

Międzynarodowa współpraca w zwalczaniu cyberprzestępczości

Streszczenie: Internet jest doskonałym narzędziem wykorzystywanym przez cyberprzestępców, w tym cyberterrorystów. W artykule autorzy przedstawili inicjatywy podejmowane w ostatnich latach na szczeblu międzynarodowym w celu zwalczania cyberprzestępczości. Bazując na międzynarodowych aktach prawnych definiujących cyberprzestępczość omówili działania organizacji Europejskich i policyjnych zmierzające do podniesienia bezpieczeństwa w Internecie.

Abstract: The Internet is an excellent tool used by cyber-criminals, including cyber-terrorists. The authors present initiatives undertaken in recent years at international level to combat cyber-crime. Based on international legal instruments that define cyber-crime activities they discuss European and Police organizations aimed at increasing Internet safety.

W wielu publikacjach i wystąpieniach na konferencjach ich autorzy prezentują pogląd, że cyberprzestrzeń, a wraz z nią nowy typ zagrożenia, czyli cyberprzestępczość, narodziła się w momencie powstania politycznej koncepcji „autostrad informacyjnych”, w czasie kampanii prezydenckiej Billa Clintona, w 1992 roku. Koncepcja ta zakładała, że wszelkiego typu informacje zawierające tekst, dźwięk i obraz będą mogły być przekazywane na duże odległości szybko i bez przeszkód. Świat globalnej sieci coraz bardziej się rozrastał i stawał się coraz bardziej podobny do świata rzeczywistego, dlatego też różne zjawiska istniejące „w realu”, w tym przestępczość, a także terroryzm znalazły swoje miejsce w przestrzeni wirtualnej¹. Kiedyś, przed laty, również Stanisław Lem napisał, że "większość technologii ma świetlisty awers, ale życie dało im rewers - czarną rzeczywistość". To zdanie z całą pewnością można odnieść do cyberprzestrzeni, do Internetu. Cyberprzestępcy zadomowili się w Internecie, widząc w nim miejsce, gdzie łatwiej i przy mniejszym ryzyku poniesienia konsekwencji można funkcjonować. Policyjne statystyki cyberprzestępczości wskazują na jej niewielki trend wzrostowy. Nie są to jednak statystyki dające rzetelny obraz tego zjawiska. Trochę inaczej, gorzej widzą tę tendencję międzynarodowe koncerny informatyczne oraz organizacje zajmujące się bezpieczeństwem w Internecie. To spojrzenie znalazło swoje odzwierciedlenie także na płaszczyźnie politycznej. Przykładem może być „Strategia Komisji Europejskiej nt. zwalczania cyberprzestępczości” z listopada 2008 oraz polski „Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011” z marca 2009. W obu dokumentach znalazły się zapisy mówiące o wymogu zorganizowania współpracy organów ścigania z sektorem prywatnym oraz w wymiarze międzynarodowym w celu skutecznego zwalczania cyberprzestępczości.

Mimo upływu prawie ośmiu lat od podpisania Konwencji Rady Europy o cyberprzestępczości², ciągle pojęcie cyberprzestępczości nie jest pojęciem jednoznacznym. Warto przypomnieć, że Konwencja zawiera szereg zapisów, które:

- nakazują traktowanie umyślnego dostępu do całości albo części systemu informatycznego bez uprawnienia jako przestępstwo (artykuł 2),
- nakazują penalizowanie umyślnego i bez uprawnienia przechwytywania transmisji danych informatycznych z, do, albo w obrębie systemu informatycznego (artykuł 3),

¹ Np. prof. Ryszard Tadeusiewicz

² Council of Europe Convention on Cybercrime, Budapest 23.11.2001 – ETS 185

- zakazują umyślnego i bez uprawnienia uszkodzenia, usuwania, niszczenia, zmiany lub blokowania danych informatycznych (artykuł 4),

- uznają umyślne spowodowanie zakłócenia w funkcjonowaniu systemu informatycznego na skutek wprowadzenia, przesłania, uszkodzenia, usunięcia, zniszczenia, lub zablokowania danych informatycznych bez uprawnienia za przestępstwo (artykuł 5),

- zakazują wytwarzania, sprzedaży, uzyskania w celu używania, sprowadzania, rozpowszechniania lub udostępniania w inny sposób wszelkich środków, w tym także programów komputerowych zaprojektowanych lub przystosowanych do popełniania przestępstw z artykułów 2-5 konwencji. Powyższy zakaz dotyczy także haseł, kodów dostępu lub innych podobnych danych umożliwiających dostęp do systemu komputerowego lub jego części w zamiarze popełnienia przestępstw z artykułów 2-5 (artykuł 6).

Konwencja o cyberprzestępczości, oprócz wprowadzenia nakazu ścigania przestępstw przeciwko poufności, integralności i dostępności danych i systemów komputerowych, zobowiązuje państwa-strony do wprowadzenia środków ustawodawczych i innych, niezbędnych do uznania w prawie krajowym za przestępstwo:

- umyślnego i bez uprawnienia wprowadzenia, modyfikacji, usunięcia lub zablokowania danych komputerowych, w wyniku czego powstają dane nieautentyczne, które mogą być uznane i wykorzystane jako autentyczne (art. 7 – fałszerstwo komputerowe),

- umyślnego spowodowania utraty własności przez inną osobę na skutek wprowadzenia, modyfikacji, usunięcia lub zablokowania danych komputerowych lub innej ingerencji w funkcjonowanie systemu informatycznego w oszukańczym lub nieuczciwym zamiarze uzyskania bezprawnych korzyści ekonomicznych (art. 8 – oszustwo komputerowe),

- czynów zabronionych związanych z pornografią z udziałem małoletnich, które polegają na:

- wytwarzaniu w celu jej rozpowszechniania,
- oferowaniu i udostępnianiu,
- rozpowszechnianiu i przesyłaniu,
- pozyskiwaniu dla siebie lub innej osoby,
- posiadaniu w systemie informatycznym lub na nośnikach danych.

Uzupełnieniem Konwencji jest Protokół Dodatkowy do Konwencji³ zakazujący szerzenia w cyberprzestrzeni nienawiści na tle rasowym i treści ksenofobicznych. W praktyce, konwencyjny termin cyberprzestępczość odnosi się do trzech rodzajów przestępstw. Pierwszy obejmuje tradycyjne formy przestępstw, takie jak oszustwo czy fałszerstwo, jednak w kontekście cyberprzestępczości dotyczy przestępstw popełnionych przy użyciu elektronicznych sieci informatycznych i systemów informatycznych. Drugi rodzaj stanowi publikacja nielegalnych treści w mediach elektronicznych (np. materiałów związanych z seksualnym wykorzystywaniem dzieci, czy też nawoływaniem do nienawiści rasowej). Trzeci rodzaj obejmuje przestępstwa typowe dla sieci łączności elektronicznej, tj. ataki przeciwko systemom informatycznym, np. ataki typu DoS (*denial of service*), włamania do systemów komputerowych, pharming, naruszenie integralności systemów informatycznych, itp. Tego rodzaju ataki mogą być również skierowane przeciwko najważniejszym infrastrukturom krytycznym w Europie i uszkodzić istniejące systemy szybkiego reagowania w wielu obszarach, co może spowodować dramatyczne konsekwencje dla całego społeczeństwa. W Konwencji o cyberprzestępczości jest wymieniona jeszcze czwarta kategoria cyberprzestępstw - „cyfrowe” zwielokrotnianie i rozpowszechnianie utworów lub wykonan artystycznych bez zgody osoby uprawnionej w celu uzyskania korzyści.

Na poziomie Unii Europejskiej przyjęte zostały inne akty prawne odnoszące się do cyberprzestępczości. Niektóre dotyczą konkretnego aspektu cyberprzestępczości, jak np.

³ Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.01.2003 – ETS 189

decyzja ramowa 2005/222/WSiSW w sprawie ataków na systemy informatyczne. Decyzja nakazuje penalizację: umyślnego, bezprawnego dostępu do całości lub części systemu informatycznego (art. 2), umyślnego, bezprawnego, poważnego naruszenia lub przerwania funkcjonowania systemu informatycznego poprzez wprowadzanie, przekazywanie, uszkodzanie, usuwanie, niszczenie, zmienianie, zatajanie lub uczynienie niedostępnymi danych komputerowych (art. 3) oraz umyślnego, bezprawnego usunięcia, uszkodzenia, pogorszenia, zmiany, zatajania lub uczynienia niedostępnymi danych komputerowych w systemie informatycznym (art. 4) - przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi. Decyzja wymaga karania także osób kierujących popełnieniem przestępstwa, pomagających w jego popełnieniu lub nakłaniających do jego popełnienia (podżeganie) oraz zakłada karalność usiłowania popełnienia przestępstwa (co jest bardzo często spotykanym przypadkiem w cyberprzestępczości).

Inne akty prawne, odnosząc się do konkretnego problemu przestępczości, zawierają zapisy dotyczące bezprawnego wykorzystywania Internetu, jak np. Decyzja Ramowa 2004/68/WSiSW w sprawie ochrony dzieci. Decyzja Ramowa 2001/413/WSiSW z dnia 28 maja 2001 r. w sprawie walki z oszustwami i fałszerstwami dotyczącymi bezgotówkowych środków płatności (dotycząca m.in. kradzieży tożsamości). Dyrektywa 2002/58/WE o prywatności i łączności elektronicznej nakłada na dostawców usługi dostępu do Internetu obowiązek zapewnienia bezpieczeństwa ich usług. Również stworzenie w 2004 roku Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) stanowiło postęp, jeśli chodzi o uświadomienie państwom członkowskim i obywatelom europejskim wyzwania, jakim jest zapewnienie bezpieczeństwa systemów informatycznych, aby możliwe było wypracowanie na poziomie europejskim podstaw wspólnych praktyk w zakresie zabezpieczania systemów informatycznych. Zagadnienie to zostało również poruszone w siódmym ramowym programie badawczym UE.

W komunikacie Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 2007 r. zatytułowanym „W kierunku ogólnej strategii zwalczania cyberprzestępczości”⁴ jako cyberprzestępstwa wymienione zostały:

- przestępstwa przeciwko poufności, integralności i dostępności danych (tzw. przestępstwa CIA). Do tych przestępstw zaliczamy głównie nielegalny dostęp do systemów poprzez hacking, podsłuch i oszukiwanie uprawnionych pracowników, szpiegostwa komputerowe, sabotaż oraz wymuszenia komputerowe (wirusy, ataki DoS, DDoS, spam),
- przestępstwa tradycyjne powiązane z komputerami, takie jak oszustwa (od klasycznych oszustw manipulacji fakturami lub kontami firmowymi, do manipulacji online - oszukańczych aukcji czy nielegalnego używania kart kredytowych). Przestępstwa obejmują również komputerowe podróbki, molestowanie dzieci, aż do ataków na życie ludzkie, np. przez manipulowanie systemami szpitalnymi lub kontroli ruchu powietrznego,
- przestępstwa "contentowe" (dotyczące zawartości). Ta kategoria obejmuje na przykład dziecięcą pornografię, dostarczanie instrukcji przestępczych, oferty popełnienia przestępstw. Do tej kategorii zaliczamy także molestowanie i lobbing poprzez sieć, rozpowszechnianie fałszywych informacji (np. czarny PR, schematy "pump-and-dump") oraz internetowy hazard,
- przestępstwa powiązane z naruszeniem prawa autorskiego i praw pokrewnych, takie jak nieautoryzowane kopiowanie i rozpowszechnianie programów komputerowych, nieautoryzowane użycie baz danych.

W komunikacie zwrócono także uwagę na obserwowaną narastającą tendencję popełniania klasycznych przestępstw, których ślady pozostają w systemach komputerowych - kradzieży, korupcji, oszustw, defraudacji.

⁴ Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, W kierunku ogólnej strategii zwalczania cyberprzestępczości, KOM(2007) 267

W podręczniku Interpolu⁵ z 2007 zwraca się szczególną uwagę na cztery obszary, na których koncentruje się aktualnie cyberprzestępczość: hacking, oprogramowanie złośliwe (włącznie z botnetami), piractwo intelektualne, nielegalna zawartość cyfrowych nośników danych.

Specyfika cyberprzestępczości została bardzo trafnie ujęta w raporcie Europolu⁶ za 2007 rok. Cyberprzestępstwa są w nim wykazane w dwóch ujęciach – wertykalnym i horyzontalnym. Ujęcie wertykalne dotyczy przestępstw, które są specyficzne dla cyberprzestrzeni i poza nią nie mogą być dokonane. Wśród nich wyróżniono: hacking (ataki ddos, botnety, zombies, ...), crimeware (wirusy, robaki, konie trojańskie, ...), spamming. W ujęciu horyzontalnym znalazły się przestępstwa, w których wypadku wykorzystanie technik komputerowych i informatycznych uprościło znacznie ich dokonanie. Jako wnoszące największe zagrożenia uznano: pornografię dziecięcą, nieuprawnione wykorzystanie kart płatniczych, kradzież tożsamości (phishing), piractwo intelektualne, pranie brudnych pieniędzy za pośrednictwem Internetu (cyberlaundering), cyberterrorizm.

Bardzo aktywna w obszarze zwalczania cyberprzestępczości Prezydencja francuska w lipcu 2008 roku przedstawiła „Globalny plan w sprawie zwalczania cyberprzestępczości”. W planie zwrócono szczególną uwagę na to, że:

- Internet stanowi również bardzo skuteczny środek komunikowania się i werbowania stosowany przez terrorystów na całej kuli ziemskiej.
- Umożliwia upowszechnianie nielegalnych treści. Zawierają one pochwałę przemocy i terroryzmu i zachęcają rasowej. Pokazują obrazy przemocy seksualnej wobec dzieci.
- Internet ułatwia przestępcom – używającym fałszywej tożsamości – wyszukiwanie przyszłych ofiar.
- Internet i gospodarka cyfrowa same mogą stać się ofiarą ataków przestępczych. Zagrożone może być bezpieczeństwo systemów niezbędnych dla zapewnienia bezpieczeństwa ludności, suwerenności państw i życia gospodarczego. Jako przykład z niedawnej przeszłości przedstawiono internetowy atak na Estonię.

Można uznać, że efektem prac Prezydencji francuskiej jest Strategia Komisji Europejskiej nt. zwalczania cyberprzestępczości z 28 listopada 2008. Strategia zaleca podjęcie serii środków operacyjnych, takich jak powołanie do życia tzw. "Cyberpatroli", wspólnych zespołów dochodzeniowo-śledczych, wprowadzenie zdalnego przeszukania w Internecie oraz osobnych jednostek badawczych, które zostałyby zaangażowane do walki z cyberprzestępczością w następnych pięciu latach. Strategia KE wprowadza również konkretne rozwiązania bliższej współpracy i wymiany informacji pomiędzy organami wymiaru sprawiedliwości a jednostkami sektora prywatnego (Partnerstwo Publiczno-Prywatne).

W roku 2009 jest planowane wydanie, w ramach Prevention and Fight Against Crime, prawie 71 mln Euro. Priorytetami są m.in. seksualne wykorzystanie dzieci on-line, nielegalne wykorzystanie Internetu, przestępczość ekonomiczna i finansowa. Z tego funduszu istnieje także możliwość dofinansowania krajowych centrów doskonałości w zakresie zwalczania cyberprzestępczości.

Wbrew głośzonym obawom, że organa ścigania nazbyt ingerują w prywatność obywateli w Internecie i głośzonym w związku z tym poglądom, że należy ograniczyć możliwości organów ścigania, Parlament Europejski w zaleceniach z dnia 26 marca 2009 r. dla Rady w sprawie utrwalenia bezpieczeństwa i podstawowych wolności w Internecie⁷ polecił dbanie o pełny i bezpieczny dostęp do Internetu dla wszystkich, ciągłą czujność w odniesieniu do bezwzględnej ochrony i intensywnego promowania podstawowych swobód

⁵ IT Crime Manual of the Interpol Working Party on Information Technology Crime – Europe 2007

⁶ High Tech Crimes within EU. Threat Assessment 2007. Europol, Hague 2007

⁷ Strengthening security and fundamental freedoms on the Internet 2008/2160(INI)

w Internecie, ale jednocześnie jednoznacznie zobowiązał do zwalczania przestępczości w cyberprzestrzeni.

Tworząc ten dokument Parlament wziął pod uwagę Decyzję Ramową Rady 2008/919/WSiSW z dnia 28 listopada 2008 r. zmieniającą ramową decyzję 2002/475/WSiSW w sprawie zwalczania terroryzmu oraz niemiecką inicjatywę na rzecz wykrywania ciężkiej przestępczości i terroryzmu (projekt "Check the Web"⁸). Zwrócił także uwagę, że dzięki wolności, jaką gwarantuje Internet, wykorzystuje się go również jako miejsce rozpowszechniania przesłań charakteryzujących się przemocą, takich jak nawoływanie do ataków terrorystycznych, jak również tworzenie stron internetowych, które mogą wyraźnie prowokować do opartych na nienawiści działań przestępczych.

Warto pamiętać, że oprócz wymienionych wcześniej organizacji w zwalczaniu cyberprzestępczości bardzo aktywną rolę odgrywa także ONZ, Organizację Współpracy Gospodarczej i Rozwoju (OECD) oraz Grupa G8 (G8 Rome/Lyon Group - High-Tech Crime SubGroup).

Współpraca międzynarodowa w zwalczaniu cyberprzestępczości zawsze kojarzona jest z dwoma płaszczyznami pozaoperacyjnymi – edukacją i szkoleniami oraz współpracą z sektorem prywatnym. W tej pierwszej płaszczyźnie ton działaniom nadają Europol i Interpol. Dzięki działaniom Europolu, w ramach projektu AGIS opracowano 7 kursów na poziomie podstawowym i średnim (Applied NTFS Forensics, Intermediate Internet Investigations, Intermediate Network Investigations, Linux as an Investigative Tool, Mobile Phone Forensics, Wireless LANs and Voice over IP oraz szkolenie trenerów), a dwa kolejne poziomy jeszcze nie są zrealizowane (zaawansowany i doskonalący). Opracowane kursy są wykorzystywane także przez University College of Dublin do prowadzenia studiów magisterskich dla policjantów (3 moduły w pierwszym roku, w tym dwa 2-tygodniowe pobyty w Dublinie, a pełny cykl to 10 modułów w 2 lata). Wśród współpracujących (dostarczających wykładowców i tematy prac) jest 6 uniwersytetów i Policje praktycznie z wszystkich krajów Europy. W ramach Interpolu pracują grupy zadaniowe, które w roku 2008 zajmowały się 8 zagadnieniami: The Computer Crime Manual Revision, Policing the Virtual Internet Project, First Responders Project, Counter Forensics Project, Botnet Follow-Up Project, Live Data Forensics. Na konferencji, która odbędzie się w maju 2009 r. zostaną przedstawione i udostępnione dla organów ścigania wypracowane efekty.

Swój wkład w działalność edukacyjną policjantów ma także CEPOL (Europejskie Kolegium Policyjne), który realizuje dla policjantów szkolenia w zakresie zwalczania przestępczości komputerowej i pornografii dziecięcej w Internecie.

W pracach edukacyjno-szkoleniowych zarówno Europolu, jak i Interpolu, aktywny udział biorą przedstawiciele sektora prywatnego. Sektor prywatny jest również inicjatorem wielu działań zmierzających do skuteczniejszej walki z cyberprzestępczością. Wśród najważniejszych inicjatyw warto wymienić:

- Task Forces
 - BotNet Task Force
 - Anti-Phishing Working Group
- HotLines
- IMPACT
- Advanced Fee Fraud Coalition
- McAfee Initiative to Fight Cybercrime.

Koncentrując się na cyberterroryzmie warto szczególną uwagę zwrócić na powstałą w 2008 roku organizację non-profit The International Multilateral Partnership Against Cyber Threats

⁸ Więcej o projekcie można przeczytać np. w dokumentach: "Conclusions of the Kick-off conference "Check the Web" - Berlin, 26-27 September 2006", ENFOPOL 196 ST013930/06-EXT2 z 10.1.2008 oraz "Council Conclusions on cooperation to combat terrorist use of the Internet ("Check the Web")", ENFOPOL 66 ST08457/3/07-REV3,

(IMPACT) z siedzibą w Malezji⁹. Działalność IMPACT nastawiona jest na analizę poważnych zagrożeń związanych z cyberprzestrzenią, infrastrukturą krytyczną, takich jak cyberprzestępczość. Działa w 4 obszarach: Global Response Center - całodobowo obserwuje stan cyberprzestrzeni na świecie, publikuje wiadomości na stronie www oraz posiada zamkniętą sieć dla specjalistów (jak facebook); szkolenia - koordynują i dostarczają miejsca na przeprowadzenie szkoleń i szerzenia najlepszych praktyk na poziomie ministrów; badania nad bezpieczeństwem - dostarczają ekspertyz, współpracują z ponad 20 centrami doskonałości oraz uczelniami; centrum współpracy międzynarodowej - w zakresie cyberprzestępczości.

Przedstawiony w niniejszym artykule przegląd działań mających w wymiarze międzynarodowym zapewnić poprawę bezpieczeństwa cyberprzestrzeni i zwiększyć skuteczność zwalczania cyberprzestępczości powinien unaocznić, że wiele w tym zakresie w Europie jest czynione. Z przykrością należy jednak zauważyć, że aktywność Polski w tych gremiach jest niewielka zarówno w zakresie dostarczania wiedzy i doświadczeń, jak i wykorzystania wiedzy. Może zalecenie: „należy również zapewnić ekspertom krajowym możliwości poszerzania wiedzy i doświadczenia poprzez aktywny udział w pracach grup roboczych Unii Europejskiej oraz szkoleniach z zakresu bezpieczeństwa teleinformatycznego” zapisane w Rządowym programie ochrony cyberprzestrzeni RP na lata 2009-2011 coś zmienić.

9 <http://www.impact-alliance.org/> - motto organizacji to: Cyber-terrorism is real. Join the forces of IMPACT.