Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową Rady 2005/222/WSiSW

COM(2010) 517 wersja ostateczna – 2010/0273 (COD)

(2011/C 218/27)

Sprawozdawca generalny: **Peter MORGAN**

Dnia 20 stycznia 2011 r. Rada, działając na podstawie art. 114 Traktatu o funkcjonowaniu Unii Europejskiej, postanowiła zasięgnąć opinii Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie

wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową Rady 2005/222/WSiSW

COM(2010) 517 wersja ostateczna – 2010/0273 (COD).

Dnia 15 lutego 2011 r. Prezydium Europejskiego Komitetu Ekonomiczno-Społecznego powierzyło przygotowanie opinii w tej sprawie Sekcji Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego.

Mając na względzie pilny charakter prac (art. 59 regulaminu wewnętrznego), na 471. sesji plenarnej w dniach 4–5 maja 2011 r. (posiedzenie z 4 maja) Europejski Komitet Ekonomiczno-Społeczny wyznaczył Petera Morgana na sprawozdawcę generalnego oraz stosunkiem głosów 173 do 1 – 7 osób wstrzymało się od głosu – przyjął następującą opinię:

1. **Wnioski i zalecenia**

1.1 Komitet z zadowoleniem przyjmuje komunikat Komisji w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady dotyczącej ataków na systemy informatyczne. Komitet podziela głębokie zaniepokojenie Komisji rozmiarami zjawiska cyberprzestępczości w Europie oraz faktyczną i potencjalną szkodliwością dla gospodarki i dobrobytu obywateli z powodu rosnących zagrożeń.

1.2 Komitet podziela rozczarowanie Komisji, z powodu tego, że tylko 15 z 27 państw członkowskich dotychczas ratyfikowało Konwencję Rady Europy o cyberprzestępczości ([1]). Komitet wzywa pozostałe państwa członkowskie ([2]) – Austrię, Belgię, Republikę Czeską, Grecję, Irlandię, Luksemburg, Maltę, Polskę, Szwecję i Zjednoczone Królestwo – do jak najszybszego ratyfikowania Konwencji o cyberprzestępczości.

1.3 Komitet zgadza się z Komisją co do pilnej potrzeby przyjęcia dyrektywy, aby zaktualizować definicję przestępstw związanych z atakami na systemy informatyczne oraz zapewnić lepszą koordynację i współpracę wymiarów sprawiedliwości w sprawach karnych w celu rozwiązania tego poważnego problemu.

1.4 Ze względu na konieczność przedsięwzięcia pilnych środków legislacyjnych specjalnie w celu rozwiązania problemu ataków na systemy informatyczne Komitet zgadza się z decyzją Komisji co do skorzystania z możliwości politycznej polegającej na przyjęciu dyrektywy wraz z towarzyszącymi środkami nielegislacyjnymi skierowanymi przeciwko temu konkretnemu aspektowi cyberprzestępczości.

1.5 Zgodnie z wezwaniem wyrażonym w poprzedniej opinii ([3]) Komitet pragnie jednak, aby działania Komisji przebiegały jednocześnie z pracami nad opracowaniem wszechstronnego prawodawstwa UE przeciwko cyberprzestępczości. Komitet jest przekonany, że dla powodzenia agendy cyfrowej i strategii „Europa 2020" niezbędne są wszechstronne ramy prawne ([4]). Oprócz egzekwowania prawa i kar, ramy te powinny obejmować również zagadnienia związane z zapobieganiem, wykrywaniem i edukacją.

1.6 W odpowiednim momencie EKES chciałby rozważyć propozycje Komisji dotyczące szerokich ram działań na rzecz rozwiązania ogólnego problemu bezpieczeństwa internetu. Jeśli wybiec myślą 10 lat do przodu, kiedy większość ludzie będzie korzystać z internetu, a większość działalności gospodarczej i społecznej będzie od niego zależeć, jest nie do pomyślenia, abyśmy wciąż mogli wtedy polegać na obecnym nieformalnym i niezorganizowanym podejściu do korzystania z internetu, zwłaszcza że ekonomiczna wartość tej działalności nie da się zmierzyć. Pojawią się rozmaite zagadnienia związane z innymi problemami, takimi jak bezpieczeństwo danych osobowych i prywatność oraz cyberprzestępczość. Nad bezpieczeństwem lotnictwa czuwa centralny organ, ustalający normy samolotów, portów lotniczych i działalności linii lotniczych. Czas na utworzenie analogicznego organu, który ustalałby normy niezawodnych urządzeń końcowych (komputerów osobistych, tabletów, telefonów), bezpieczeństwa sieci, stron internetowych i danych. Kluczowym elementem obrony przed cyberprzestępczością jest fizyczna konfiguracja internetu. W UE potrzebny będzie organ regulacyjny z uprawnieniami w zakresie zarządzania internetem.

1.7 Dyrektywa skoncentruje się na definicji przestępstwa i zagrożenia karami. EKES wnosi, by równolegle skupiono się na kwestii zapobiegania poprzez lepsze środki bezpieczeństwa. Producenci sprzętu powinni spełniać normy dotyczące dostarczania niezawodnych urządzeń. Jest niedopuszczalne, by bezpieczeństwo urządzeń, a zatem i sieci zależało od kaprysów ich właścicieli. Należy rozważyć wprowadzenie ogólnoeuropejskiego systemu tożsamości elektronicznej, jednakże zaprojektowanego z zachowaniem ostrożności, by uniknąć naruszania prywatności; należy zapoczątkować pełne wykorzystanie możliwych zabezpieczeń w protokole IPv6, a jedną z kluczowych części szkoleń w zakresie posługiwania się technologiami cyfrowymi powinno być uczenie zasad osobistego bezpieczeństwa

([1]) Konwencja Rady Europy o cyberprzestępczości, Budapeszt, 23.11.2001, CETS nr 185.

([2]) Zob. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

([3]) Opinia EKES-u w sprawie bezpiecznego społeczeństwa informacyjnego, Dz.U. C 97 z 28.4.2007, s. 21.

([4]) COM(2010) 245, COM(2010) 2020.

cyfrowego, w tym bezpieczeństwa danych. Komisja powinna odwołać się do wcześniejszych opinii Komitetu, w których poruszano te zagadnienia ([5]).

1.8 Komitet wyraża zadowolenie, że we wniosku dotyczącym dyrektywy należycie uwzględniono ataki na systemy informatyczne z wykorzystaniem botnetów ([6]), w tym ataki typu „denial-of-service" ([7]). Komitet jest również przekonany, że dyrektywa pomoże władzom w ściganiu cyberprzestępczości, która charakteryzuje się wykorzystywaniem międzynarodowych połączeń międzysystemowych, a także w ściganiu sprawców, którzy usiłują wykorzystywać skomplikowane narzędzia cyberprzestępcze do ukrycia swojej tożsamości.

1.9 Komitet wyraża również zadowolenie z powodu zawartego w dyrektywie wykazu przestępstw, szczególnie z uwzględnienia „nielegalnego przechwytywania" oraz wyraźnego wskazania „narzędzi używanych do popełniania przestępstw".

1.10 Biorąc jednak pod uwagę znaczenie zaufania do gospodarki cyfrowej i jej bezpieczeństwa oraz ogromne koszty, jakie pochłania co roku cyberprzestępczość ([8]), Komitet proponuje przewidzieć w dyrektywie kary na tyle surowe, aby odzwierciedlały one wagę przestępstwa, a także stanowiły czynnik skutecznie odstraszający. We wniosku w sprawie dyrektywy przewidziano minimalne kary w wymiarze 2 lub 5 lat więzienia (5 lat w przypadku okoliczności obciążających). EKES przewiduje zróżnicowanie kary w zależności od wagi przestępstwa.

1.11 Europejski Komitet Ekonomiczno-Społeczny proponuje skorzystać z nadarzającej się sposobności do nadania jasnego komunikatu w postaci przyjęcia bardziej surowych kar, skierowanego do przestępców i obywateli, którzy potrzebują bezpieczeństwa. Na przykład w Wielkiej Brytanii ([9]) kara za zakrojony na wielką skalę atak na system informatyczny wynosi do 10 lat pozbawienia wolności. Również Estonia zwiększyła przewidywane kary i obecnie za przeprowadzenie atak na wielką skalę w celach terrorystycznych grozi kara do 25 lat pozbawienia wolności ([10]).

1.12 Komitet z zadowoleniem przyjmuje propozycję Komisji dotyczącą wsparcia dyrektywy środkami nielegislacyjnymi w celu promowania dalszych skoordynowanych działań na szczeblu UE oraz skuteczniejszego egzekwowania prawa. EKES podkreśla również potrzebę rozszerzenia współpracy, tak aby objęła ona ścisłą współpracę ze wszystkimi państwami EFTA i NATO.

1.13 Komitet zdecydowanie popiera programy szkoleń i zalecenia dotyczące sprawdzonych rozwiązań proponowanych w celu skuteczniejszego wykorzystywania przez organy ścigania istniejących całodobowych punktów kontaktowych działających przez całą dobę siedem dni w tygodniu.

1.14 Komitet wzywa Komisję, aby poza wspomnianymi we wniosku środkami nielegislacyjnymi szczególnie ukierunkowała fundusze B+R na rozwój systemów wczesnego wykrywania i reagowania w celu powstrzymania ataków na systemy informatyczne. Najnowsze osiągnięcia technologiczne w dziedzinach chmur obliczeniowych ([11]) i przetwarzania rozproszonego ([12]) mogą zapewnić Europie lepszą ochronę przed licznymi zagrożeniami.

1.15 Komitet zaleca, aby Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji, poza egzekwowaniem prawa, udzieliła finansowego wsparcia ukierunkowanemu programowi rozwoju kompetencji w celu poprawy zabezpieczeń w europejskim sektorze bezpieczeństwa technologii informacyjno-komunikacyjnych (TIK) ([13]).

1.16 Aby wzmocnić europejskie zabezpieczenia przed atakami cybernetycznymi, Komitet pragnie ponownie podkreślić znaczenie utworzenia europejskiego partnerstwa publiczno-prywatnego na rzecz odporności (EP3R) oraz włączyć je w działania Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) i Europejskiej Grupy Rządowych Zespołów Reagowania Na Incydenty Komputerowe (EGC).

([5]) Opinia EKES-u w sprawie bezpiecznego społeczeństwa informacyjnego, Dz.U. C 97 z 28.4.2007, s. 21;
opinia EKES-u w sprawie udoskonalenia techniki internetowej, Dz.U. C 175 z 28.7.2009, s. 92;
opinia EKES-u w sprawie ochrony krytycznej infrastruktury informatycznej, Dz.U. C 255 z 22.9.2010, s. 98;
opinia EKES-u w sprawie europejskiej agendy cyfrowej, Dz.U. C 54 z 19.2.2011, s. 58;
opinia EKES-u w sprawie nowego rozporządzenia ENISA, jeszcze nieopublikowana w Dz.U.;
opinia EKES-u w sprawie poprawy kultury informatycznej, umiejętności informatycznych i e-integracji, jeszcze nieopublikowana w Dz.U.

([6]) Pojęcie botnetu oznacza sieć komputerów zarażonych złośliwym oprogramowaniem (wirusami komputerowymi). Taka sieć zainfekowanych komputerów (tzw. zombie) może zostać aktywowana do wykonywania szczególnych zadań takich jak ataki na systemy informatyczne (cyberataki). Zainfekowane komputery „zombie" mogą być kontrolowane, często bez wiedzy użytkowników takich komputerów, przez inny komputer. Trudno jest namierzać sprawców, ponieważ komputery składające się na botnet i wykorzystywane do ataku mogą znajdować się w innymi miejscu niż sam przestępca.

([7]) Atak typu „denial-of-service" (odmowa dostępu) polega na zablokowaniu dostępu do zasobów komputerowych (na przykład strony internetowej lub usługi internetowej) użytkownikom, dla których są one przeznaczone. Przy próbie kontaktu z serwerem lub stroną internetową pokaże się komunikat o niedostępności serwisu lub strony. Na skutek takiego ataku na przykład internetowy system płatniczy może przestać działać, powodując straty dla jego użytkowników.

([8]) Według analizy z 2009 r. przedstawionej na Światowym Forum Gospodarczym, światowy koszt cyberprzestępczości wynosi 1 bilion USD i szybko rośnie. Zob. pkt 2.5 i 2.7 poniżej.

([9]) Zob. http://www.legislation.gov.uk/ukpga/2006/48/contents.

([10]) SEC(2010) 1122 wersja ostateczna – dokument roboczy służb Komisji „Streszczenie oceny wpływu", dołączony do wniosku dotyczącego dyrektywy w sprawie ataków na systemy informatyczne.

([11]) **Chmury obliczeniowe** (ang. *cloud computing*) dotyczą udostępniania zasobów obliczeniowych (na żądanie lub automatycznie) przez internet. Usługi chmur obliczeniowych prezentowane są użytkownikom w prosty i łatwy do zrozumienia sposób, a użytkownicy nie muszą posiadać technicznej wiedzy o sposobie ich świadczenia. Za pomocą platform opartych na chmurach obliczeniowych można by wszystkim użytkownikom podłączonym do internetu w Europie dostarczać najnowocześniejsze oprogramowanie antywirusowe i dotyczące bezpieczeństwa w sieci, zmniejszając tym samym potrzebę indywidualnego zabezpieczania się poszczególnych użytkowników.

([12]) **Przetwarzanie rozproszone** (ang. *grids*) to forma rozproszonego obliczania, w której „wirtualny superkomputer" złożony jest z wielu komputerów luźno połączonych w sieć, które pracują wspólnie nad wykonaniem bardzo dużych zadań. Technologie przetwarzania rozproszonego mogą stanowić platformę systemów analizy cyberataków i reakcji na nie w czasie rzeczywistym.

([13]) Opinia EKES-u w sprawie nowego rozporządzenia ENISA, Dz.U. C 107 z 6.4.2011, s. 58.

1.17 W Europie należy wspierać rozwój silnego sektora bezpieczeństwa informatycznego, aby dorównał on kompetencjom bardzo dobrze finansowanego sektora w Stanach Zjednoczonych ([14]). Na badania i rozwój w dziedzinie bezpieczeństwa cybernetycznego oraz na edukację w tej dziedzinie należy przeznaczać znacznie większe środki.

1.18 Komitet przyjmuje do wiadomości zagwarantowane na mocy Protokołów do Traktatu zwolnienie Wielkiej Brytanii, Irlandii i Danii z obowiązku przyjęcia dyrektywy, której dotyczy wniosek. Bez względu na to zwolnienie Komitet wzywa te państwa członkowskie do jak największej współpracy w ramach przepisów dyrektywy, aby uniemożliwić przestępcom wykorzystywanie luk prawnych w Unii.

2. **Wprowadzenie**

2.1 Obecnie jakość życia i dobrobyt w Europie zależą w dużym stopniu od systemów informatycznych. Ważne jest, by takiemu rosnącemu uzależnieniu towarzyszyły coraz bardziej zaawansowane środki bezpieczeństwa i rygorystyczne prawo, które zapewnia ochronę systemów informatycznych przed atakiem.

2.2 Internet stanowi najistotniejszą platformę społeczeństwa cyfrowego. Zlikwidowanie zagrożeń bezpieczeństwa systemów informatycznych ma decydujące znaczenie dla rozwoju społeczeństwa cyfrowego i gospodarki cyfrowej. Internet obsługuje większą część krytycznej infrastruktury informatycznej, która stanowi bazę informacyjno-komunikacyjną potrzebną do dostarczania podstawowych towarów i świadczenia podstawowych usług. Poważnym problemem są obecnie ataki na systemy informatyczne – systemy rządowe, finansowe, świadczeń socjalnych oraz na infrastrukturę o podstawowym znaczeniu, taką jak infrastruktura umożliwiająca zaopatrzenie w energię elektryczną i w wodę, infrastruktura transportowa, w dziedzinie służby zdrowia i ratownictwa medycznego.

2.3 Struktura Internetu opiera się na wzajemnych połączeniach milionów komputerów, a funkcje przetwarzania danych, łączności i kontroli są rozproszone po całym świecie. Taka rozproszona struktura jest kluczem do stabilności i odporności Internetu, a w razie wystąpienia problemu umożliwia szybkie przywrócenie sprawnego przepływu danych. Oznacza to jednak również, że zakrojonych na szeroką skalę ataków cybernetycznych z brzegowej części sieci przy użyciu np. botnetów może dokonać dowolna osoba mająca taki zamiar i podstawową wiedzę.

2.4 Rozwój technologii informatycznych przyczynił się do zaostrzenia tych problemów, ponieważ obecnie łatwiej jest produkować i rozpowszechniać narzędzia (złośliwe oprogramowanie ([15]) i botnety) z zachowaniem anonimowości przestępców i rozłożeniem odpowiedzialności pomiędzy różnymi państwami. Ze względu na trudności w ściganiu cyberprzestępstw przestępczość zorganizowana może przynosić w tej dziedzinie znaczne zyski przy niewielkim ryzyku.

2.5 Z opracowania przedstawionego w 2009 r. ([16]) na Światowym Forum Gospodarczym wynika, że łączne straty z powodu cyberprzestępczości wynoszą 1 bln USD i szybko rosną, a w sporządzonym ostatnio rządowym raporcie ([17]) oszacowano roczne straty w samej Wielkiej Brytanii na kwotę 27 mld GBP. Wysokie koszty ponoszone z powodu cyberprzestępczości gwarantują podejmowanie zdecydowanych działań, bezwzględne egzekwowanie prawa i wysokie kary dla przestępców.

2.6 Zgodnie ze szczegółowymi informacjami zawartymi w dokumencie roboczym służb Komisji dołączonym do wniosku dotyczącego dyrektywy ([18]) przestępczość zorganizowana i wrogie rządy wykorzystują destrukcyjny potencjał ataków na systemy informatyczne w Unii. Ataki przeprowadzane przy użyciu botnetów stanowią poważne zagrożenie dla funkcjonowania całego państwa i mogą być również wykorzystywane przez terrorystów lub inne osoby do wywierania presji politycznej na państwo.

2.7 Problem ujawnił się podczas ataku na Estonię na przełomie kwietnia i maja 2007 r. W wyniku ataku krytyczna rządowa struktura informatyczna w znacznym stopniu przestała działać, a sektor prywatny poniósł z powodu zakrojonych na wielką skalę ataków znaczne straty w wysokości 19–28 mln EUR oraz poważne koszty polityczne, a skutki ataku utrzymywały się przez wiele dni. Również Litwa i Gruzja ucierpiały na skutek podobnych ataków.

2.8 Globalne sieci łączności są w znacznym stopniu wzajemnie powiązane w wymiarze transgranicznym. Niezwykle istotne jest wspólne podjęcie przez wszystkie 27 państw członkowskich spójnych działań wobec cyberprzestępczości, a szczególnie wobec ataków na systemy informatyczne. Taka międzynarodowa współzależność nakłada na UE obowiązek prowadzenia zintegrowanej polityki ochrony systemów informatycznych przed atakami i karania sprawców.

2.9 W swojej opinii z 2007 r. w sprawie strategii na rzecz bezpiecznego społeczeństwa informacyjnego ([19]) Komitet zalecił przyjęcie wszechstronnego prawodawstwa UE przeciwko cyberprzestępczości. Poza atakami na systemy informatyczne wszechstronne ramy prawne powinny obejmować cyberprzestępstwa finansowe, nielegalne treści w internecie, gromadzenie/przechowywanie/przekazywanie dowodów elektronicznych oraz bardziej szczegółowe przepisy jurysdykcyjne.

2.10 Komitet rozumie, że utworzenie wszechstronnych ram prawnych stanowi bardzo ciężkie zadanie dodatkowo utrudnione brakiem porozumienia politycznego ([20]) oraz problemami wynikającymi z istotnych różnic między państwami członkowskimi co do dopuszczalności dowodów w formie elektronicznej w postępowaniach sądowych. Takie wszechstronne ramy prawne oznaczałybyx jednak maksymalne korzyści wynikające

([14]) Z oficjalnych danych Białego Domu wynika, że rząd Stanów Zjednoczonych w 2010 r. wydał 407 mln USD na badania i rozwój w dziedzinie bezpieczeństwa cybernetycznego oraz edukację w tej dziedzinie i proponuje, aby w roku budżetowym 2012 przeznaczyć na ten cel 548 mln USD; http://www.whitehouse.gov/sites/default/files/microsites/ostp/FY12-slides.pdf.

([15]) Złośliwe oprogramowanie to oprogramowanie stworzone z myślą o potajemnym uzyskaniu dostępu do systemu komputerowego bez świadomej zgody jego użytkownika.

([16]) *Unsecured Economies: Protecting Vital Information* [„Gospodarka bez zabezpieczeń: ochrona podstawowych informacji"] opracowanie sporządzone dla McAfee przez naukowców z Centrum Badawczego i Edukacyjnego w dziedzinie Bezpieczeństwa Informacji przy Purdue University (2009 r.), http://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf.

([17]) Zob. http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime.

([18]) SEC(2010) 1122.

([19]) Opinia EKES-u w sprawie bezpiecznego społeczeństwa informacyjnego, Dz.U. C 97 z 28.4.2007, s. 21 (TEN/254).

([20]) SEC(2010) 1122, ocena wpływu dotycząca COM(2010) 517.

zarówno z instrumentów prawnych, jak i pozaprawnych dla rozwiązania szerokiego spectrum problemów związanych z cyberprzestępczością. Umożliwiłyby również uporanie się z trudnościami związanymi z prawem karnym, a jednocześnie doprowadziły do lepszej współpracy w dziedzinie egzekwowania prawa w Unii. Komitet ponagla Komisję do prowadzenia dalszych prac zmierzających do utworzenia wszechstronnych ram prawnych w odniesieniu do cyberprzestępczości.

2.11 Walka z cyberprzestępczością wymaga specjalnych umiejętności. W swojej opinii w sprawie wniosku dotyczącego rozporządzenia w sprawie ENISA ([21]) Komitet podkreślił znaczenie przeszkolenia personelu organów ścigania. Komitet wyraża zadowolenie z postępów Komisji w tworzeniu platformy szkoleniowej w dziedzinie cyberprzestępczości z udziałem organów ścigania i sektora prywatnego, zgodnie z propozycją przedstawioną w komunikacie COM(2007) 267 ([22]).

2.12 Podmiotami zainteresowanymi bezpieczeństwem cybernetycznym w UE są wszyscy obywatele, których życie może zależeć od usług o kluczowym znaczeniu. Ci sami obywatele są odpowiedzialni za ochronę swojego połączenia z Internetem przed atakami w miarę swoich możliwości. Jeszcze większą odpowiedzialność ponoszą dostawcy technologii i usług TIK, którzy opracowują systemy informatyczne.

2.13 Należyte poinformowanie wszystkich tych zainteresowanych stron o bezpieczeństwie cybernetycznym jest sprawą o decydującym znaczeniu. Ważne dla Europy jest również utworzenie licznego grona ekspertów mających specjalistyczne kompetencje w dziedzinie bezpieczeństwa cybernetycznego.

2.14 W Europie należy wspierać rozwój silnego sektora bezpieczeństwa informatycznego, aby dorównał on kompetencjom bardzo dobrze finansowanego sektora w Stanach Zjednoczonych ([23]). Na badania i rozwój w dziedzinie bezpieczeństwa cybernetycznego oraz na edukację w tej dziedzinie należy przeznaczyć znacznie większe środki.

3. **Streszczenie wniosku dotyczącego dyrektywy**

3.1 Wniosek ma na celu zastąpienie decyzji ramowej Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne ([24]). Decyzja ramowa stanowiła, jak czytamy w jej motywach, odpowiedź na potrzebę usprawnienia współpracy między organami sądowymi i innymi właściwymi organami, włącznie z policją i innymi wyspecjalizowanymi organami ścigania państw członkowskich, poprzez zbliżanie w państwach członkowskich przepisów prawa karnego w dziedzinie ataków na systemy informatyczne. Wprowadziła ona przepisy UE dotyczące postępowania w przypadku przestępstw takich jak nielegalne uzyskiwanie dostępu do systemów informatycznych, nielegalne ingerowanie w te systemy oraz nielegalne ingerowanie w dane, jak również szczegółowe przepisy dotyczące odpowiedzialności osób prawnych, jurysdykcji i wymiany informacji. Państwa członkowskie zobowiązane były do przedsięwzięcia środków niezbędnych w celu wykonania przepisów decyzji ramowej do dnia 16 marca 2007 r.

3.2 W dniu 14 lipca 2008 r. Komisja opublikowała sprawozdanie z wykonania decyzji ramowej ([25]). We wnioskach stwierdzono, że liczne „ataki, jakie miały miejsce w całej Europie od czasu przyjęcia decyzji ramowej, uświadamiają wiele rodzących się zagrożeń, a w szczególności pojawienie się zjawiska masowych jednoczesnych ataków na systemy informatyczne oraz wzrost przestępczego wykorzystania tzw. botnetów". Ataki te nie znajdowały się w centrum uwagi w momencie przyjmowania decyzji ramowej.

3.3 W przedmiotowym wniosku uwzględniono nowe metody popełniania cyberprzestępstw, w szczególności wykorzystanie botnetów ([26]). Bardzo trudno jest namierzać sprawców, ponieważ komputery składające się na botnet i wykorzystywane do ataku mogą znajdować się w innymi miejscu niż sam przestępca.

3.4 Ataki przeprowadzane za pośrednictwem botnetu wykonywane są często na wielką skalę. Ataki na wielką skalę to ataki przeprowadzane z wykorzystaniem narzędzi oddziałujących na znaczną liczbę systemów informatycznych (komputerów) bądź ataki powodujące znaczne szkody, np. polegające na zakłóceniu świadczenia usług realizowanych przez system, powodujące koszty finansowe, utratę danych osobowych itp. Szkody powodowane atakami na wielką skalę mają istotny wpływ na funkcjonowanie samego celu tych ataków lub negatywnie oddziałują na jego środowisko pracy. W tym kontekście uważa się, że „duży botnet" jest siecią zdolną do wyrządzenia poważnych szkód. Trudno jest zdefiniować botnety pod względem wielkości, jednak największe odnotowane wśród nich szacowano na od 40 do 100 tys. połączeń (tzn. zainfekowanych komputerów) w ciągu 24 godzin ([27]).

3.5 Przepisy decyzji ramowej wykazują szereg braków, pod względem tendencji w zakresie skali i liczby przestępstw (cyberataków). Dyrektywa zbliża przepisy wyłącznie w odniesieniu do ograniczonej liczby przestępstw, równocześnie nie likwidując w pełni potencjalnego zagrożenia, jakie stwarzają dla społeczeństwa ataki na wielką skalę. Nie uwzględnia ona również wystarczająco wagi tych przestępstw i kar za nie nakładanych.

3.6 Przedmiotowa dyrektywa ma na celu zbliżenie przepisów prawa karnego w państwach członkowskich w dziedzinie ataków na systemy informatyczne oraz poprawę współpracy między organami sądowymi i innymi właściwymi organami, w tym policją i pozostałymi wyspecjalizowanymi organami ścigania państw członkowskich.

([21]) Opinia EKES-u dotycząca nowego rozporządzenia w sprawie agencji ENISA, dotychczas niepublikowana w Dz.U. (Dz.U. C 107 z 6.4.2011, s. 58).

([22]) COM(2007) 267 „W kierunku ogólnej strategii zwalczania cyberprzestępczości".

([23]) Z oficjalnych danych Białego Domu wynika, że rząd Stanów Zjednoczonych w 2010 r. wydał 407 mln USD na badania i rozwój w dziedzinie bezpieczeństwa cybernetycznego oraz edukację w tej dziedzinie i proponuje, aby w roku budżetowym 2012 przeznaczyć na ten cel 548 mln USD, http://www.whitehouse.gov/sites/default/files/microsites/ostp/FY12-slides.pdf.

([24]) Dz.U. L 69 z 16.3.2005, s. 68.

([25]) Sprawozdanie Komisji dla Rady na podstawie art. 12 decyzji ramowej Rady z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, COM (2008) 448.

([26]) Zob. przyp. 6 powyżej.

([27]) Jednostką pomiaru używaną powszechnie do szacowania wielkości botnetów jest liczba połączeń w okresie 24 godzin.

3.7 Ataki na systemy informatyczne, w szczególności ze względu na zagrożenie ze strony przestępczości zorganizowanej, są coraz bardziej niebezpieczne, narastają również obawy o możliwość ataków terrorystycznych lub mających podłoże polityczne ukierunkowanych na systemy informatyczne stanowiące element infrastruktury krytycznej państw członkowskich i Unii. Zagraża to dążeniom do zapewnienia bezpieczniejszego społeczeństwa informacyjnego oraz przestrzeni wolności, bezpieczeństwa i sprawiedliwości, dlatego też wymaga reakcji na szczeblu Unii Europejskiej.

3.8 Istnieją dowody wskazujące na tendencję do coraz bardziej niebezpiecznych i ponawianych ataków na wielką skalę przeprowadzanych na systemy informatyczne o zasadniczym znaczeniu dla państw lub poszczególnych funkcji w sektorze publicznym lub prywatnym. Tendencji tej towarzyszy tworzenie coraz bardziej wyrafinowanych narzędzi, z których przestępcy mogą korzystać do przeprowadzania różnego rodzaju cyberataków.

3.9 Wspólne definicje w tej dziedzinie, w szczególności definicje systemów informatycznych oraz danych komputerowych, mają istotne znaczenie dla zapewnienia przyjęcia przez państwa członkowskie spójnego podejścia do stosowania przedmiotowej dyrektywy.

3.10 Zachodzi potrzeba zapewnienia wspólnego podejścia do kwestii znamion przestępstwa poprzez powszechne wprowadzenie definicji przestępstw polegających na nielegalnym dostępie do systemu informatycznego, nielegalnym ingerowaniu w system, nielegalnym ingerowaniu w dane oraz nielegalnym przechwytywaniu.

3.11 Państwa członkowskie powinny przewidzieć kary za ataki na systemy informatyczne. Kary te powinny być skuteczne, proporcjonalne i odstraszające.

3.12 Dyrektywa uchyli wprawdzie decyzję ramową 2005/222/WSiSW, jednak zachowa jej obecne przepisy z dodaniem następujących nowych elementów:

(a) Penalizuje wytwarzanie, sprzedaż, dostarczanie w celu użytkowania, przywóz, dystrybucję lub inne sposoby udostępniania urządzeń/narzędzi służących do popełniania przestępstw.

(b) Obejmuje okoliczności obciążające:

— przeprowadzanie ataków na wielką skalę – problem botnetów lub podobnych narzędzi zostałby uwzględniony poprzez wprowadzenie nowej okoliczności obciążającej – czyn polegający na stworzeniu botnetu lub innego podobnego narzędzia stanowi okoliczność obciążającą przy popełnianiu przestępstw wyszczególnionych w obecnej decyzji ramowej;

— jeśli takie ataki popełniane są przez sprawcę ukrywającego swoją prawdziwą tożsamość, a podejrzenia obciążają prawowitego właściciela tożsamości.

(c) Dyrektywa wprowadza pojęcie nowego przestępstwa, a mianowicie „nielegalne przechwytywanie".

(d) Wprowadza środki, które mają poprawić współpracę europejskich wymiarów sprawiedliwości w sprawach karnych poprzez udoskonalenie obecnej struktury całodobowych punktów kontaktowych działających przez siedem dni w tygodniu ([28]).

(e) Dyrektywa stanowi odpowiedź na potrzebę dostarczania danych statystycznych dotyczących cyberprzestępczości, w tym przestępstw, o których mowa w obowiązującej decyzji ramowej, oraz nowo dodanego „nielegalnego przechwytywania".

(f) W definicjach przestępstw wyszczególnionych w art. 3, 4 i 5 (nielegalny dostęp do systemów informatycznych, nielegalne ingerowanie w system oraz nielegalne ingerowanie w dane) dyrektywa zawiera przepis umożliwiający kryminalizację wyłącznie tych „przypadków, które nie są przypadkami mniejszej wagi" w procesie transpozycji dyrektywy do prawa krajowego.

Bruksela, 4 maja 2011 r.

Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego
Staffan NILSSON

([28]) Wprowadzonej konwencją oraz decyzją ramową 2005/222/WSiSW w sprawie ataków na systemy informatyczne.