KOMISJA WSPÓLNOT EUROPEJSKICH

Bruksela, dnia 22.5.2007
KOM(2007) 267 wersja ostateczna

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY ORAZ KOMITETU REGIONÓW

W kierunku ogólnej strategii zwalczania cyberprzestępczości

{SEK(2007) 641}
{SEK(2007) 642}

KOMUNIKAT KOMISJI
DO PARLAMENTU EUROPEJSKIEGO, RADY
ORAZ KOMITETU REGIONÓW

W kierunku ogólnej strategii zwalczania cyberprzestępczości

1. WPROWADZENIE

1.1. Czym jest cyberprzestępczość?

Bezpieczeństwo systemów informatycznych, których znaczenie w naszym społeczeństwie stale wzrasta, obejmuje wiele aspektów, a zwalczanie cyberprzestępczości jest jego kluczowym elementem. Wobec braku uzgodnionej definicji cyberprzestępczości terminy takie jak „cyberprzestępczość", „przestępczość komputerowa", „przestępczość związana z komputerami" czy „przestępczość przy użyciu zaawansowanych technologii" używane są często zamiennie. Do celów niniejszego komunikatu pod pojęciem cyberprzestępczości rozumie się „czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takich sieciom i systemom".

W praktyce terminu cyberprzestępczość używa się w odniesieniu do trzech rodzajów przestępstw. Pierwszy obejmuje **tradycyjne formy przestępstw**, takie jak oszustwo czy fałszerstwo, jednak w kontekście cyberprzestępczości odnoszą się one konkretnie do przestępstw popełnionych przy użyciu elektronicznych sieci informatycznych i systemów informatycznych (zwanych dalej sieciami łączności elektronicznej). 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, ataki typu *denial of service* oraz hakerstwo. 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. Wszystkie te rodzaje przestępstw łączy to, że mogą być popełnianie na masową skalę, a odległość geograficzna między miejscem popełnienia przestępstwa a jego skutkami może być znaczna. W związku z tym stosowane metody dochodzeniowe wymagają często takich samych możliwości technicznych. Te podobieństwa stanowią główny temat niniejszego komunikatu.

1.2. Ostatnie tendencje w cyberprzestępczości

1.2.1. Wymiar ogólny

Trudno jest uzyskać dokładny obraz obecnej sytuacji ze względu na ciągły rozwój przestępczości i brak wiarygodnych informacji. Można jednak zauważyć kilka ogólnych trendów:

- liczba przestępstw informatycznych stale wzrasta, działania przestępcze stają się też coraz bardziej wyrafinowane i wykraczają poza granice państwowe[1];

- wyraźne przesłanki wskazują na rosnący udział w cyberprzestępczości zorganizowanych grup przestępczych;

- nie wzrasta jednak liczba aktów oskarżenia na podstawie transgranicznej współpracy oddziałów ścigania w Europie.

1.2.2. Przestępstwa tradycyjne w sieciach łączności elektronicznej

Przy użyciu sieci łączności elektronicznej popełnić można większość przestępstw; szczególnie popularnymi i częstymi formami przestępstw w sieciach łączności elektronicznej są różnego rodzaju oszustwa i próby oszustw. Do popełniania oszustw na masową skalę używane są takie metody jak kradzież tożsamości, *phishing* (łowienie haseł)[2], spam oraz złośliwe kody. Rosnącym problemem staje się również nielegalny krajowy i międzynarodowy handel internetowy. Obejmuje on handel narkotykami, bronią oraz zagrożonymi gatunkami zwierząt.

1.2.3. Nielegalne treści

W Europie dostępnych jest coraz więcej stron internetowych zawierających nielegalne treści, takie jak materiały związane z wykorzystywaniem seksualnym dzieci, podżeganiem do aktów terrorystycznych, nielegalną gloryfikacją przemocy, terroryzmem, rasizmem i ksenofobią. Interwencja organów ścigania w przypadku takich stron jest bardzo trudna, ponieważ ich właściciele i administratorzy mieszkają często w innych krajach, często poza UE. Strony można szybko przenieść do innego kraju, również poza terytorium UE, a definicje tego, co nielegalne, są w różnych państwach bardzo różne.

1.2.4. Przestępstwa typowe dla siei łączności elektronicznej

Coraz częstsze stają się ataki na masową skalę, skierowane przeciwko systemom informatycznym, organizacjom i osobom prywatnym (często za pośrednictwem tzw. botnetów[3]). Ostatnio zaobserwowano również przypadki systematycznych, dobrze skoordynowanych bezpośrednich masowych ataków na krytyczne infrastruktury informatyczne państw. Sytuację pogarsza łączenie technologii i coraz częstsze powiązania między systemami informatycznymi, co sprawia, że są one bardziej podatne na takie ataki. Ataki te są często bardzo dobrze zorganizowane, a ich celem jest wymuszenie. Można przypuszczać, że liczba zgłoszonych ataków jest zaniżona, przede wszystkim ze względu na straty, jakie mogłoby przynieść przedsiębiorstwom upublicznienie informacji o problemach z bezpieczeństwem.

---

1 Większość stwierdzeń zawartych w niniejszym komunikacie dotyczących obecnych trendów jest oparta na zamówionym w 2006 r. przez Komisję badaniu dotyczącym oceny wpływu komunikatu w sprawie cyberprzestępczości (umowa nr JLS/2006/A1/003).

2 *Phishing* polega na próbach oszukańczego zdobycia poufnych informacji, takich jak hasła i dane karty kredytowej, poprzez podawanie się podczas komunikacji elektronicznej za osobę godną zaufania.

3 *Botnet* oznacza grupę komputerów zainfekowanych złośliwym oprogramowaniem pod wspólną zdalną kontrolą.

1.3. Cele

W związku z tymi dynamicznymi zmianami konieczne jest szybkie podjęcie działań – zarówno na szczeblu krajowym, jak i unijnym – zwalczających wszelkie formy cyberprzestępczości zagrażające w coraz większym stopniu społeczeństwu, przedsiębiorstwom i obywatelom. Ochrona osób prywatnych przed cyberprzestępczością zostaje często osłabiona na skutek problemów związanych z określeniem jurysdykcji krajowej i prawa właściwego, transgranicznym ściganiem przestępstw oraz uznawaniem i stosowaniem dowodów elektronicznych. Trudności te pogłębia fakt, że cyberprzestępczość ma głównie charakter transgraniczny. Aby odpowiedzieć na te zagrożenia, Komisja zamierza wdrożyć ogólną inicjatywę polityczną w celu usprawnienia koordynacji zwalczania cyberprzestępczości na szczeblu europejskim i międzynarodowym.

Celem jest lepsze zwalczanie cyberprzestępczości na poziomie krajowym, unijnym i międzynarodowym. Za główny cel Komisja i państwa członkowskie uznały w szczególności dalszy rozwój konkretnej polityki UE w tej dziedzinie. Inicjatywa będzie koncentrować się na ściganiu przestępstw i aspektach prawnokarnych zwalczania przestępczości, a strategia będzie uzupełniała inne działania UE poprawiające ogólne bezpieczeństwo w przestrzeni wirtualnej. Strategia będzie obejmowała: lepszą współpracę operacyjną organów ścigania; lepszą współpracę i koordynację polityczną między państwami członkowskimi; współpracę polityczną i prawną z krajami trzecimi; podnoszenie świadomości; szkolenia, badania; ściślejszy dialog z sektorem przemysłu i ewentualne działania legislacyjne.

Strategia w sprawie zwalczania i ścigania cyberprzestępczości zostanie opracowana i wdrożona w sposób w pełni respektujący prawa podstawowe, w szczególności prawo do wolności słowa, prawo do prywatności i życia rodzinnego oraz ochrony danych osobowych. Wszystkie działania legislacyjne podjęte w kontekście tej strategii zostaną najpierw skontrolowane pod względem zgodności z tymi prawami, w szczególności z Kartą praw podstawowych UE. Należy również zauważyć, że wszystkie te inicjatywy zostaną przeprowadzone z całkowitym uwzględnieniem art. 12-15 tzw. dyrektywy o e-handlu[4], w przypadkach, gdy instrument ten ma zastosowanie.

Cel niniejszego komunikatu można podzielić na trzy główne zadania operacyjne:

- poprawa i ułatwienie koordynacji i współpracy między zespołami ds. przestępczości internetowej, innymi właściwymi organami oraz ekspertami w całej Unii;

- stworzenie przy współpracy z państwami członkowskimi, właściwymi organizacjami unijnymi i międzynarodowymi oraz innymi zaangażowanymi podmiotami spójnej strategii ramowej UE w sprawie zwalczania cyberprzestępczości;

- zwiększenie wiedzy na temat kosztów i niebezpieczeństw związanych z cyberprzestępczością

[4] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (Dz.U. L 178, 17.7.2000, str. 1).

2. ISTNIEJĄCE INSTRUMENTY PRAWNE W WALCE Z CYBERPRZESTĘPCZOŚCIĄ

2.1. Działania i instrumenty na poziomie UE

Niniejszy komunikat dotyczący strategii wobec cyberprzestępczości stanowi konsolidację i rozwinięcie komunikatu w sprawie budowania bezpieczniejszego społeczeństwa informacyjnego poprzez zwiększanie bezpieczeństwa struktur informacyjnych i zwalczanie przestępczości komputerowej[5] (zwany dalej komunikatem z 2001 r.). W komunikacie z 2001 r. zaproponowano odpowiednie przepisy materialne i proceduralne służące zwalczaniu zarówno krajowych jak i transgranicznych czynów przestępczych. W następstwie przedstawiono kilka ważnych wniosków. Szczególnie należy tu wymienić wniosek dotyczący decyzji ramowej 2005/222/WSiSW w sprawie ataków na systemy informatyczne[6]. W związku z tym warto również odnotować, że przyjęto także inne, bardziej ogólne akty prawne, również dotyczące aspektów zwalczania cyberprzestępczości, takie jak decyzja ramowa 2001/413/WSiSW w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi[7].

Decyzja ramowa 2004/68/WSiSW dotycząca zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej[8] stanowi dobry przykład szczególnych starań Komisji w zakresie **ochrony dzieci**, zwłaszcza związanych ze zwalczaniem wszystkich rodzajów materiałów związanych z seksualnym wykorzystywaniem dzieci, nielegalnie publikowanych przy użyciu systemów informatycznych, stanowiącym ogólny priorytet na przyszłość.

Aby stawić czoła wyzwaniom związanym z bezpieczeństwem w społeczeństwie informatycznym, Wspólnota Europejska opracowała trójstopniową koncepcję bezpieczeństwa sieci i informacji, obejmującą konkretne środki bezpieczeństwa sieci i informacji, ramy prawne dotyczące komunikacji elektronicznej oraz zwalczanie cyberprzestępczości. Wszystkie te trzy aspekty można w pewnym stopniu traktować oddzielnie, jednak ich liczne wzajemne powiązania wymagają ścisłej koordynacji. W powiązanym obszarze bezpieczeństwa sieci i informacji Komisja przyjęła w 2001 r. – równocześnie z komunikatem z 2001 r. o cyberprzestępczości – komunikat w sprawie bezpieczeństwa sieci i informacji: propozycję koncepcji strategicznej UE[9]. Dyrektywa 2002/58/WE o prywatności i łączności elektronicznej nakłada na dostawców ogólnodostępnych usług komunikacji elektronicznej obowiązek zadbania o bezpieczeństwo ich usług. Zawarte są w niej również przepisy o ochronie przed spamem i oprogramowaniem szpiegującym. Strategię bezpieczeństwa sieci i informacji rozwijano od tego czasu poprzez liczne działania, ostatnio przez komunikat dotyczący strategii na rzecz bezpiecznego społeczeństwa informacyjnego[10] (opracowano w nim nową strategię i stworzono ramy pozwalające rozwijać i ulepszać spójne podejście do bezpieczeństwa sieci i informacji), komunikat w sprawie w sprawie walki ze spamem, oprogramowaniem szpiegującym i złośliwym[11], a w 2004 r. rozporządzenie ustanawiające ENISA[12]. Głównym celem ENISA jest dostarczanie wiedzy fachowej w celu stymulowania

---

5 KOM(2000) 890, 26.1.2001.
6 Dz.U. L 69 z 16.3.2005, str 67.
7 Dz.U. L 149 z 2.6.2001, str. 1 .
8 Dz.U. L 13, 20.1.2004, str. 44.
9 KOM(2001) 298.
10 KOM(2006) 251.
11 KOM(2006) 688.
12 Rozporządzenie 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji, (Dz.U. L 77 z 13.3.2004, str. 1.).

współpracy między sektorem publicznym i prywatnym oraz pomoc Komisji i państwom członkowskim. **Wyniki badań** w dziedzinie technologii służących zabezpieczaniu systemów informatycznych odgrywają również ważną rolę w zwalczaniu cyberprzestępczości. W związku z tym w 7. ramowym programie badań UE, obejmującym lata 2007-2013[13], wśród celów znalazły się zarówno technologie informatyczne i komunikacyjne jak i bezpieczeństwo. Przegląd przepisów dotyczących komunikacji elektronicznej może zaowocować wprowadzeniem poprawek do przepisów dyrektywy 2002/58/WE o prywatności i łączności elektronicznej oraz dyrektywy 2002/22/WE[14] o usłudze powszechnej dotyczących bezpieczeństwa.

2.2. Istniejące instrumenty międzynarodowe

Ze względu na globalny charakter sieci informacyjnych żadna strategia dotycząca cyberprzestępczości nie będzie skuteczna, jeśli wysiłki będą podejmowane jedynie w obrębie UE. Przestępcy mogą dokonywać ataku na systemy informatyczne oraz popełniać przestępstwa w jednym państwie członkowskim działając z innego państwa członkowskiego, mogą również działać spoza obszaru jurysdykcji UE. Dlatego Komisja aktywnie uczestniczyła w międzynarodowych dyskusjach i strukturach współpracy, tj. grupie G8 Lyon-Rzym ds. przestępczości z wykorzystaniem zaawansowanych technologii oraz w projektach zarządzanych przez Interpol. Komisja szczególnie uważnie śledzi pracę całodobowej sieci kontaktów ds. międzynarodowej przestępczości w zakresie zaawansowanych technologii (sieć 24/7)[15], do której należy wiele państw na całym świecie, w tym większość państw członkowskich UE. Sieć G8 stanowi mechanizm usprawniający kontakty między państwami uczestniczącymi w tej sieci poprzez całodobowe punkty kontaktowe, z których można korzystać w sprawach związanych z dowodami elektronicznymi lub wymagających pilnej pomocy zagranicznych organów ścigania.

Prawdopodobnie najważniejszym instrumentem europejskim i międzynarodowym w tej dziedzinie jest konwencja Rady Europy z 2001 r. w sprawie cyberprzestępczości[16]. Konwencja, która została przyjęta i weszła w życie w 2004 r., zawiera wspólne definicje różnych rodzajów przestępstw komputerowych oraz ustanawia podstawy funkcjonowania współpracy sądowej między państwami-sygnatariuszami konwencji. Została ona podpisana przez wiele krajów, m.in. przez Stany Zjednoczone i inne państwa pozaeuropejskie, a także przez wszystkie państwa członkowskie UE. Jednak wiele państw członkowskich jeszcze nie ratyfikowało konwencji lub jej dodatkowych protokołów dotyczących czynów przestępczych o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych. Biorąc pod uwagę uznane znaczenie konwencji, Komisja będzie zachęcać państwa członkowskie i odpowiednie kraje trzecie do jej ratyfikacji oraz rozważy możliwość przystąpienia do konwencji przez Wspólnotę Europejską.

---

13 Już w ramach 6. ramowego programu badań i rozwoju technologicznego UE wsparła szereg udanych projektów badawczych w tej dziedzinie.

14 KOM(2006) 334, SEK(2006) 816, SEK(2006) 817.

15 Patrz art. 35 konwencji Rady Europy w sprawie cyberprzestępczości.

16 http://conventions.coe.int/treaty/en/treaties/html/185.htm

3. DALSZE TWORZENIE KONKRETNYCH INSTRUMENTÓW DO ZWALCZANIA CYBERPRZESTĘPCZOŚCI

3.1. Wzmocnienie operacyjnej współpracy organów ścigania oraz szkoleń na poziomie UE

Brak struktur służących operacyjnej współpracy transgranicznej lub ich niedostateczne wykorzystywanie pozostaje głównym problemem w obszarze sprawiedliwości, wolności i bezpieczeństwa. Tradycyjna współpraca w obliczu nagłych przypadków przestępstw komputerowych jest zbyt wolna i nieskuteczna, a nowe struktury współpracy nie zostały jeszcze odpowiednio rozwinięte. Mimo że krajowe organy sądowe i organy ścigania w Europie współpracują ściśle za pośrednictwem Europolu, Eurojustu i innych struktur, koniecznie jest wzmocnienie i doprecyzowanie ich obowiązków. Z konsultacji przeprowadzonych przez Komisję wynika, że te kluczowe kanały nie są wykorzystywane w optymalny sposób. Lepiej skoordynowane podejście europejskie musi być zarówno funkcjonalne jak i strategiczne, powinno także obejmować wymianę informacji i najlepszych praktyk.

Komisja w najbliższej przyszłości położy szczególny nacisk na potrzeby **szkoleniowe.** Rozwój technologiczny powoduje konieczność ciągłego szkolenia organów sądowych i organów ścigania w kwestiach dotyczących cyberprzestępczości. Planowane jest udzielanie przez UE większego i lepiej skoordynowanego wsparcia finansowego dla międzynarodowych projektów szkoleniowych. Komisja będzie również, w ścisłej współpracy z państwami członkowskimi i innymi właściwymi organami takimi jak Europol, Europejskie Kolegium Policyjne (CEPOL) oraz europejska sieć szkolenia kadr wymiaru sprawiedliwości (EJNT), dążyć do koordynacji szkoleń na poziomie UE i wzajemnego powiązania wszystkich programów szkoleniowych w tej dziedzinie.

Komisja zorganizuje **spotkanie** ekspertów z wymiaru sprawiedliwości państw członkowskich jak również z Europolu, CEPOL-u i EJTN, w celu przedyskutowania, w jaki sposób można usprawnić współpracę operacyjną i strategiczną oraz szkolenia w zakresie cyberprzestępczości w 2007 r. w Europie. Rozważony zostanie m.in. pomysł stworzenia stałego punktu kontaktowego UE w celu wymiany informacji oraz unijnej platformy szkoleniowej w zakresie cyberprzestępczości. Spotkanie w 2007 r. będzie pierwszym z serii spotkań zaplanowanych w najbliższej przyszłości.

3.2. Lepszy dialog z sektorem przemysłu

Zarówno sektor prywatny jak i państwowy są zainteresowane wspólnym opracowywaniem sposobów identyfikowania zagrożeń wynikających z działalności przestępczej oraz zapobiegania im. Wspólne działania sektora prywatnego i publicznego, oparte na wzajemnym zaufaniu i realizacji wspólnego celu, jaki jest redukcja zagrożeń, wydają się być skutecznym sposobem zwiększenia bezpieczeństwa, również w ramach walki z cyberprzestępczością. Publiczno-prywatne aspekty strategii Komisji w sprawie cyberprzestępczości zostaną w odpowiednim czasie włączone do przygotowywanej ogólnej strategii UE dotyczącej dialogu między sektorem publicznym i prywatnym, która obejmie całą dziedzinę bezpieczeństwa europejskiego. Strategia ta będzie szczególnie rozwijana w ramach europejskiego forum badań nad bezpieczeństwem i innowacjami, które Komisja planuje wkrótce stworzyć i skupić w nim odpowiednie podmioty z sektora publicznego i prywatnego.

Rozwój nowoczesnych technologii informacyjnych i systemów komunikacji elektronicznej jest w dużym stopniu kontrolowany przez operatorów prywatnych. Prywatne przedsiębiorstwa przeprowadzają oceny zagrożeń, opracowują programy zwalczania przestępczości i tworzą rozwiązania techniczne zapobiegające przestępczości. Sektor przemysłu przyjął bardzo pozytywną postawę w zakresie wspierania organów publicznych w walce z cyberprzestępczością, szczególnie w zwalczaniu pornografii dziecięcej[17] i innych rodzajów nielegalnych treści w Internecie.

Inna kwestią jest wyraźny brak przepływu informacji, wiedzy fachowej oraz najlepszych praktyk między sektorem prywatnym i publicznym. Przedsiębiorstwa sektora prywatnego – ze względu na ochronę modeli biznesowych i tajemnic przedsiębiorstwa – często niechętnie zgłaszają przypadki przestępstw lub informują o nich organy ścigania, ponadto często nie są do tego wyraźnie zobowiązane przepisami. Takie informacje mogą pomóc organom publicznym podczas opracowywania skutecznej i właściwej strategii zwalczania przestępczości. Możliwości usprawnienia międzysektorowego przepływu informacji zostaną zbadane również w świetle obowiązujących przepisów dotyczących ochrony danych.

Komisja odgrywa istotną rolę w różnych strukturach publiczno-prywatnych zajmujących się cyberprzestępczością, takich jak grupa ekspertów ds. walki z nadużyciami finansowymi[18]. Komisja jest przekonana, że skuteczna ogólna strategia zwalczania cyberprzestępczości musi obejmować również strategię współpracy między podmiotami sektora publicznego i prywatnego, w tym organizacjami społeczeństwa obywatelskiego.

W celu zacieśnienia współpracy publiczno-prywatnej w tej dziedzinie, Komisja zamierza w 2007 r. zorganizować konferencję z udziałem ekspertów wymiaru sprawiedliwości i przedstawicieli sektora prywatnego, szczególnie dostawców usług internetowych, aby omówić sposoby usprawnienia operacyjnej współpracy publiczno-prywatnej w Europie[19]. Na konferencji poruszone zostaną wszystkie zagadnienia, które mogą przynieść korzyści dla obu sektorów, szczególnie jednak następujące kwestie:

- poprawa operacyjnej współpracy w zwalczaniu nielegalnych działań i treści w Internecie, a konkretnie w zakresie terroryzmu, materiałów związanych z seksualnym wykorzystywaniem dzieci i innych nielegalnych działań szczególnie istotnych z punktu widzenia ochrony dziecka;

- inicjowanie porozumień publiczno-prywatnych zmierzających do blokowania na całym obszarze UE stron internetowych zawierających treści nielegalne, w szczególności materiały związane z seksualnym wykorzystywaniem dzieci;

- opracowanie europejskiego modelu wymiany przydatnych i ważnych informacji między sektorem prywatnym a publicznym z myślą o tworzeniu atmosfery wzajemnego zaufania i uwzględnianiu interesów wszystkich stron;

---

17 Jednym z ostatnich przykładów w tej dziedzinie jest współpraca wymiaru sprawiedliwości ze spółkami rozliczeniowymi kart płatniczych, w ramach której spółki te pomogły policji w wytropieniu osób kupujących on-line pornografię dziecięcą.

18 Patrz http://ec.europa.eu/internal_market/payments/fraud/index_en.htm

19 Konferencja taką można by uznać za kontynuację forum UE omówionego w pkt 6.4 komunikatu w sprawie cyberprzestępczości.

- utworzenie sieci punktów kontaktowych wymiaru sprawiedliwości, zarówno w sektorze prywatnym jak i publicznym.

3.3. Prawodawstwo

Ze względu na dużą różnorodność rodzajów przestępstw objętych pojęciem cyberprzestępczości nie jest jeszcze właściwe ogólne ujednolicenie definicji przestępstw i krajowych przepisów prawa karnego w dziedzinie cyberprzestępczości. Skuteczna współpraca między organami ścigania zależy często od przynajmniej częściowo ujednoliconych definicji przestępstw, dlatego długoterminowym celem pozostają prace nad harmonizacją przepisów prawnych państw członkowskich[20]. Jeśli chodzi o niektóre najważniejsze definicje przestępstw, znaczne postępy udało się osiągnąć w decyzji ramowej w sprawie ataków na systemy informatyczne. Jak wspomniano powyżej, od tego czasu pojawiły się nowe zagrożenia, dlatego też Komisja uważnie śledzi te zmiany, ponieważ ważne jest stałe badanie, czy istnieje konieczność wprowadzenia dodatkowych przepisów. Monitorowanie zmieniających się zagrożeń jest ściśle skoordynowane z Europejskim Programem Ochrony Infrastruktury Krytycznej (ang. *European Programme for Critical Infrastructure Protection – EPCIP)*.

Należy jednak rozważyć również przyjęcie aktów prawnych dotyczących konkretnych aspektów cyberprzestępczości. Kwestią szczególną, która może wymagać odrębnych przepisów, jest sytuacja, w której cyberprzestępstwo jest popełnianie w powiązaniu z **kradzieżą tożsamości.** Zasadniczo przez „kradzież tożsamości" rozumie się wykorzystywanie identyfikujących danych personalnych, np. numeru karty kredytowej, jako narzędzia do popełnienia innych przestępstw. W większości państw członkowskich przestępca najprawdopodobniej byłby ścigany nie za kradzież tożsamości, ale za oszustwo lub inne przestępstwo, które uznaje się za poważniejsze. Kradzież tożsamości jako taka nie we wszystkich państwach członkowskich stanowi przestępstwo. Często łatwiej jest udowodnić kradzież tożsamości niż oszustwo; w związku z tym z korzyścią dla unijnej współpracy w wymiarze sprawiedliwości byłoby uznanie kradzieży tożsamości za przestępstwo we wszystkich państwach członkowskich. Komisja w 2007 r. zamierza rozpocząć konsultacje, pozwalające ocenić, czy właściwe jest przyjęcie odpowiedniego aktu prawnego.

3.4. Opracowanie danych statystycznych

Powszechnie uznaje się, że stan wiedzy o liczbie dokonywanych przestępstw jest obecnie w dużym stopniu niewystarczający. Szczególnie potrzebne są lepsze dane pozwalające porównywać sytuacje w różnych państwach członkowskich. Ambitny plan pięcioletni mający pomóc rozwiązać ten problem został ustanowiony w komunikacie Komisji pt. *Opracowanie kompleksowej i spójnej strategii UE w zakresie statystyk dotyczących przestępczości i wymiaru sprawiedliwości w sprawach karnych: plan działania UE na lata 2006–2010* z dnia 7 sierpnia 2006 r[21]. Zespół ekspertów powołany na podstawie tego planu działań stanowić będzie właściwe forum do opracowania odpowiednich wskaźników służących do oceny poziomu cyberprzestępczości.

---

[20] Ten długoterminowy cel został już wspomniany na str. 3 komunikatu z 2001 r.

[21] KOM(2006) 437, 7.8.2006.

4. PERSPEKTYWY

Komisja chce dalej rozwijać ogólną strategię zwalczania cyberprzestępczości. Ze względu na ograniczone uprawnienia Komisji w zakresie prawa karnego strategia ta może być tylko uzupełnieniem działań podejmowanych przez państwa członkowskie i inne organy. Najważniejsze działania – z których każde będzie się wiązało z wykorzystaniem jednego, kilku lub wszystkich narzędzi przedstawionych w pkt 3 - będą wspierane również w ramach programu finansowego „Zapobieganie i zwalczanie przestępczości":

4.1. Ogólne zwalczanie cyberprzestępczości

- nawiązanie ściślejszej współpracy operacyjnej między organami ścigania i organami sądowymi państw członkowskich. Początkiem tych działań będzie organizacja w 2007 r. spotkania ekspertów poświęconego tym zagadnieniom. W ramach współpracy stworzony może zostać centralny unijny punkt kontaktowy ds. cyberprzestępczości;

- zwiększenie wsparcia finansowego dla inicjatyw na rzecz lepszych szkoleń dla organów ścigania i organów sądowych w zakresie spraw dotyczących cyberprzestępstw oraz próba koordynacji wszystkich międzynarodowych działań szkoleniowych w tym zakresie poprzez stworzenie unijnej platformy szkoleniowej;

- promowanie mocniejszego zaangażowania państw członkowskich i wszystkich organów publicznych w podejmowanie skutecznych działań przeciw cyberprzestępczości oraz przeznaczania odpowiednich zasobów na zwalczanie tego rodzaju przestępstw;

- wsparcie badań pomagających w zwalczaniu cyberprzestępczości;

- zorganizowanie przynajmniej jednej dużej konferencji (w 2007 r.) z udziałem organów ścigania oraz podmiotów prywatnych, szczególnie w celu rozpoczęcia współpracy w zwalczaniu nielegalnej działalności internetowej w sieciach łączności elektronicznej oraz przeciwko tym sieciom, a także promowania skuteczniejszej wymiany danych nieosobowych, a następnie wdrażanie wniosków z tej konferencji poprzez konkretne projekty współpracy publiczno-prywatnej;

- podjęcie inicjatywy na rzecz działań i udział w działaniach publiczno-prywatnych służących zwiększaniu wiedzy (szczególnie wśród konsumentów) o kosztach i niebezpieczeństwach spowodowanych cyberprzestępczością, a równocześnie unikanie koncentrowania się tylko na zagrożeniach bezpieczeństwa, aby nie podważać zaufania konsumentów i użytkowników;

- aktywny udział w światowej współpracy międzynarodowej w zakresie zwalczania cyberprzestępczości i promowanie takiej współpracy;

- inicjowanie, współtworzenie i wspieranie międzynarodowych projektów zgodnych ze strategią Komisji w tej dziedzinie, np. projektów prowadzonych przez G8 i zgodnych z krajowymi i regionalnymi dokumentami strategicznymi (dotyczącymi współpracy z krajami trzecimi);

- podjęcie konkretnych działań zachęcających wszystkie państwa członkowskie i odpowiednie kraje trzecie do ratyfikacji konwencji Rady Europy o cyberprzestępczości i jej dodatkowych protokołów oraz rozważenie możliwości przystąpienia Wspólnoty jako strony do konwencji;

- zbadanie wspólnie z państwami członkowskimi zjawiska dobrze zorganizowanych masowych ataków na krytyczne infrastruktury informatyczne państw członkowskich w celu zapobiegania im i ich zwalczania, a także skoordynowanego reagowania na nie i wymiany informacji i najlepszych praktyk.

4.2. Walka z tradycyjnymi formami przestępczości w sieciach łączności elektronicznej

- rozpoczęcie dogłębnych badań w celu opracowania wniosku w sprawie specjalnego aktu prawnego UE dotyczącego kradzieży tożsamości;

- promowanie rozwoju metod i procedur technicznych służących zwalczaniu oszustw i nielegalnego handlu w Internecie, również poprzez projekty współpracy publiczno-prywatnej;

- kontynuowanie i rozwijanie prac w konkretnych ukierunkowanych dziedzinach, takich jak zwalczanie nadużyć finansowych przy użyciu bezgotówkowych środków płatniczych w sieciach łączności elektronicznej w ramach grupy ekspertów ds. walki z nadużyciami finansowymi.

4.3. Nielegalne treści

- dalsze opracowywanie działań przeciwko konkretnym nielegalnym treściom w Internecie, szczególnie w odniesieniu do materiałów związanych z seksualnym wykorzystywaniem dzieci oraz nawoływaniem do terroryzmu, zwłaszcza poprzez działania następcze związane z wdrożeniem decyzji ramowej dotyczącej zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej;

- zachęcanie państw członkowskich do przydzielenia odpowiednich środków finansowych na zwiększenie skuteczności działań organów ścigania, ze szczególnym uwzględnieniem identyfikacji ofiar w materiałach związanych z wykorzystywaniem seksualnym rozprowadzanych on-line;

- rozpoczęcie i wspieranie działań przeciwko nielegalnym treściom, które mogą nawoływać nieletnich do przemocy lub innych poważnych nielegalnych zachowań, m.in. pewnych rodzajów szczególnie pełnych przemocy gier on-line;

- rozpoczęcie i promowanie dialogu między państwami członkowskimi i krajami trzecimi na temat technicznych metod zwalczania nielegalnych treści, jak również procedur w zakresie zamykania nielegalnych witryn internetowych, również w celu osiągania formalnych porozumień w tej kwestii z krajami ościennymi i nie tylko;

- zawieranie dobrowolnych porozumień i konwencji na szczeblu unijnym między organami publicznymi i podmiotami publicznymi, zwłaszcza dostawcami usług internetowych, w odniesieniu do procedur blokowania i zamykania nielegalnych stron internetowych.

4.4. Dalsze działania

W niniejszym komunikacie wiele działań służących ulepszeniu struktur współpracy w UE określono jako działania przyszłe. Komisja będzie dalej prowadzić te działania, oceniać postępy i ich realizację oraz przedstawi Radzie i Parlamentowi sprawozdanie w 2010 r.