Anna Kańciak

Problematyka cyberprzestępczości w Unii Europejskiej

Kwoty utraconych pieniędzy z powodu przestępstw popełnianych w cyberprzestrzeni, o czym dowiadujemy się, analizując statystyki, na każdym robią ogromne wrażenie, niezależnie czy odbiorcą tych danych jest ekspert, czy zwykły obywatel. Nie trudno się więc dziwić, że z powodu straconych rocznie miliardów dolarów kwestia bezpieczeństwa w cyberprzestrzeni staje się centralnym punktem zainteresowania decydentów, służb ochrony porządku publicznego oraz przedstawicieli sektora prywatnego. Tak szerokie zainteresowanie powoduje, że wymiar cyberprzestępczości nie jest wyłącznie prawno-karny czy informatyczny, ale również społeczny i gospodarczy[1].

Ponadto uwagę opinii społecznej zwracają również tzw. cyberataki na obiekty należące do infrastruktury krytycznej czy na strony internetowe organów administracji państwowej, które w połączeniu z ponadnarodowym sporem o ACTA[2] powodują że społeczność międzynarodowa stanęła wobec nowego niebezpieczeństwa, jakim jest cyberprzestępczość.

Już po kilkuzdaniowym wstępie można mieć wyobrażenie, jakie trudności pojawiają się podczas analizowania przestępstw popełnianych w cyberprzestrzeni. Od kwestii terminologicznych przez zakres przedmiotowy i podmiotowy cyberprzestępstw po kluczowe pytanie o istotę i powszechnie przypisywaną cechę nowości temu zjawisku.

Z uwagi na zakres artykułu nie jest możliwe udzielenia odpowiedzi na wszystkie pytania i rozstrzygnięcie wątpliwości. Dlatego też, po krótkim wyjaśnieniu istoty przestępstw w cyberprzestrzeni, zostanie przedstawiony zarys podejmowanych obecnie działań w Unii Europejskiej zapobiegających tego rodzaju przestępczości i ją zwalczających.

Międzynarodowy wymiar prac nad cyberprzestępczością

„Cyberprzestępczość" jest pojęciem, które dość szybko zostało włączone do powszechnego użycia. Nie stanowi również większej trudności intuicyjne zdefiniowanie go. Jednak z uwagi na swoją wieloaspektowość, zarówno po stronie doktryny, jak i praktyki, pojawiło się wiele sporów i niejasności terminologicznych.

Na poziomie krajowym wyjaśnienie tego pojęcia zostało zawarte w kluczowym dla tej problematyki dokumencie – Rządowym Programie Ochrony Cyberprzestrzeni

---

[1] R Lusawa., *Ekonomiczno-społeczne uwarunkowania cyberprzestępczości, wersja elektroniczna* [online], http://wbs.ks.net.pl/pliki/Lusowa9.pdf., s. 2 [dostęp: 2 VI 2012].

[2] Umowa handlowa dotycząca zwalczania obrotu towarami podrabianymi (*Anti-Counterfeiting Trade Agreement* – ACTA) – umowa międzynarodowa mająca ustalić międzynarodowe standardy w walce z naruszeniami własności intelektualnej. Szerzej: *Wniosek. Decyzja Rady w sprawie zawarcia umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi między Unią Europejską i jej Państwami Członkowskimi, Australią, Kanadą, Japonią, Republiką Korei, Meksykańskimi Stanami Zjednoczonymi, Królestwem Marokańskim, Nową Zelandią, Republiką Singapuru, Konfederacją Szwajcarską i Stanami Zjednoczonymi Ameryki*, Bruksela, dnia 24.06.2011 r., KOM(2011) 380 wersja ostateczna.

RP – i oznacza *czyn zabroniony popełniony w obszarze cyberprzestrzeni*[3]. Z kolei „cyberprzestrzeń" określono jako cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami między nimi oraz relacjami z użytkownikami[4]. Dodatkowo program wprowadza, na potrzeby realizacji jego założeń, definicję „cyberprzestrzeni RP"[5].

Sama problematyka cyberprzestępczości nie jest zjawiskiem zupełnie nowym. Zainteresowanie tym tematem pojawiło się już na początku XX wieku, jednak dowodem podjęcia faktycznych prac w przedmiotowym zakresie jest ogłoszona w 2001 r. Konwencja Rady Europy o cyberprzestępczości[6]. Co prawda w konwencji nie zdefiniowano wprost pojęcia cyberprzestępczości, ale wskazano na zagrożenia wymagające wspólnego działania w ramach ochrony sieci informatycznych i informacji elektronicznych przed ich wykorzystaniem w celu popełniania przestępstw[7]. Poza środkami, jakie należy podjąć na szczeblu krajowym, zwrócono w niej uwagę na trzy rodzaje przestępstw[8]:

1) komputerowe:
   – fałszerstwo komputerowe,
   – oszustwo komputerowe,
2) ze względu na charakter zawartych informacji:
   – przestępstwa związane z pornografią dziecięcą,
3) związane z naruszeniem praw autorskich i praw pokrewnych.

Przedmiotowa konwencja, która z perspektywy kilkunastu lat od momentu jej przyjęcia i zdobytych doświadczeń może wydawać się bardzo ogólna i nieprecyzyjna, jest solidną podstawą do tworzenia wspólnej polityki krajów członkowskich[9] Rady Europy w zakresie zwalczania cyberprzestępczości. Ponadto wciąż jest punktem odniesienia wielu rozwiązań prawnych w pracach nad przeciwdziałaniem zagrożeniom cyberbezpieczeństwa i zwalczaniem tych zagrożeń. Dowodem na to są dokumenty i programy pojawiające się na forum Unii Europejskiej. Najnowszym dokumentem jest komunikat Komisji Europejskiej z 28 marca 2012 r. wprowadzający definicję „cyberprzestępczości" rozumianej jako *wysokodochodowa, niskiego ryzyka forma przestępczej działalności, która coraz bardziej staje się powszechna i szkodliwa*[10].

Jednak wyjaśnienie terminu cyberprzestępczości pojawiło się już wcześniej w *Europejskiej agendzie cyfrowej*, dokumencie Komisji Europejskiej, w którym okre-

---

[3] *Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011–2016*, MSWiA, Warszawa 2010, s. 6,. http://bip.msw.gov.pl/portal/bip/6/19057, s. 6 [dostęp: 24 VI 2012].

[4] Tamże.

[5] Cyberprzestrzeń RP to cyberprzestrzeń w obrębie terytorium państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe), tamże, s. 6.

[6] *Konwencja o cyberprzestępczości* (*Convention on cybercrime*), Budapeszt, 23 listopada 2001 r., ETS nr 185.

[7] Tamże, s. 1.

[8] Tamże, s. 3–6.

[9] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, Warszawa 2010, Wolters Kluwer, s. 81.

[10] *Komunikat Komisji do Rady i Parlamentu Europejskiego. Zwalczanie przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością*, Bruksela, dnia 28.03.2012, KOM(2012) 140 wersja ostateczna, s. 2.

ślono ją jako *nową formę przestępczości obejmującą między innymi wykorzystywanie dzieci, kradzież tożsamości i ataki cybernetyczne*[11].

Analizując przytoczone sposoby definiowania pojęcia cyberprzestępczości, można zuważyć nie tylko niejednolity stopień szczegółowości tych definicji, ale również – z uwagi na okoliczności powstawania dokumentów, w których są zawarte – różny ich zakres przedmiotowy. Dodatkowo należy również przywołać charakterystykę cyberprzestępczości przedstawioną w obszernym materiale Parlamentu Europejskiego, która została opracowana na podstawie doświadczeń państw członkowskich UE. Parlament Europejski dokonując analizy zebranych materiałów oraz korzystając z dorobku całej Unii w zakresie cyberprzestępczości, wskazał, że jako jedna z największych obaw i zagrożeń dla zinformatyzowanego współczesnego świata, charakteryzuje się ona:

- ogromną skalą,
- niejednoznaczną naturą podmiotów w cyberprzestrzeni,
- używaniem w dużej mierze podobnych technik ataków,
- zaawansowaniem i wysokim poziomem dochodowości,
- dużym zróżnicowaniem i trudnością w przeciwdziałaniu i zwalczaniu[12].

Rozpatrując działania Unii Europejskiej w zakresie ochrony cyberprzestrzeni, przede wszystkim należy zwrócić uwagę na dwutorowość podejmowanych prac, w czym również jest upatrywana słabność wszelkich inicjatyw. Podział prac UE został dokonany na dwa obszary ze względu na krytetium przedmiotu:

1) zwalczanie cyberataków (włączając w to cyberprzestępczość i cyberterroryzm),
2) utrzymanie ochrony:
   – infrastruktury krytycznej (Critical Infrastructure Security – CIS),
   – bezpieczeństwa sieci i informacji (Network and Information Security – NIS),
   – krytycznej infrastruktury informatycznej (Critical Information Infrastructure Protection – CIIP)[13].

Zgodnie podziałem na kwestie ochrony z jednej strony, a zwalczanie cyberataków z drugiej, są przygotowywane kluczowe unijne programy i strategie. Jednak z uwagi na pewien wspólny zakres odnoszący się chociażby do definiowania podstawowych pojęć, wielokrotnie dochodzi do powielania prac i braku jednolitości instytucji unijnych w podejściu do tej problematyki.

Zanim jednak podda się krytyce wysiłki UE podejmowane w celu przeciwdziałania cyberprzestępczości, należy zwrócić uwagę na bardzo istotną kwestię. Zauważona powyższej rozbieżność w podejściu i próbach uregulowania zagadnienia ochrony cyberprzestrzeni wynika z traktatowego[14] podziału obszarów, w ramach których odpowiednie podmioty wypracowują nowe narzędzia i mechanizmy działania.

W zakresie pierwszego kierunku zmierzającego do zwalczania cyberprzestępstw jako czynów prawnie zabronionych, niosących za sobą konkretny wymiar karny

---

[11] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Europejska agenda cyfrowa*, Bruksela, dnia 26.08.2010, KOM(2010) 245 wersja ostateczna/2, s. 6.

[12] *Cybersecurity and cyberpower: concepts, conditions and capabilities for cooperation for action within the EU*, Policy Department Directorate-General for External policies of the Union, EXPO/B/SEDE/FWC/2009-01/LOT6/09, April 2009 r., s. 7.

[13] Tamże, s. 27.

[14] Stan prawny wprowadzony *Traktatem z Lizbony zmieniającym Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską*", Dz.Urz. UE C 306 z 17 grudnia 2007, s. 1.

i społeczny, wszelkie działania podlegają przepisom Tytułu V (*Przestrzeń wolności, bezpieczeństwa i sprawiedliwości*) *Traktatu o funkcjonowaniu Unii Europejskiej* (TFUE)[15]. Dlatego też, zgodnie z przedmiotowym i kompetencyjnym podziałem struktur unijnych, problematyka ta jest podejmowana przez Dyrekcję Generalną do Spraw Wewnętrznych. Z kolei ochrona infrastruktury krytycznej i teleinformatycznej, należąca do kompetencji Dyrekcji Generalnej ds. Społeczeństwa Informatycznego (DG INFOSO)[16], jest uregulowana w Tytule VIII (*Polityka gospodarcza i pieniężna*) TFUE[17].

Każdy z tych dwóch tematów doczekał się szczegółowych regulacji i planów działania. Jednak z uwagi na zakres artykułu zostanie w nim przedstawiona problematyka cyberprzestępczości w kontekście przeciwdziałania temu zjawisku i jego zwalczania, czyli pierwszemu z przedstawionych obszarowi.

W ramach kierunku zajmującego się cyberprzestępczością, realizowanego zgodnie z przepisami *Przestrzeni wolności, bezpieczeństwa i sprawiedliwości,* przede wszystkim należy zwrócić uwagę na *Decyzję Ramową Rady w sprawie ataków na systemy informatyczne* przyjętą w 2005 r.[18] stanowiącą kamień milowy w zwalczaniu tego procederu. Wymaga ona od państw członkowskich wprowadzenia do krajowych systemów prawnych regulacji dotyczących skutecznego działania przeciwko podstawowym typom cyberataków. Ponadto, co ważniejsze, wprowadza wspólną definicję takich ataków. Przyjmując tę decyzję, państwa zgodziły się na wspólne wyjaśnienia takich czynów zabronionych, jak:

- nielegalny dostęp do systemów informatycznych,
- nielegalna ingerencja w system,
- nielegalna ingerencja w dane[19].

Kolejne kroki podjęto w następstwie ataków terrorystycznych w Londynie i Madrycie. Wtedy to cała uwaga instytucji i agencji unijnych oraz organizacji międzynarodowych zajmujących się zapewnianiem bezpieczeństwa skupiła się wokół problematyki zagrożenia atakami terrorystycznymi. Po analizach tamtych wydarzeń zaczęto identyfikować słabe punkty całego systemu bezpieczeństwa oraz rozważać możliwości ograniczania zakresu praw i obowiązków na rzecz *porządku publicznego, tj. zachowania bezpieczeństwa narodowego (tj. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego czy też zapobiegania, dochodzenia, wykrywania i ścigania przestępstw lub nielegalnego wykorzystania systemów łączności elektronicznej*[20]. Zwrócono uwagę na stopień dostępności do danych i przygotowano – jak się później okazało, kontrowersyjny – dokument w sprawie retencji danych[21], zwany w skrócie Europejską Dyrektywą. Konieczność wprowadzenia takich regulacji wynikała z dąże-

---

[15] Wersja skonsolidowana *Traktatu o funkcjonowaniu Unii Europejskiej* (TFUE), Dz.Urz. UE C 83 z 30 marca 2010 r., s. 73–85.

[16] Od 1 lipca 2012 r. zmienione na DG CONNECT – *Directorate General for Communications Networks, Content and Technology.*

[17] *Traktat o funkcjonowaniu Unii Europejskiej…*, s. 78–79.

[18] *Decyzja Ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne*, Dz.Urz. UE L 69 z 16 marca 2005 r.

[19] Tamże, s. 69.

[20] *Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE*, Dz.Urz. UE L 105 z 15 marca 2006 r., s. 54.

[21] Tamże.

nia do nałożenia na dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności obowiązków w zakresie przechowywania pewnych danych przez nich generowanych lub przetwarzanych, aby zapewnić dostępność tych danych w razie dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego[22]. Drugim celem, który pośrednio przyświecał pomysłodawcom tego dokumentu, było zwiększenie efektywności środków służących zwalczaniu cyberprzestępczości oraz innych form przestępczej aktywności.

Z kolei w 2007 r. Komisja Europejska przygotowała Komunikat pod nazwą *W kierunku ogólnej strategii zwalczania cyberprzestępczości*[23], obecnie dość rzadko przytaczany z uwagi na niepodjęcie dalszych prac na forum unijnym nad przedmiotową strategią. Warto jednak poświęcić mu chwilę uwagi ze względu na poruszone w nim zagadnienia mające istotne znaczenie w działaniach w zakresie przeciwdziałania cyberprzestępczości.

W komunikacie, poza ogólnym celem, jakim jest zwalczanie cyberprzestępczości na poziomie krajowym, unijnym i międzynarodowym oraz próbą zdefiniowania cyberprzestępczości i określeniem jej wymiaru i tendencji, za najważniejsze inicjatywy Komisja i państwa członkowskie uznały:

- koncentrację działań na ściganiu przestępstw oraz na aspektach prawnokarnych zwalczania przestępczości,
- uzupełnienie innych działań UE poprawiających ogólne bezpieczeństwo w przestrzeni wirtualnej o elementy przyszłej strategii zwalczania cyberprzestępczości,
- 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[24].

Tego rodzaju założenia w zestawieniu z praktyczną ich realizacją mogą spotkać się z pewną krytyką. Należy jednak mieć na uwadze nie tylko procedury obowiązujące w instytucjach unijnych, ich traktatowy zakres kompetencyjny, lecz także skutki tego rodzaju dokumentów i ich przełożenie w późniejszych działaniach na poziomie UE.

Wynikiem podjętych prac zmierzających do zidentyfikowania kluczowych obszarów wymagających wspólnych działań na poziomie międzynarodowym, w ramach przestrzeni wolności, bezpieczeństwa i sprawiedliwości, było przyjęcie w 2009 r. *Programu sztokholmskiego*[25] będącego najnowszym programem pięcioletnim (na lata 2010–2014[26]), w którym przez wyznaczanie obszarów priorytetowych sprecyzowano postanowienia Traktatu z Lizbony dotyczące tego zagadnienia. Należy podkreślić, że

---

[22] Tamże, art. 1.

[23] *Komunikat Komisji do Parlamentu Europejskiego, Rady i Komitetu Regionów. W kierunku ogólnej strategii zwalczania cyberprzestępczości,* Bruksela, dnia 22.05.2007, KOM (2007) 267 wersja ostateczna.

[24] Tamże, s. 4.

[25] *Informacje instytucji, organów i jednostek organizacyjnych Unii Europejskiej, Rada Europejska Program sztokholmski – otwarta i bezpieczna Europa dla dobra i ochrony obywateli*, Dz.Urz. UE C 115 z 4 maja 2010 r., s. 1.

[26] Przyjęty przez Radę Europejską na posiedzeniu 10–11 grudnia 2009 r., zaczął obowiązywać od 1 stycznia 2010 r. Jest to trzeci z kolei program obejmujący szeroki zakres tematyczny bezpieczeństwa, począwszy od zarządzania zewnętrznymi granicami UE do sądowej współpracy w sprawach karnych i cywilnych. Pierwszy powstał w Tempere (1999–2004), kolejny to Program haski (2005–2009). Więcej: *Unia Europejska. System prawny, porządek instytucjonalny, proces decyzyjny*, J. Barcz (red. nauk.), Warszawa 2009, KSAP & EuroPres. s. 657.

dokument ten to olbrzymi krok w zwiększaniu bezpieczeństwa wewnętrznego UE, gdyż zawiera wiele odwołań do ochrony cyberprzestrzeni. Nie tylko zalicza cyberprzestępczość do sześciu głównych priorytetów dla całej UE, lecz także wzywa do:

- propagowania prawodawstwa, które zapewnia bardzo wysoki poziom bezpieczeństwa sieci i umożliwia szybsze reagowanie w przypadku ataków cybernetycznych,
- przyspieszenia procesu ratyfikacyjnego *Konwencji o cyberprzestępczości*[27],
- udzielenia pełnego poparcia krajowym podmiotom powiadamiania o zagrożeniach, odpowiedzialnym za walkę z cyberprzestępczością,
- współpracy z państwami spoza Unii,
- wzmocnienia (usprawnienia) partnerstwa publiczno-prywatnego,
- poprawy współpracy sądowej w sprawach dotyczących cyberprzestępczości[28].

Kolejnym krokiem Komisji Europejskiej było przygotowanie wniosku Dyrektywy Parlamentu Europejskiego i Rady dotyczącej ataków na systemy informatyczne[29], który był związany z wdrożeniem i zastosowaniem postanowień wspomnianej już Decyzji Ramowej z 2005 r. w sprawie ataków na systemy informatyczne. W wyniku przeprowadzonego przeglądu okazało się, że *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*[30]. Wniosek został, co prawda z pewnymi poprawkami, pozytywnie przyjęty przez Parlament Europejski[31]. Obecnie trwają prace w Komisji Europejskiej nad jego zaktualizowaniem, uzupełnieniem o opinię Parlamentu oraz rozpoczęciem i przeprowadzeniem procedury legislacyjnej tak, aby akt wszedł w życie najpóźniej na początku 2013 r.

Z kolei drugim dokumentem o dość dużym poziomie ogólności, choć kluczowym z punktu widzenia ochrony bezpieczeństwa wewnętrznego, jest Strategia Bezpieczeństwa Wewnętrznego[32]. Odnosi się ona wprost do cyberprzestępczości, którą zaliczono

---

[27] Polska podpisała Konwencję 23 listopada 2001 r., jednak nie została ona dotychczas ratyfikowana. [podkreślenie aut. art.]. Prace legislacyjne podjęte w Polsce po podpisaniu konwencji doprowadziły do zgodności prawa krajowego z większością jej przepisów. Podobna sytuacja jest z *Protokołem dodatkowym do Konwencji o cyberprzestępczości dotyczącym kryminalizacji działań o charakterze rasistowskim i ksenofobicznym popełnianych przy użyciu systemów komputerowych*, który Polska podpisała 21 lipca 2003 r. Więcej: http://bip.ms.gov.pl/pl/ministerstwo/wspolpraca-miedzynarodowa/rada-europy/konwencje-rady-europy-z-obszaru-sprawiedliwosc-i-sprawy-wewnetrzne-podpisaneratyfikowane-przez-polske/ [dostęp: 17 VI 2012].

[28] *Informacje instytucji, organów i jednostek organizacyjnych*…, s. 15–23.

[29] *Wniosek. Dyrektywa Parlamentu Europejskiego i Rady dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW*, Bruksela, dnia 30.09.2010 r., KOM(2010)517 wersja ostateczna, 2010/0273 (COD).

[30] Tamże, s. 1. 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). Owe komputery „zombie" można kontrolować – często bez wiedzy użytkowników zainfekowanych komputerów – z innego komputera* […] nazywanego również „centrum dowodzenia i kontroli" (*command-and-control centre*). Szerzej: tamże, s. 2 (*Uzasadnienie pkt 1.*).

[31] *Opinia Komisji Spraw Zagranicznych dla Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową Rady 2005/222/WSiSW, z 28.11.2011 r.*, [COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)] [online], http://www.europarl.europa.eu/meetdocs/2009_2014/documents/afet/ad/883/883545/883545pl.pdf, 2010/0273(COD).

[32] *Komunikat Komisji do Parlamentu Europejskiego i Rady. Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy*, Bruksela, dnia 22.11.2010 r., KOM(2010) 673 wersja ostateczna (dok. 16797/10 JAI 990 z 23.11.2010 r.). Zgodnie z założeniem Programu

do pięciu strategicznych celów dla bezpieczeństwa wewnętrznego UE z uwagi na fakt, że Europa ze względu na zaawansowaną infrastrukturę Internetu, wysoką liczbę jego użytkowników oraz przekazywane przez Internet oszczędności i system płatności jest kluczowym celem dla cyberprzestępców. Wymaga to jeszcze lepszej ochrony zarówno obywateli, przedsiębiorców czy rządów, jak i infrastruktury krytycznej[33]. Mając na uwadze zadania stawiane Strategii przez *Program sztokholmski*[34], zakłada się w niej podjęcie następujących kroków[35]:

1) do 2013 r. ustanowienie centrum ds. cyberprzestępczości w UE, które pomoże wzmocnić analityczne i operacyjne zdolności dochodzeniowo-śledcze oraz przyczyni się do zwiększenia współpracy z państwami trzecimi,
2) zapewnienie, w toku postępowań dochodzeniowo-śledczych, wspólnych standardów dla policji, sądów, prokuratorów,
3) w zakresie współpracy z sektorem przemysłowym, w celu ochrony i wzmocnienia pozycji obywateli, zapewnienie systemu raportowania o incydentach w cyberprzestrzeni,
4) w celu poprawy zdolności zwalczania przestępstw w cyberprzestrzeni:
   – utworzenie do 2012 r. sprawnego Centrum Reagowania na Incydenty Komputerowe UE (EU CERT)[36],
   – połączenie do 2012 r. krajowych (rządowych) zespołów CERT działających w państwach członkowskich; będzie to ważnym instrumentem w utworzeniu do 2013 r. Europejskiego System Wymiany Informacji i Powiadamiania (*European Information Sharing and Alert System* – EISAS) dla szerszej rzeszy odbiorców,
   – rozwój krajowych programów reagowania i przeprowadzenie regularnych ćwiczeń na poziomie krajowym i europejskim z zakresu reagowania na incydenty i naprawy szkód.

Ostatnim dokumentem, co prawda dość ogólnie odnoszącym się do problematyki cyberprzestępczości, ale bezpośrednio wiążącym się z wcześniejszym dokumentem określającym wstępną strategię pracy służącą zwalczaniu cyberprzestępczości[37], jest projekt konkluzji Rady na temat planu wdrażania zorganizowanej strategii walki z cyber-

sztokholmskiego nowa strategia powinna uwzględniać postanowienia Europejskiej Strategii Bezpieczeństwa przyjętej przez Radę Europejską 12 grudnia 2003 r., która dotyczy bezpieczeństwa Europy w wymiarze zewnętrznym, często nazywaną Europejską Strategią Bezpieczeństwa (European Security Strategy).

[33] Tamże, s. 4.

[34] *W celu zwiększenia bezpieczeństwa w Europie strategia powinna mieć na celu zacieśnienie współpracy w dziedzinie egzekwowania prawa, zarządzania granicami, ochrony ludności, zarządzania katastrofami, jak również współpracy wymiarów sprawiedliwości w sprawach karnych*, szerzej: *Informacje instytucji, organów i jednostek organizacyjnych Unii Europejskiej, Rada Europejska Program sztokholmski – otwarta i bezpieczna Europa dla dobra i ochrony obywateli*, Dz.Urz. UE C 115 z 4 maja 2010 r., s. 5.

[35] *Komunikat Komisji do Parlamentu Europejskiego i Rady. Strategia bezpieczeństwa wewnętrznego…*, s. 9–10.

[36] Testowa wersja Centrum Reagowania na Incydenty Komputerowe (*Computer Emergency Response Pre-configuration Team* – CERT-EU) powstała 1 czerwca 2011 r. Centrum składa się z ekspertów ds. bezpieczeństwa IT z głównych instytucji unijnych: Komisji Europejskiej, Parlamentu Europejskiego, Sekretariatu Generalnego Rady UE, Komitetu Regionów, Komitetu Ekonomiczno-Społecznego. Po roku od jego utworzenia, po pozytywnej opinii wydanej po przeprowadzeniu przeglądu, została wydana decyzja o ustanowieniu od 11 września 2012 r. w pełni funkcjonującego CERT-u UE. Szerzej: http://www.enisa.europa.eu/activities/cert/background/inv/cert-eu [dostęp: 17 XII 2012].

[37] *Projekt konkluzji Rady w sprawie uzgodnionej strategii pracy i konkretnych środków służących zwalczaniu cyberprzestępczości*, dok. 15569/08 ENFOPOL 224 CRIMORG 190. W konkluzjach zwrócono się do państw członkowskich i Komisji, aby wprowadziły środki opracowane na podstawie analizy zaist-

przestępczością[38]. Wskazano w nim, jakie działania należy podjąć, aby zrealizować postanowienia strategii, której celem jest dostosowanie sposobów eliminowania cyberprzestępczości w zależności od rodzaju przestępstw popełnianych drogą elektroniczną: pornografii dziecięcej, działalności terrorystycznej, ataków na sieci elektroniczne, oszustw, kradzieży tożsamości itd.[39] W perspektywie krótkoterminowej, zgodnie z dokumentem, należy zwrócić uwagę na działania zmierzające do zweryfikowania i zintensyfikowania prac Europejskiej Platformy ds. Walki z Cyberprzestępczością[40] tak, aby ułatwić gromadzenie, wymianę i analizowanie informacji[41].

Z kolei w perspektywie średnioterminowej przede wszystkim zwrócono uwagę na konieczność ratyfikacji Konwencji o cyberprzestępczości z 2001 r., a następnie na podniesienie standardów procedur szkolenia policji, sędziów, prokuratorów i służb kryminalistycznych ułatwiającego prowadzenie czynności procesowych w dziedzinie cyberprzestępczości. Konieczne jest również propagowanie procesu zharmonizowania różnych całodobowych sieci oraz punktów kontaktowych dla organów ochrony porządku publicznego, eliminując nakładanie się działań podejmowanych na forach współpracy międzynarodowej takich, jak np. G8 i Interpol[42].

Europejskie Centrum ds. Walki z Cyberprzestępczością (*European Cybercrime Centre* – EC3)

Wspomniane postulaty, w myśl których chodziło nie tylko o zbieranie danych na temat cyberprzestępstw, przyjmowanie wspólnych standardów szkolenia i działania, lecz także o unikanie powielania działań, miały na celu stworzenie właściwej podstawy powołania centrum ds. cyberprzestępczości, zapowiadanego już od 2007 r.[43] Idea stworzenia w Unii Europejskiej jednego ośrodka, który w sposób kompleksowy zająłby się problematyką cyberprzestępczości, była wielokrotnie przywoływana we wszystkich wspomnianych dokumentach: od aktów wypracowywanych na poziomie eksperckim przez komunikaty Komisji po kluczowe programy i strategie w ramach przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Po niemalże pięcioletnich wysiłkach, po wcześniejszym przeprowadzeniu przez Komisję Europejską studium wykonalności oraz po osiągnięciu wstępnego

niałych przypadków, uwzględniające postęp techniczny i umożliwiające przygotowanie – w krótkiej lub średniej perspektywie – narzędzi operacyjnych.

[38] *Projekt konkluzji Rady na temat planu wdrażania zorganizowanej strategii walki z cyberprzestępczością*, dok. 5957/2/10 z 25 marca 2010 r.

[39] *Projekt konkluzji Rady na temat planu wdrażania*…, s. 1.

[40] Platforma (*European Cybercrime Platform* – ECCP) została utworzona zgodnie z postanowieniami *Komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Europejska agenda cyfrowa,* Bruksela, dnia 26.08.2010 r., KOM(2010) 245 wersja ostateczna/2.

[41] Europejski Urząd Policji (Europol) wraz z Komisją został poproszony o połączenie wszystkich właściwych krajowych platform w UE w jedną platformę ostrzegania o cyberprzestępczości. Europejska platforma ostrzegania funkcjonowałaby jako centrum, które zbierałoby i przechowywało informacje na temat przestępstw związanych z Internetem w celu dokonywania regularnych raportów statystycznych poświęconych cyberprzestępczości. W dalszych działaniach ECCP będzie znaczącym elementem mającego powstać do 2013 r. Centrum ds. Cyberprzestępczości.

[42] *Projekt konkluzji Rady na temat planu wdrażania*…, s. 6–7.

[43] W ramach ogólnych perspektyw zwalczania cyberprzestępczości wskazano na możliwość stworzenia, w ramach współpracy, centralnego unijnego punkt kontaktowego ds. cyberprzestępczości, *Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów. W kierunku ogólnej strategii zwalczania cyberprzestępczości*, Bruksela, dnia 22.05.2007 r., KOM(2007) 267 wersja ostateczna, s. 11.

kompromisu co do siedziby i zadań, społeczność unijna doczekała się oficjalnej informacji zawartej w Komunikacie Komisji Europejskiej[44] o sformalizowaniu prac nad utworzeniem Europejskiego Centrum ds. Walki z Cyberprzestępczością (*European Cybercrime Centre* – EC3). W dokumencie tym Komisja zaleca utworzenie takiego centrum, które będąc częścią struktur Europolu, będzie spełniać funkcję punktu koordynującego działania w zakresie walki z cyberprzestępczością w UE[45]. Nie tylko sprecyzowano w nim przedmiot[46] prac EC3, lecz także wskazano na jego zadania, do których należy:

- służenie jako europejski punkt kontaktowy w zakresie informacji dotyczących cyberprzestępczości,
- gromadzenie dostępnej w Europie wiedzy specjalistycznej na temat cyberprzestępczości potrzebnej do budowania potencjału państw członkowskich w zakresie walki z tym zjawiskiem,
- wspieranie krajowych dochodzeń dotyczących cyberprzestępstw,
- zapewnienie wspólnego głosu służbom ścigania i służbom sądowniczym zaangażowanym w europejskie dochodzenia w zakresie cyberprzestępczości[47].

Kierując się zasadą racjonalnego gospodarowania środkami w dobie światowego kryzysu finansowego, wskazano, że Centrum EC3 powinno zostać umieszczone w ramach struktur Europolu. Z perspektywy rachunku zysków i strat, powszechnie wiadomo, że tworzenie jakiegokolwiek nowego podmiotu, w krajowym czy miedzynarodowym systemie organizacyjnym, zawsze pociąga za sobą znaczne koszty.

Centrum ze względu na spodziewane korzyści[48] oraz potrzebę reagowania na rozwijające się zjawisko cyberprzestępczości powinno współdziałać z czterema grupami podmiotów. Poza państwami członkowskimi, sektorem prywatnym oraz parnterami międzynarodowymi[49] na uwagę zasługuje grupa podmiotów unijnych takich, jak: Europejskie Kolegium Policyjne – CEPOL, Europejska Jednostka Współpracy Sądowej – EUROJUST czy unijny CERT-EU, z którymi Centrum powinno intensywnie współpracować. Dość długa lista podmiotów, które od momentu utworzenia EC3 będą zaangażowane w problematykę walki z cyberprzestępczością, jest wyrazem aktywnej odpowiedzi UE na wzrost

---

[44] *Komunikat Komisji do Rady i Parlamentu Europejskiego, Zwalczanie przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością*, Bruksela, dnia 28.03.2012 r., KOM(2012) 140 wersja ostateczna.

[45] Tamże, s. 2.

[46] Główne formy cyberprzestępczości objęte zakresem działania prac Centrum:

– cyberprzestępstwa popełniane przez zorganizowane grupy przestępcze, szczególnie przestępstwa przynoszące duże zyski, takie jak oszustwa internetowe,
– cyberprzestępstwa wyrządzające poważne szkody ofiarom, np. przemoc seksualna wobec dzieci w internecie,
– cyberprzestępstwa (m.in. ataki cybernetyczne) w odniesieniu do infrastruktury kluczowej i najważniejszych systemów informacyjnych na terenie Unii.

Szerzej: *Komunikat Komisji do Rady i Parlamentu Europejskiego, Zwalczanie przestępczości w erze cyfrowej…*, s. 4.

[47] Tamże, s. 5–7.

[48] *Niesie to ze sobą różnorodne korzyści. Europol cieszy się uznaniem państw członkowskich i innych zainteresowanych stron, m.in. Interpolu i międzynarodowych organów ścigania. Posiada również uprawnienia w zakresie działań dotyczących przestępstw komputerowych* [...]. *Podstawowym zadaniem Europolu jest pomoc w osiągnięciu celu, jakim jest bezpieczniejsza Europa, z korzyścią dla wszystkich obywateli, i wspieranie organów ścigania UE dzięki wymianie i analizie danych wywiadu kryminalnego*, cyt. za: *Komunikat Komisji do Rady i Parlamentu Europejskiego, Zwalczanie przestępczości w erze cyfrowej…*, s. 7.

[49] Poza Interpolem wskazano na innych strategicznych partnerów na całym świecie, tamże, s. 8.

tego zjawiska. Wśród tych instytucji została także wskazana Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA), wzbudzająca najwiecej pytań i wątpliwości.

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji została utworzona w 2004 r.[50] w celu zapewnienia wysokiego poziomu bezpieczeństwa sieci i informacji na rzecz: obywateli, konsumentów, przedsiębiorstw oraz organizacji sektora publicznego Unii Europejskiej[51]. Mając to na uwadze, można postawić pytanie, czy prace Agencji nie będą w pewnym zakresie powielały działań podejmowanych przez Centrum, co więcej, czy ENISA nie jest odpowiednim miejscem do jego umiejscowienia i stworzenia szeroko pojętej kompleksowej ochrony: od bezpieczeństwa sieci i informacji w sensie technicznym po ochronę prawno-karną w cyberprzestrzeni.

W tym miejscu należy wyjaśnić kwestie formalne i jednocześnie przywołać wspomniany na początku artykułu traktatowy podział problematyki odnoszącej się do cyberprzestrzeni, mający decydujący wpływ na działania całej UE w tym zakresie. Zgodnie z artykułem ust. 3 art. 1 Rozporządzenia[52] cele i zadania Agencji dotyczą:

- prac z dziedziny bezpieczeństwa sieci i informacji, które nie należą do działań objętych, po zmianach wprowadzonych Traktatem z Lizbony, Tytułem V (*Przestrzeń wolności, bezpieczeństwa i sprawiedliwości*) i VI (*Transport*) TFUE,
- wszystkich działań związanych z bezpieczeństwem publicznym, obroną, bezpieczeństwem państwa, w tym dobrem państwa, w odniesieniu do zagadnień dotyczących bezpieczeństwa, a także działań państwa w obszarze prawa karnego[53].

Wprowadzony rozporządzeniem zakres działania Agencji pozwala zrozumieć istniejącą dwutorowość w podejściu do cyberbezpieczeństwa, która uniemożliwia przekazanie jej nowych zadań w postaci zwalczania cyberprzestępczości.

Z punktu widzenia zasadności wyboru Europolu na siedzibę EC3 należy zwrócić uwagę na okres działania ENISY, która początkowo została utworzona na pięć lat[54]. Od tego momentu dwukrotnie, w 2008 r.[55] i 2011 r.[56], przedłużano mandat tej Agencji odpowiednio: o kolejne cztery lata, a następnie o rok – obecnie jest on ważny do 13 września 2013 r., co z pewnością nie stanowi dobrej podstawy do zmiany zakresu jej funkcjonowania oraz rozszerzania jej struktury.

Biorąc więc pod uwagę dokonywane co jakiś czas rewizje prac i działań ENISY oraz jej znacznie szerszy zakres kompetencyjny, wybór Europolu jako siedziby nowego Centrum ds. Walki z Cyberprzestępczością wydaje się być zasadny.

Na koniec należy zwrócić uwagę na wymiar merytoryczny i praktyczny utworzenia oraz umiejscowienia Centrum EC3 w ramach Europolu, czyli na to, co Komisja w swoim komunikacie nazwała *wpływem ustanowienia Europejskiego Centrum*

---

[50] *Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji*, Dz.Urz. UE L 77 z 13.03.2004 r., s. 1.

[51] Tamże, art. 1, s. 38.

[52] Tamże.

[53] Tamże.

[54] Zgodnie z art. 27 rozporządzenia (WE) nr 460/2004 Agencja została utworzona na pięć lat, od 14 marca 2004 r.

[55] *Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1007/2008 z dnia 24 września 2008 r. zmieniające rozporządzenie (WE) nr 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji w zakresie okresu jej działania*, Dz.Urz. UE L 293 z 31.10.2008 r., s. 1–2.

[56] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 580/2011 z dnia 8 czerwca 2011 r. zmieniające rozporządzenie (WE) nr 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji w zakresie okresu jej działania*, Dz. Urz. UE L 165 z 24.06.2011 r., s. 3.

ds. Walki z Cyberprzestępczością na zasoby[57]. Biorąc pod uwagę uprawnienia Europolu w zakresie działań dotyczących przestępstw komputerowych[58], funckjonującą w jego ramach europejską platformę do walki z cyberprzestępczością (*European Cyber Crime Platform* – ECCP), Centrum ds. Przestępczości Zaawansowanej Technologicznie (*Hight Tech Crime Centre*)[59] oraz Europejską Grupę Zadaniową ds. Cyberprzestępczości (*European Cybercrime Task Force* – EUCTF)[60], szerokie zaangażowanie państw członkowskich, mające wpływ na posiadany zasób informacji, i jednocześnie możliwości analityczne Europolu, umiejscowienie Centrum w sprawnie funkcjonującym i dobrze znanym urzędzie wydaje się być uzasadnione. Z jednej strony rozwijanie kompetencji i możliwości zwalczania cyberprzestępczości, a z drugiej przesunięcie środków finansowych na rzecz Centrum, zostało wskazane jako kluczowe działanie nie tylko w *Ocenie zagrożenia wykorzystania Internetu przez zorganizowane grupy przestępcze* (tzw. iOCTA)[61], lecz także we wstępnym Programie Prac Europolu na 2013 r.[62]

Abstrakt

Pomimo pojawiających się sprzeciwów, nierzadko słusznych, niegodne z prawem działania w Internecie określono mianem cyberprzestępczości. Należy zauważyć, że zagrożenia w cyberprzestrzeni, z uwagi na daleko idące i dotkliwe konsekwencje, stały się jednym z priorytetowych tematów na arenach krajowej i międzynarodowej. Wyraźnym tego przejawem są pojawiające się programy walki z tym zjawiskiem, wspólne przedsięwzięcia sektora prywatnego i publicznego. Z uwagi na transgraniczny wymiar cyberprzestępczości czy ogólniej, działalności w Internecie, temat ten stał się również głównym zagadnieniem w polityce bezpieczeństwa wewnętrznego Unii Europejskiej, która podjęła działania w kierunku wypracowania mechanizmów przeciwdziałania i zwalczania przestępczości w cyberprzestrzeni.

W imię ochrony interesów państw członkowskich oraz samej Unii zostały podjęte działania legislacyjne i instytucjonale. Choć pierwszych inicjatyw z zakresu bezpieczeństwa w sieci na poziomie wspólnotowym można doszukiwać się już pod koniec lat 90., Unia weszła w fazę bardziej intensywnych prac z momentem przyjęcia kluczowego aktu, jakim jest Europejska Agenda Cyfrowa. Agenda stanowi odpowiedź i pierwszą na taką skalę reakcję Unii na widoczną zmianę punktu ciężkości w obszarach ludzkiej działalności – z form tradycyjnych na aktywność

---

[57] *Komunikat Komisji do Rady i Parlamentu Europejskiego, Zwalczanie przestępczości w erze cyfrowej…*, s. 7.

[58] Art. 4 ust. 1 (w związku z załącznikiem odnoszącym się do tego artykułu) *Decyzji Rady z dnia 6 kwietnia 2009 r. ustanawiająca Europejski Urząd Policji* (Europol) (2009/371/WSiSW, Dz.Urz. UE L 121 z 15.05.2009 r., s. 37.

[59] Centrum ds. Przestępczości Zaawansowanej Technologicznie w Europolu zapewnia państwom członkowskim wsparcie w ogólnym zwalczaniu cyberprzestępczości. W centrum tym powstaje europejska platforma służąca zaspokajaniu potrzeb państw członkowskich w tym ważnym i rozwijającym się obszarze działalności przestępczej. Szerzej: *Przegląd Europolu. Sprawozdanie ogólne z działalności Europolu*, Europejski Urząd Policji, 2011, s. 47.

[60] Utworzona przez szefów jednostek ds. cyberprzestępczości w UE, Komisję Europejską i Eurojust, powstała w Europolu w 2010 r. w celu stworzenia platformy dla osób zarządzających dochodzeniami i sprawami dotyczącymi cyberprzestępczości.

[61] *Threat Assessment (Abridged) Internet Facilitated Organised Crime – iOCTA*, Europol Public Information, Haga 7 stycznia 2011 r., File nr 2530–264, s. 3.

[62] *Europol Preliminary Work Programme*, Haga, 2 lutego 2012 r., File nr 1422–110r5.

w cyberprzestrzeni, co zostało zauważone zarówno w wymiarze gospodarczym (np. handel elektroniczny), jak i przestępczym (niezgodna z prawem działalność w sieci). Po trzech latach od jej przyjęcia, pomimo opóźnień terminowych i trudności finansowych, Agenda stała się punktem odniesienia do kolejnych działań Unii, które przejawiły się nie tylko w formie planów, projektów aktów pozalegislacyjnych czy komunikatów Komisji Europejskiej, ale również przyczyniły się do utworzenia nowego podmiotu na forum unijnym – Europejskiego Centrum ds. Cyberprzestępczości. Centrum, z uwagi na usytuowanie w Europolu oraz zakres zadań, stało się przedmiotem krytyki i fali wątpliwości.

Pamiętając jednak o traktatowych zdaniach Unii i ich zakresie oraz uwzględniając fakt, że Centrum rozpoczęło swoje funkcjonowanie z początkiem stycznia 2013 r., z oceną zasadności decyzji oraz prac unijnego ustawodawcy w zakresie cyberprzestępczości należy się jednak wstrzymać.

Abstract

Although some objections have been made, frequently justified ones, the unlawful acts committed online are called cybercrimes. Except for the technical imprecision, it must be noted that threats in the cyberspace, because of the far-reaching and severe consequences, have become a priority both in the national and international arena. A visible sign of that are new programmes designed to fight with this phenomenon, as well as joint initiatives launched jointly by the private and public sectors. Due to the trans-border dimension of cybercrime, or generally, of the activities in the Internet, it has become the main problem of the EU internal security policy. The European Union, often criticized for its ineffective and expensive actions, like other international organizations, has taken actions aiming to develop mechanisms of preventing and countering crime in the cyberspace.

In order to protect the interests of Member States and the EU, particularly at a time of crisis, legislative and institutional actions have been taken. Though the first initiatives regarding the Web were launched at the Community level in late 90s, the EU has intensified its work on this issue once the key act - the European Digital Agenda was adopted. In view of its scope, the Agenda is the EU's answer and its first wide range reaction to the shift of its focus in the area of human activity - from traditional behaviors to the activity in cyberspace, which has affected the economic (e.g. electronic commerce) and criminal areas (online illegal activity). Three years after its adoption, despite delays and financial difficulties, the Agenda has become a point of reference for any subsequent actions taken in the EU. They included plans, drafts of non-binding acts or the European Commission Communications. Moreover, those actions also contributed to the establishment of a new EU body, i.e. European Cyber Crime Centre. Due to its location in Europol's infrastructure as well as its scope of actions the Centre met with a lot of criticism and raised many doubts.

However, bearing in mind the EU treaty commitments and their scope and also the fact that the Centre was launched in January 2013, we should refrain from any premature judgment of the decisions and legitimacy as well as the EU law making as regards cybercrime.