu towarami podrabianymi – porozumienie, wprowadzające międzynarodowe standardy w walce z naruszeniami własności intelektualnej.

[11] Http://niezalezna.pl/22307-hakerzy-znow-atakuja-ujawniaja-dane, [Online], 2012 [dostęp: 21 marca 2013].

[12] Http://www.rp.pl/artykul/797013.html, [Online], 2012 [dostęp: 21 marca 2013].

[13] Http://www.gazetaprawna.pl/wiadomosci/artykuly/587082,rzad_ zapomnial_o_cyberbezpieczenstwie.html, [Online], 2012 [dostęp: 21 marca 2013].

[14] CERT.GOV.PL funkcjonuje w ramach Departamentu Bezpieczeństwa Teleinformatycznego ABW, natomiast CERT Polska funkcjonuje w ramach NASK.

[15] Takim rozszerzeniem domenowym oznaczane są polskie strony rządowe.

tysięcy nowych materiałów. 70% wykorzystywanych dzieci ma mniej niż 10 lat[16].

Obecnie bardzo poważny problem stanowią sieci i fora TOR[17], które wykorzystywane są również do rozpowszechniania treści pedofilskich. Sieć TOR ma za zadanie zapewnić jak największy poziom anonimowości użytkownika, który z niej korzysta, uniemożliwiając tzw. analizę ruchu sieciowego[18]. Działanie tej sieci polega na wielokrotnym szyfrowaniu wiadomości oraz przesyłaniu jej przez szereg węzłów zwanych „routerami cebulowymi", które usuwają warstwę szyfrowania, w celu uzyskania informacji o dalszym trasowaniu i przesyłają dane do kolejnego routera w sieci. Takie działanie zapobiega ujawnieniu poszczególnym węzłom pośredniczącym pochodzenia, odbiorcy oraz treści wiadomości[19]. Pedofile działający za pośrednictwem sieci komputerowych wykorzystują TOR nie tylko do ukrywania swoich adresów IP w sieci Internet, ale także w celu korzystania z ukrytych i anonimowych usług, które nie są dostępne bezpośrednio w sieci Internet. Fora dyskusyjne publikowane za pośrednictwem The Onion Router zawierają wiele szokujących i bulwersujących treści. Publikowane są tam nie tylko zdjęcia i materiały wideo, zawierające dziecięcą pornografię, ale także porady opisujące jak skutecznie uwodzić dzieci, opisy doświadczeń oraz wiele podobnych skandalicznych treści[20]. Techniczne namierzenie przestępców, którzy w swoich działaniach korzystają z sieci TOR, jest obecnie niezwykle trudne, a często niemożliwe.

---

[16] Http http://www.euractiv.pl/wersja-do-druku/artykul/ue-walczy-z-pornografi-dziecic-w-internecie-004265, [Online], 06.12.2012 [dostęp: 21 marca 2013].

[17] Ang. The Onion Router – sieć wykorzystująca trasowanie „cebulowe".

[18] Https://www.torproject.org/about/overview.html.en, [Online], [dostęp: 21 marca 2013].

[19] Http://www.naukowy.pl/encyklo.php?title=Trasowanie_cebulowe, [Online], [dostęp: 21 marca 2013].

[20] Http://natemat.pl/32267,najciemniejszy-zakatek-internetu-naprawde-istnieje-ukryta-siec-tor-lewe-papiery-pedofilia-przekrety-i-narkotyki, [Online] 2012, [dostęp: 22 marca 2013].

Bardzo poważnymi zagrożeniami są włamania internetowe i wycieki baz danych międzynarodowych korporacji, a także stron rządowych. W pierwszej połowie 2011 roku doszło do wycieku bazy danych firmy SONY. Włamywacze uzyskali dostęp do danych, ponad 100 milionów kont użytkowników, a także prawdopodobnie do 10 milionów kart kredytowych. Cyberwłamywacze uzyskali również dostęp do danych kont użytkowników firm takich jak Nintendo i Codemasters, a także 200 tysięcy kont Citibanku[21].

Na gruncie zagrożeń cybernetycznych należy przedstawić zjawisko cyberterroryzmu oraz wojen internetowych, określanych jako „i-War" lub cyberwojna. Prowadzone są one w cyberprzestrzeni przy pomocy dysponujących specjalistyczną wiedzą „hackerów". Według ekspertów Światowego Forum Gospodarczego w nadchodzącym dziesięcioleciu o 10 proc. wzrośnie ryzyko wystąpienia poważnego zakłócenia krytycznej infrastruktury teleinformatycznej powodującego straty gospodarcze o wartości ponad 200 mld dolarów[22].

Podstawowym aspektem przeciwdziałania cyberprzestępczości, który jak w każdym przypadku przestępczości, stanowi fundament do zwalczania określonych zjawisk, jest penalizacja konkretnych czynów, których szkodliwość destrukcyjnie wpływa na bezpieczeństwo sieci komputerowych i jej użytkowników. Na gruncie polskiego prawodawstwa, kluczową rolę w zakresie kryminalizacji szkodliwych zachowań, względem oraz za pośrednictwem elektronicznych systemów przetwarzania danych, stanowi Kodeks karny. Przestępstwa komputerowe *sensu stricte*, czyli te, w których przedmiotem zamachu jest sieć lub system informatyczny, zostały ujęte w rozdziale XXIII Kodeksu karnego, dotyczącym przestępstw przeciwko ochronie informacji.

Znaczna grupa czynów zabronionych, noszących znamiona przestępczości komputerowej, to tradycyjne przestępstwa dokonywane za pośrednictwem elektronicznych systemów przetwa-

[21] CERT Polska, Raport Roczny CERT Polska 2011, s. 6.

[22] Http://di.com.pl/news/46940,0,Rok_2012_byl_pelen_....html, [Online], 2012 [dostęp: 18 stycznia 2013].

rzania informacji. Przykładem może być regulowana w art. 200, 200a, 202 k.k. pedofilia i pornografia dziecięca[23]. Obecna skala tego zjawiska skłoniła ustawodawcę do posłużenia się w art. 200a pojęciami systemu teleinformatycznego oraz sieci telekomunikacyjnej. W zakresie zwalczania wszechobecnego w Internecie piractwa komputerowego, prawny fundament stanowi ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.

Skutki czynów zabronionych, dokonywanych za pośrednictwem Internetu, mogą wystąpić nie tylko na wielu płaszczyznach, ale również w wielu państwach. Biorąc pod uwagę transgraniczny charakter cyberprzestępczości należy dążyć do wypracowania wspólnej, międzynarodowej polityki legislacyjnej.

Zasadniczym dokumentem w zakresie zwalczania przestępczości komputerowej na europejskim gruncie jest Konwencja Rady Europy o Cyberprzestępczości, podpisana przez Polskę w Budapeszcie 23 listopada 2001 r.[24] Do chwili obecnej konwencja nie została ratyfikowana przez stronę polską, jednakże wniosła znaczący wkład na płaszczyźnie działań legislacyjnych polskich organów ustawodawczych.

Prowadzenie kampanii społecznych o charakterze edukacyjno-prewencyjnym jest jednym z głównych założeń Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2011–2016. Społeczne kampanie proedukacyjne w zakresie przeciwdziałania cyberprzestępczości promują właściwą postawę moralną w odniesieniu do czynów kryminalnych popełnianych za pośrednictwem sieci komputerowych, a także przedstawiają poważne zagrożenia, których źródłem może być Internet.

Z inicjatywy Departamentu Bezpieczeństwa Teleinformatycznego ABW oraz działającego w ramach NASK zespołu CERT Polska, został stworzony system wczesnego ostrzegania o zagrożeniach w sieci – ARAKIS[25], którego celem jest *wykrywanie i opisywanie zautomatyzowanych zagrożeń występujących w sieci na pod-*

[23] Kwestię tę omawia się w podrozdziale 2.2.

[24] Tamże, s. 62.

[25] Skrót od – Agregacja, Analiza i Klasyfikacja Incydentów Sieciowych.

stawie agregacji i korelacji danych z różnych źródeł, w tym rozproszonej sieci honeypotów[26]*, sieci darknet*[27]*, firewalli oraz systemów antywirusowych*[28]*.*

W zakresie zapewnienia bezpieczeństwa danych, przesyłanych za pośrednictwem Internetu, ważny element stanowią zabezpieczone kryptograficznie protokoły komunikacyjne, takie jak np. HTTPS, czyli szyfrowana za pośrednictwem protokołu SSL[29] wersja protokołu HTTP[30].

Istotnymi problemami w zakresie wykrywania sprawców przestępstw komputerowych dokonywanych za pośrednictwem Internetu, są hermetyka środowisk „hackerskich", automatyzacja działania złośliwego oprogramowania, ciągła modyfikacja metod i sposobów działań przestępczych oraz stały rozwój technologii informacyjnej, jednakże najpoważniejszym czynnikiem, który w wielu przypadkach całkowicie uniemożliwia wykrycie sprawców, jest stosowanie przez przestępców oprogramowania zapewniającego znaczny poziom anonimowości w sieci.

Pomimo występowania znacznej ilości czynników utrudniających wykrywanie sprawców przestępstw komputerowych, organy ścigania korzystając z tradycyjnych metod pracy operacyjno-rozpoznawczej i dochodzeniowo-śledczej, a także z rozwoju technologii informacyjnej oraz rozwoju dziedziny nauk sądowych jaką jest informatyka śledcza, odnoszą szereg sukcesów w zakresie ujawniania czynów zabronionych dokonywanych za pośrednictwem komputerów i sieci teleinformatycznych oraz wykrywania ich sprawców. Działania te wymierzone są nie tylko w powszech-

[26] Ang. honey, pot – miód, garnek – miejsce sieciowe będące w rzeczywistości pułapką, którego celem jest wykrycie wszelkich prób wykrycie prób nieautoryzowanego dostępu do systemu i danych.

[27] Ang. dark net – ciemna sieć – miejsca tworzone w sieciach takich jak np. TOR, zawierające treści i materiały o charakterze przestępczym.

[28] Rządowy Program Ochrony…, dz. cyt., s. 13.

[29] Ang. Secure Sockets Layer – ustandaryzowany zestaw wcześniej znanych algorytmów, technik i schematów szyfrowania danych.

[30] Ang. Hypertext Transfer Protocol – protokół przesyłania dokumentów hipertekstowych stosowany w usłudze WWW.

ną przestępczość komputerową, taką jak np. oszustwa internetowe, ale również w najpoważniejsze rodzaje przestępstw dokonywanych za pośrednictwem Internetu, takich jak pedofilia, handel bronią i amunicją, handel narkotykami i środkami psychoaktywnymi, handel organami ludzkimi, cyberterroryzm.