Rada
Unii Europejskiej

Bruksela, 2 marca 2017 r.
(OR. en)

14585/2/16
REV 2 (pl)

GENVAL 120
CYBER 133

SPRAWOZDANIE

Dotyczy:	Sprawozdanie oceniające z siódmej rundy wzajemnych ocen poświęconej praktycznemu wdrożeniu i funkcjonowaniu europejskich polityk w dziedzinie zapobiegania cyberprzestępczości i jej zwalczania - Polska

ZAŁĄCZNIK

Spis treści

1 PODSUMOWANIE

Wizyta została bardzo dobrze przygotowana przez polskie władze; obejmowała spotkania z odpowiednimi podmiotami pełniącymi obowiązki z zakresu zapobiegania cyberprzestępczości i zwalczania jej, a także z zakresu wdrażania i realizacji polityk europejskich. Podmioty te to m.in. Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Cyfryzacji, Ministerstwo Sprawiedliwości, Komenda Główna Policji, Centralne Biuro Śledcze Policji, Biuro Bezpieczeństwa Narodowego, Rządowe Centrum Bezpieczeństwa, Prokuratura Generalna (obecnie Prokuratura Krajowa), Urząd Komunikacji Elektronicznej, Generalny Inspektor Ochrony Danych Osobowych, Naukowa i Akademicka Sieć Komputerowa (NASK), Agencja Bezpieczeństwa Wewnętrznego (cert.gov.pl), oraz organizacja pozarządowa Fundacja Dzieci Niczyje.

Podczas wizyty na miejscu polskie władze bardzo się starały, by przekazać zespołowi oceniającemu kompletne informacje oraz objaśnienia dotyczące prawnych i operacyjnych aspektów zapobiegania cyberprzestępczości i jej zwalczania, współpracy transgranicznej oraz współpracy z agencjami UE, a także na temat strategii cybernetycznej. Należy podkreślić uprzejmość i profesjonalizm polskich organów odpowiadających za organizację wizyty oceniającej, ich stałą dyspozycyjność podczas trwania wizyty i gotowość do udzielania dalszych informacji lub wyjaśnień.

Krajowa strategia bezpieczeństwa cybernetycznego Rzeczypospolitej Polskiej jest zdecentralizowana. Polska nie ma jednego dokumentu zawierającego krajową strategię bezpieczeństwa cybernetycznego, lecz zamiast tego trzy główne dokumenty dotyczące cyberbezpieczeństwa: *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej* i *Doktryna cyberbezpieczeństwa RP*. Dokumenty te obejmują dziedzinę cyberbezpieczeństwa, cyberobrony, świadomości cybernetycznej, kwestie szkoleniowe i reakcję na cyberataki. Wraz ze zdefiniowanymi priorytetami opracowanymi w Polsce, strategia ta stanowi solidną podstawę zwalczania cyberprzestępczości.

Rolę politycznego i strategicznego koordynatora ds. cyberbezpieczeństwa w Polsce pełni Ministerstwo Cyfryzacji. [1] Zatem głównym wyzwaniem w kategoriach cyberbezpieczeństwa jest stworzenie sprawnego systemu z wyraźnym podziałem kompetencji między instytucjami zajmującymi się cyberbezpieczeństwem i cyberprzestępczością, oraz zacieśnienie współpracy z przedsiębiorstwami działającymi w dziedzinie cyberbezpieczeństwa.

Jeżeli chodzi o ustawodawstwo, Polska podpisała i ratyfikowała Konwencję o cyberprzestępczości, a także wdrożyła do ustawodawstwa krajowego dyrektywy europejskie dotyczące cyberprzestępczości. Tak jak w wielu krajach, tak i w polskim ustawodawstwie brak jest konkretnej definicji cyberprzestępczości. Na szczeblu praktycznym cyberprzestępczość obejmuje wszelkie przestępstwa na systemach komputerowych i danych komputerowych, jak również przestępstwa umożliwiane poprzez wykorzystywanie komputerowego systemu informacyjnego. Stwierdzono jednak, że brak jednej definicji cyberprzestępczości w ustawodawstwie może utrudniać zmierzenie skali wszystkich incydentów mieszczących się w kategorii cyberprzestępczości.

System odpowiadający za zwalczanie cyberprzestępczości wydaje się być odpowiednio wyposażony i skalibrowany. Zdaniem oceniających Polska stworzyła solidną strukturę służącą zwalczaniu cyberprzestępczości i zapewnieniu bezpieczeństwa cybernetycznego.

[1] W świetle przepisów ustawy o podziale zadań i kompetencji organów administracji rządowej w Polsce.

Wizyta złożona w siedzibie Komendy Głównej Policji i przedstawione przez Policję przykłady wykazały doskonałe umiejętności organizacyjne i zdolności do zwalczania cyberprzestępczości, a także strukturę zgodną z najwyższymi normami w zakresie wiedzy i know-how. Na szczeblu centralnym, w Biurze Kryminalnym utworzono Wydział do walki z Cyberprzestępczością odpowiedzialny za wszczynanie i koordynowanie działań policji w zakresie cyberprzestępczości[2]. Wydział ten wspiera też prace prowadzone na szczeblu regionów, na którym działa 18 jednostek (tj. w każdym województwie i w Komendzie Stołecznej Policji w Warszawie oraz w Centralnym Biurze Śledczym Policji). Jednostki te są stale wyposażane w sprzęt, a funkcjonariusze Policji przechodzą szkolenia podwyższające ich kwalifikacje. Chociaż wydział ten nie zajmuje się faktycznie każdym przypadkiem, to wsparcie udzielane różnym komendom wojewódzkim przy technicznych działaniach śledczo-dochodzeniowych oraz pomoc z zakresu forensyki sprawiają, że istniejący system zwalczania cyberprzestępczości jest skuteczny. Ponadto komendy wojewódzkie współpracują z wyspecjalizowanymi organami ścigania takimi jak Centralne Biuro Śledcze Policji i Agencja Bezpieczeństwa Wewnętrznego.

Ogólnie Policja i prokuratura zajmują się wszelkimi przypadkami przestępczości, w tym cyberprzestępczością. Postępowania przygotowawcze prowadzą funkcjonariusze Policji z wydziału śledczego. Jednak w prokuraturze nie ma wydzielonej struktury, stanowiącej odpowiednik wspomnianego wydziału Policji, do zwalczania cyberprzestępczości w ramach prac operacyjnych. Ponadto, biorąc pod uwagę niezmiernie ważną rolę, jaką odgrywają sędziowie i prokuratorzy, stwierdzono z ich strony pewien brak proaktywnej postawy przy ustalaniu własnych priorytetów w celu podwyższania kompetencji zawodowych i podnoszenia skuteczności w zwalczaniu cyberprzestępczości.

[2] Po wizycie na miejscu zespół oceniający poinformowano, że 1 grudnia 2016 r. utworzono Biuro do walki z Cyberprzestępczością. Biuro ma cztery wydziały: ogólny, rozpoznania, operacyjny oraz wsparcia i badań. W najbliższej przyszłości funkcje objąć ma tam pięćdziesięciu dwóch policjantów i czterech pracowników cywilnych.

Pomimo tego, że system ochrony cyberprzestrzeni w Polsce jest zdecentralizowany, to działa właściwie. O takim zdecentralizowanym podejściu świadczy także istnienie kilku zespołów reagowania na incydenty komputerowe oraz Rządowego Zespołu Reagowania na Incydenty Komputerowe (CERT.GOV.PL).

CERT.GOV.PL działa w strukturach Agencji Bezpieczeństwa Wewnętrznego i odpowiada za podwyższanie zdolności służb publicznych do ochrony ich własnych systemów informatycznych. Stanowi on także drugi poziom krajowego systemu reagowania na incydenty komputerowe w cyberprzestrzeni i jako taki, jest ostatnią instancją dla innych zespołów reagowania lub podmiotów mających do czynienia z poważnym incydentem komputerowym. W przypadku wystąpienia incydentów o szerokim zakresie oddziaływania CERT.GOV.PL ma koordynować reakcję na atak.

Z drugiej strony CERT POLSKA odgrywa rolę faktycznego krajowego zespołu reagowania. Został on utworzony w ramach struktur polskiej Naukowej i Akademickiej Sieci Komputerowej (NASK). Jest autonomiczny wobec administracji publicznej i stanowi dobry przykład współpracy publiczno-prywatnej. Jego zadania obejmują reagowanie na zagrożenia i incydenty w domenie .pl; świadczy on usługi dla banków i innych stron trzecich poza administracją publiczną, a także prowadzi badania z zakresu bezpieczeństwa, tworząc narzędzia i systemy informatyczne służące ochronie polskiej cyberprzestrzeni. W Polsce działa kilka innych zespołów reagowania (np. MIL-CERT, PIONIERCERT itp.). Dlatego też oficjalne powołanie krajowego zespołu reagowania mogłoby ułatwić koordynację ich działań.

Pomimo tego rozproszonego charakteru NASK i Agencja Bezpieczeństwa Wewnętrznego opracowują bardzo dobre sprawozdania z sytuacji w zakresie bezpieczeństwa w cyberprzestrzeni w kraju. Opisują poziom krajowych systemów bezpieczeństwa, w tym krytyczną infrastrukturę informatyczną oraz działanie służb i instytucji odpowiadających za bezpieczeństwo w Polsce.

Należy stwierdzić istnienie ścisłej współpracy z sektorem prywatnym, zwłaszcza przy zwalczaniu niegodziwego traktowania dzieci, oraz z sektorem bankowym – w tym wypadku ma ona charakter strategiczny i fundamentalny. Współpraca między polską Policją a Związkiem Banków Polskich stanowi przykład bardzo dobrej współpracy między organami ścigania a sektorem prywatnym. Kolejnym doskonałym przykładem tego rodzaju współpracy jest działanie opracowane przez Fundację Dzieci Niczyje – organizację pozarządową pracującą z maltretowanymi dziećmi i ich rodzinami, by nie dopuszczać do ponownej wiktymizacji. Specjalne pokoje umożliwiają przesłuchiwanie ofiar przy fizycznej obecności sędziego, śledczego i prokuratora, a jednocześnie umożliwiają obronie przysłuchiwanie się rozmowie. Oznacza to, że ofiara nie musi być obecna w sądzie w trakcie procesu.

Ochrona polskich obywateli i firm w cyberprzestrzeni jest wzmacniana przez liczne inicjatywy na rzecz zwiększania wiedzy i prewencji prowadzone przez wiele podmiotów, takich jak Ministerstwo Cyfryzacji, Policja, organizacje pozarządowe, ośrodki akademickie itp. Wydaje się jednak, że brak jest ogólnej wizji konkretnych działań i grup, do których są one skierowane. Polska nie posiada również budżetu przeznaczonego specjalnie na kampanie informacyjne i prewencyjne.

Wyższa Szkoła Policji i Krajowa Szkoła Sądownictwa i Prokuratury zademonstrowały bardzo duże możliwości w zakresie szkolenia przedstawicieli zawodu prawniczego i sił Policji. Wiele wydarzeń – organizowanych wewnętrznie lub wraz z partnerami zewnętrznymi – ma na celu zwiększenie wiedzy osób zajmujących się zwalczaniem cyberprzestępczości. Szczególnie ważne są wspólne sesje szkoleniowe organizowane dla sędziów, prokuratorów i funkcjonariuszy Policji, a mające na celu wymianę wiedzy i doświadczeń. Wydaje się jednak, że szkolenia te nie docierają do wszystkich prokuratorów i sędziów, którzy ich potrzebują. Pomimo dobrej jakości prac prowadzonych w tej dziedzinie przez Krajową Szkołę Sądownictwa i Prokuratury, szkolenia te nie są obowiązkowe.

Także istotna jest współpraca międzynarodowa, w tym z członkami Partnerstwa Wschodniego, szkolenia dla organów ścigania oraz uczestnictwo w projekcie Europolu pod nazwą EMPACT (i w wielu innych inicjatywach). Polska współpracuje z kilkoma agencjami UE (Europolem/EC3 – jest zaangażowana w trzy punkty kontaktowe (Focal Points): Terminal, Cyborg i Twins, a także z Eurojustem i ENISA), organami ścigania różnych państw (NCA, FBI, BKA) oraz z sektorem prywatnym (w dziedzinie oszustw z wykorzystaniem kart płatniczych Policja współpracuje ze Związkiem Banków Polskich na podstawie podpisanej umowy, oraz prowadzi przedsięwzięcia naukowe we współpracy z uniwersytetami).

Biorąc pod uwagę wszystkie czynniki, zespół oceniający docenił sposób, w jaki system ten działa w Polsce. Realizowana strategia jest wyraźnie opracowana tak, by przygotować kraj na przeciwdziałanie ewentualnym cyberatakom. Biorąc pod uwagę czynione przez polskie organy istotne starania, by zabezpieczyć infrastrukturę krytyczną, organy rządowe i obywateli, opinia oceniających jest jednoznacznie pozytywna.

2 WPROWADZENIE

Po przyjęciu wspólnego działania 97/827/WSiSW z dnia 5 grudnia 1997 r.[3] stworzono mechanizm oceny stosowania i realizacji na szczeblu krajowym międzynarodowych zobowiązań w walce z przestępczością zorganizowaną. Na podstawie art. 2 tego wspólnego działania Grupa Robocza do Spraw Ogólnych, w tym Oceny (GENVAL) postanowiła na posiedzeniu w dniu 3 października 2013 r., że siódma runda wzajemnych ocen będzie poświęcona praktycznemu wdrożeniu i funkcjonowaniu europejskich polityk w dziedzinie zapobiegania cyberprzestępczości i jej zwalczania.

Wybór cyberprzestępczości jako tematu siódmej rundy wzajemnych ocen został pozytywnie przyjęty przez państwa członkowskie. Ponieważ jednak pojęcie „cyberprzestępczość" obejmuje szerokie spektrum przestępstw, uzgodniono, że ocena skupi się na tych, które zdaniem państw członkowskich zasługują na szczególną uwagę. Dlatego też oceny obejmują trzy konkretne obszary: ataki cybernetyczne, niegodziwe traktowanie dzieci w celach seksualnych/pornografia dziecięca w internecie oraz przestępstwa w internecie z wykorzystaniem karty płatniczej. Powinny one zapewnić kompleksowe badanie aspektów prawnych i operacyjnych zwalczania cyberprzestępczości, ocenę współpracy transgranicznej i współpracy z właściwymi agencjami UE. Dyrektywa 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej[4] (data transpozycji: 18 grudnia 2013 r.) i dyrektywa 2013/40/UE[5] dotycząca ataków na systemy informatyczne (data transpozycji: 4 września 2015 r.) mają w tym zakresie szczególne znaczenie.

Ponadto w swoich konkluzjach na temat strategii bezpieczeństwa cybernetycznego UE[6] z czerwca 2013 r. Rada powtarza, że celem jest jak najszybsza ratyfikacja Konwencji Rady Europy o cyberprzestępczości (konwencji budapeszteńskiej)[7] z dnia 23 listopada 2001 r., a w preambule konkluzji podkreśla, że „UE nie wzywa do tworzenia nowych międzynarodowych instrumentów prawnych poświęconych kwestiom cybernetycznym". Wspomnianą konwencję uzupełnia Protokół dotyczący penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnianych przy użyciu systemów komputerowych[8].

---

3 Wspólne działanie z dnia 5 grudnia 1997 r. (97/827/WSiSW), Dz.U. L 344 z 15.12.1997, s. 7–9.
4 Dz.U. L 335 z 17.12.2011, s. 1.
5 Dz.U. L 218 z 14.8.2013, s. 8.
6 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.
7 CETS nr 185; udostępniona do podpisu w dniu 23 listopada 2001 r., weszła w życie w dniu 1 lipca 2004 r.
8 CETS nr 189; udostępniona do podpisu w dniu 28 stycznia 2003 r., weszła w życie w dniu 1 marca 2006 r.

Doświadczenie z poprzednich ocen wykazało, że państwa członkowskie mają różne stanowiska odnoszące się do wdrażania odnośnych aktów prawnych, a bieżący proces oceny może także dostarczyć przydatnych informacji tym państwom członkowskim, które mogły jeszcze nie wdrożyć wszystkich aspektów różnych aktów prawnych. Niemniej jednak ocena powinna mieć szeroki zakres i interdyscyplinarny charakter. Nie będzie ona skupiać się wyłącznie na wdrożeniu różnych aktów prawnych dotyczących zwalczania cyberprzestępczości, lecz raczej na aspektach operacyjnych w poszczególnych państwach członkowskich.

Zatem oprócz współpracy z prokuraturą, ocena będzie uwzględniać także sposób, w jaki organy policyjne współpracują z Eurojustem, ENISA i Europolem/EC3 oraz sposób, w jaki informacje zwrotne od uczestników tej współpracy są przekazywane odpowiednim służbom policyjnym i socjalnym. Ocena skupia się na kwestii wdrażania polityk krajowych służących zwalczaniu cyberataków, oszustw, i pornografii dziecięcej. Ocena obejmuje także praktyki operacyjne stosowane w państwach członkowskich w stosunku do współpracy międzynarodowej oraz wsparcie udzielane osobom, które padły ofiarą cyberprzestępczości.

Porządek wizyt w państwach członkowskich grupa robocza GENVAL przyjęła w dniu 1 kwietnia 2014 r. Polska była siedemnastym państwem członkowskim, które poddano ocenie w trakcie bieżącej rundy. Zgodnie z art. 3 wspólnego działania, prezydencja sporządziła wykaz ekspertów biorących udział w przeprowadzaniu ocen. Na podstawie pisemnego wniosku wystosowanego w dniu 28 stycznia 2014 r. do delegacji przez przewodniczącego grupy roboczej GENVAL państwa członkowskie wytypowały ekspertów posiadających dużą wiedzę praktyczną w przedmiotowej dziedzinie.

Zespoły oceniające składają się z trzech ekspertów krajowych, wspieranych przez dwóch członków personelu Sekretariatu Generalnego Rady oraz obserwatorów. Grupa robocza GENVAL zgodziła się z propozycją prezydencji, by jako obserwatorów na siódmą rundę ocen wzajemnych zaprosić Komisję Europejską, Eurojust, ENISA i Europol/EC3.

Eksperci, którym powierzono przeprowadzenie oceny w Polsce, to Giorgos Karkas (Cypr), Gianluigi Umeteli (Włochy) i Henrik Olin (Szwecja). Obecnych było także dwóch obserwatorów: José Eduardo Guerra (Eurojust) i Małgorzata Sobusiak-Fischnalle (Europol), a także Steven Cras i Sławomir Buczma z Sekretariatu Generalnego Rady.

Niniejsze sprawozdanie sporządził zespół ekspertów wspomagany przez Sekretariat Generalny Rady, na podstawie ustaleń wynikających z wizyty oceniającej, która odbyła się w Polsce w dniach 1–5 lutego 2016 r., oraz na podstawie szczegółowych odpowiedzi udzielonych przez Polskę na pytania zawarte w kwestionariuszu oceny, a także szczegółowych odpowiedzi udzielonych na dalsze pytania.

3 SPRAWY OGÓLNE I STRUKTURY

3.1 Krajowa strategia bezpieczeństwa cybernetycznego

Istniejący w Polsce system ochrony cyberprzestrzeni jest zdecentralizowany. Kompetencje dotyczące bezpieczeństwa cyberprzestrzeni są podzielone między instytucje wykonujące zadania z zakresu odporności cybernetycznej, zapobiegania cyberprzestępczości oraz cyberobrony. Trzy główne dokumenty dotyczące cyberbezpieczeństwa w Polsce to:

- *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*

W dniu 25 czerwca 2013 r. Rada Ministrów *przyjęła Politykę ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*(*polityka*)[9]. Jeżeli chodzi o odporność cybernetyczną, *polityka* odsyła do *Strategii Sprawne Państwo*[10]*,* strategii rozwojowej dla instytucji publicznych i instytucji egzekwowania prawa. Celem strategicznym *polityki* jest uzyskanie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni w Polsce. Z racji zakresu tego dokumentu – który ogranicza się do administracji rządowej – minister zajmujący się społeczeństwem informacyjnym odpowiada za wdrażanie tej polityki w imieniu Rady Ministrów.

- - *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*

Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej (*strategia*) została przyjęta w 2014 r. Jest to dokument o charakterze strategicznym, odnoszący się do obszaru cyberobrony. Strategicznym celem cyberbezpieczeństwa przedstawionym w tej *strategii* jest zapewnienie Polsce bezpieczeństwa w cyberprzestrzeni, co obejmuje zapewnianie odpowiedniego stanu krajowych systemów bezpieczeństwa, zwłaszcza państwowej infrastruktury krytycznej ICT oraz infrastruktury niezbędnej do funkcjonowania społeczeństwa oraz prywatnych podmiotów gospodarczych, w tym w sektorach finansowym, energetycznym i opieki zdrowotnej.

---

[9] Wyżej wymieniona polityka jest dostępna w wersji polskiej i angielskiej na stronie: http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html.

[10] http://administracja.mac.gov.pl/adm/departament-administra/strategia-sprawne-panst/8085,Strategia-Sprawne-Panstwo-2020.html

- *Doktryna cyberbezpieczeństwa RP*

Biuro Bezpieczeństwa Narodowego (BBN) – które jest organem świadczącym pomoc i wsparcie dla Prezydenta Rzeczypospolitej Polskiej przy wykonywaniu przez niego zadań z zakresu bezpieczeństwa i obrony – opublikowało w dniu 22 stycznia 2015 r. dokument pt. *Doktryna cyberbezpieczeństwa RP*[11]. Dokument ten zawiera oficjalne poglądy i ustalenia dotyczące celów, ocen środowiskowych oraz koncepcji operacyjnej, służące zapewnieniu bezpiecznego funkcjonowania państwa jako całości, jego struktur, poszczególnych osób i podmiotów prawnych – w tym podmiotów gospodarczych i innych podmiotów niemających osobowości prawnej – w cyberprzestrzeni.

Władze polskie zamierzają stworzyć nowy system z wyraźnym podziałem zadań między instytucjami zajmującymi się cyberbezpieczeństwem i cyberprzestępczością, oraz zacieśnić współpracę z przedsiębiorstwami działającymi w dziedzinie cyberbezpieczeństwa. W kwietniu 2015 roku przyjęto *Plan działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni*. Jednym z zadań ujętych w tym planie jest opracowanie projektu wytycznych dotyczących krajowej ustawy tworzącej system cyberbezpieczeństwa w Polsce. Ministerstwo Cyfryzacji ma odgrywać wiodącą rolę w tym przedsięwzięciu. W wytycznych tych zostanie wskazana optymalna koncepcja, która zostanie wykorzystana jako podstawa do opracowania krajowego systemu cyberbezpieczeństwa, przedstawiająca również uprawnienia i zadania przydzielane poszczególnym instytucjom. Ministerstwo Cyfryzacji zamówiło także ekspertyzę pt. *System bezpieczeństwa cyberprzestrzeni RP*, które przygotowali eksperci z NASK. W ekspertyzie określa się pewną liczbę zaleceń dotyczących utworzenia instytucji koordynującej, która zapewni właściwe funkcjonowanie systemu na szczeblu strategicznym i legislacyjnym, a także koordynację działań operacyjnych.

[11] https://www.bbn.gov.pl/pl/wydarzenia/6336,Doktryna-cyberbezpieczenstwa-RP.html

Ekspertyza ta zawiera także zalecenia dotyczące zwalczania cyberprzestępczości, z których jednym jest opracowanie wieloletniego *Narodowego programu walki z cyberprzestępczością*; będzie on podobny do niedawno przyjętego narodowego programu antyterrorystycznego. W zaleceniach wskazuje się na potrzebę zapewnienia, by krajowy Zespół Reagowania na Incydenty związane z Bezpieczeństwem Komputerowym (CSIRT) miał możliwość zgłaszania przypadków cyberprzestępczości Policji. Poza tym krajowy CSIRT powinien być wykorzystywany do rozwijania kompetencji (umiejętności) organów ścigania – nie tylko policji, lecz także prokuratur i innych organów sądowych[12].

3.2 Krajowe priorytety dotyczące cyberprzestępczości

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej jest krajowym dokumentem strategicznym z dziedziny cyberbezpieczeństwa. Polityka ta uwzględnia głównie aspekty odpornościowe ochrony cyberprzestrzeni i pośrednio związana jest z kwestią cyberprzestępczości przez działania edukacyjne i z zakresu podnoszenia świadomości. Priorytetami polityki są działania z dziedziny oceny ryzyka; bezpieczeństwo portali rządowych; działania z dziedziny ustawodawstwa; działania proceduralne i organizacyjne realizowane poprzez wdrażanie optymalnych rozwiązań i standardów z tej dziedziny; działania z dziedziny edukacji, szkolenia i zwiększania świadomości w zakresie bezpieczeństwa; oraz działania dotyczące rozwiązań technicznych służących zmniejszaniu w Polsce ryzyka związanego z zagrożeniami w cyberprzestrzeni.

[12] Po wizycie na miejscu zespół oceniający poinformowano, że w lutym 2016 r. Ministerstwo Cyfryzacji przedstawiło projekt nowej strategii bezpieczeństwa cybernetycznego. Projekt strategii aktualnie jest przedmiotem ogólnokrajowych konsultacji. Biorąc pod uwagę niedawne przyjęcie dyrektywy w sprawie bezpieczeństwa sieci i systemów informacyjnych, Ministerstwo Cyfryzacji prowadzi obecnie prace nad kompleksowymi przepisami dotyczącymi krajowego systemu cyberbezpieczeństwa. Przepisy te mają między innymi utworzyć system przewidujący przejrzysty podział kompetencji między poszczególnymi zainteresowanymi instytucjami.

Priorytety związane z kwestią cyberprzestępczości zostały ujęte także w następujących rządowych programach strategicznych przyjętych przez Radę Ministrów:

- Narodowy program antyterrorystyczny na lata 2015–2019. Jednym z priorytetów tego programu jest analizowanie możliwości współpracy między administracją publiczną a sektorem prywatnym przy zapobieganiu publikacji i rozpowszechnianiu treści o charakterze terrorystycznym i ekstremistycznym w mediach oraz przy wdrażaniu wszelkich dodatkowych środków w tym względzie. Zadanie to dotyczy także wiadomości przesyłanych w internecie.
- *Program zapobiegania i zwalczania przestępczości gospodarczej na lata 2015–2020* Obejmuje on prace nad opracowaniem taktyki i standardów kontrolowania niektórych aspektów przestępstw gospodarczych, w tym przestępstw związanych z rozwojem nowych technologii (cyberprzestępczość).

Polska opracowała także kolejne programy dotyczące zapobiegania przestępstwom w cyberprzestrzeni:

- Program „Bezpieczeństwo +" opracowany przez Ministerstwo Edukacji Narodowej na lata 2015–2018;
- Krajowy program pt. „Bezpieczna i przyjazna szkoła" na lata 2014–2020.

Programy te obejmują wiele założeń i zadań i mają na celu stabilizowanie tendencji oraz zmniejszanie zasięgu i intensywności problemów i trudnych zachowań wśród dzieci i młodzieży. Powinno to pomóc w obniżeniu poziomu agresji i przemocy, oraz przemocy w sieci, a także poprawić umiejętności uczniów z zakresu odpowiedniego postępowania w cyberprzestrzeni, zwłaszcza w sferze nowych mediów.

Priorytety Policji w zakresie zapobiegania i zwalczania cyberprzestępczości

Dokument pt. *Koncepcja działań policji w zakresie profilaktyki społecznej na lata 2015–2018* określa priorytety twórczego i obejmującego wiele instytucji podejścia do profilaktyki społecznej, które to priorytety rekomendowano na szczeblu krajowym. Z perspektywy roli Policji w profilaktyce społecznej dotyczącej przestępczości najważniejsze obszary to: podnoszenie poziomu ochrony obywateli Polski i polskich przedsiębiorstw w cyberprzestrzeni oraz zapobieganie szeroko rozumianej przemocy, w tym przemocy rówieśniczej i cyberprzemocy.

Ponadto Komendant Główny Policji wydał *Priorytety Komendanta Głównego Policji* na lata 2016–2018, w których najwyższą rangę nadano m.in. zwalczaniu przestępstw popełnianych w cyberprzestrzeni[13]. Aby uczynić działania Policji w określaniu i zwalczaniu największych bieżących zagrożeń, w tym cyberprzestępczości, bardziej skutecznymi, określono następujące zadania:

a) Komendy wojewódzkie policji i Komenda Stołeczna Policji w Warszawie wzmogą działania operacyjne zwalczające cyberprzestępczość;
b) Komenda Główna Policji stworzy krajowy system wymiany i koordynacji informacji, by wspomagać walkę z cyberprzestępczością. W tym celu planuje się usprawnienia technologiczne w wydziałach wyznaczonych do zwalczania cyberprzestępczości (np. przez utworzenie wyspecjalizowanych laboratoriów do analizy sprzętu IT i oprogramowania). Istnieją także plany poprawienia jakości i skuteczności pracy Policji przez stopniowe podwyższanie kompetencji zawodowych funkcjonariuszy i pracowników policji, m.in. za pomocą specjalistycznych szkoleń na temat zwalczania cyberprzestępczości.

Realizacja tych priorytetów będzie obejmować:

a) wprowadzenie systemu pozyskiwania i analizowania danych z otwartych źródeł w sieci;
b) utworzenie systemu/platformy sprzętowej służącej badaniom złośliwego oprogramowania takiego jak malware;
c) dostarczanie pionom zajmującym się zwalczaniem cyberprzestępczości sprzętu i oprogramowania, którego potrzebują do zbierania i zabezpieczania dowodów cyfrowych;
d) realizację specjalistycznych szkoleń dla funkcjonariuszy z Wydziału do walki z Cyberprzestępczością, prowadzonych w Wyższej Szkole Policji w Szczytnie.

[13] Dostępne w języku polskim: http://isp.policja.pl/isp/aktualnosci/7813,7-priorytetow-Komendanta-Glownego-Policji.html.

Udział polskiej policji w EMPACT

Priorytet w ramach EMPACT (europejskiej multidyscyplinarnej platformie przeciwko zagrożeniom przestępstwami) dotyczący oszustw z wykorzystaniem kart płatniczych jest wspierany przez koordynatora w Wydziale do walki z Przestępczością Gospodarczą (Biuro Kryminalne Komendy Głównej Policji). Działania w ramach EMPACT dotyczące oszustw z wykorzystaniem kart płatniczych stanowią priorytet; są to:

– badania dotyczące oszustw z wykorzystaniem kart płatniczych, z wykorzystaniem danych karty płatniczej bez jej rzeczywistego posiadania, „automatycznych koszyków sprzedażowych" (Automated Vending Carts), „słupów" oraz dotyczące odzyskiwania mienia,
– rozszerzanie operacji „Dni wspólnych działań", spotkania operacyjne i wizyty robocze bezpośrednio związane z prowadzeniem dochodzeń

Polska przewodzi projektowi, który polega na świadczeniu pomocy państwom należącym do programu Partnerstwa Wschodniego w rozwijaniu zdolności przeciwdziałania cyberprzestępczości/oszustwom z wykorzystaniem kart płatniczych. Projekt ten obejmuje szkolenie dla organów ścigania z państw Partnerstwa Wschodniego i działania przeznaczone dla tych państw w ramach tego projektu mające na celu rozwijanie zdolności i narzędzi do zapobiegania przestępczości z wykorzystaniem kart płatniczych i badanie tego zjawiska. Ponadto w ramach zwalczania oszustw z wykorzystaniem kart płatniczych ujętego w EMPACT Wydział do walki z Przestępczością Gospodarczą uczestniczy w przedsięwzięciu „Dzień Przeciwdziałania Oszustwom przy Zakupie Biletów Lotniczych" w ramach „Dni wspólnych działań".

Platforma EMPACT dotycząca cyberataków jest przeznaczona do poprawiania współpracy między państwami członkowskimi UE, właściwymi instytucjami oraz agencjami i partnerami z sektora prywatnego przy produkcji i rozpowszechnianiu oprogramowania zwalczającego oprogramowanie złośliwe oraz przy obronie przeciw sieciowym atakom na infrastrukturę. Wydział do walki z Cyberprzestępczością (Biuro Kryminalne Komendy Głównej Policji) wspiera priorytet poświęcony określaniu powiązań i udzielaniu wsparcia między państwami członkowskimi w odniesieniu do wykorzystywania bazy danych EMAS (systemu analizy złośliwego oprogramowania stworzonego przez Europol); odbywa się to poprzez przekazywanie, w miarę możliwości, próbek złośliwego oprogramowania do analizy.

Szef Wydziału do walki z Cyberprzestępczością jest także krajowym punktem kontaktowym Europejskiej Sieci Służb Technologii Bezpieczeństwa Wewnętrznego (ENLETS) w zakresie wsparcia technologicznego i wymiany informacji na temat nowych technologii i rozwiązań, badań, rozwoju oraz przedsięwzięć prowadzonych przez Radę Europy.

W dziedzinie zwalczania wykorzystywania seksualnego dzieci w sferze cyberprzestępczości Policja bierze udział w działaniach tego dotyczących w ramach EMPACT, które koncentrują się na przypadkach wykorzystywania seksualnego dzieci oraz na materiałach związanych z niegodziwym traktowaniem dzieci. W konkretnych przypadkach polska Policja wykorzystuje także System Informacyjny Europolu. Ogólnie nie ma szczególnych żądań ani procedur dotyczących współpracy z Europolem w tej dziedzinie: Ponadto od września 2014 roku Policja wdrożyła politykę bezpieczeństwa Europolu przez udział w działaniach w ramach EMPACT dotyczących zwalczania wykorzystywania seksualnego dzieci. Działanie to skupia się na wykrywaniu i zwalczaniu zorganizowanych grup przestępczych odpowiadających za umieszczanie w internecie materiałów związanych z niegodziwym traktowaniem dzieci oraz na wykrywaniu powiązań między tymi grupami.

3.3 Statystyki dotyczące cyberprzestępczości

3.3.1 Główne tendencje prowadzące do występowania cyberprzestępczości

Od roku 2003 ogólna liczba przestępstw popełnianych w Polsce nie przestaje spadać. Wskaźnik przestępczości w Polsce jest obecnie niższy od europejskiej średniej. Jednak polskie władze donoszą, że tendencja ta nie dotyczy cyberprzestępczości. W ostatnich latach istotnie wzrosła liczba wykorzystywanych urządzeń elektronicznych, jak również liczba użytkowników różnych usług elektronicznych (głównie umiejscowionych w internecie). Spowodowało to powstanie nowych form i sposobów popełniania przestępstw. Przestępcy w swoich działaniach wykorzystują nadal niedostateczną wiedzę o zagrożeniach płynących z sieci.

Według danych statystycznych CERT POLSKA w roku 2014 doszło do 1 282 incydentów cybernetycznych. Najczęściej spotykane problemy to:

- kradzież tożsamości i wyłudzanie informacji (phishing) – 383 zgłoszenia;
- obraźliwe treści – 370 zgłoszeń;
- złośliwe oprogramowanie (malware) – 98 zgłoszeń;
- zbieranie informacji (skanowanie, podsłuch komputerowy) – 98 zgłoszeń;
- włamania elektroniczne i próby takich włamań – 49 zgłoszeń.

Głównym celem sprawców jest uzyskanie informacji o użytkownikach (w większości przypadków nazw użytkowników i haseł, by uzyskać dostęp do różnych usług w internecie). Najpopularniejszą metodą infekowania użytkowników polskich sieci jest przesyłanie wiadomości elektronicznych zawierających załączniki ze złośliwym oprogramowaniem. Tradycyjny phishing kierowany jest na wiele różnych stron w sieci. Poza bardziej typowymi celami, takimi jak banki i usługi finansowe, popularne cele to m.in. strony z grami on-line, profile na serwisach społecznościowych, konta poczty elektronicznej i konta w sklepach elektronicznych.

Według *Raportu o stanie bezpieczeństwa w Polsce za rok 2014*, który stanowi podsumowanie działania służb i instytucji odpowiadających za stan bezpieczeństwa w Polsce, cyberprzestępczość pozostaje obszarem działania zarówno indywidualnych przestępców, jak i zorganizowanych grup przestępczych, społeczności ekstremistycznych i organizacji terrorystycznych. Według władz polskich najpoważniejsze zagrożenia w cyberprzestrzeni, którymi należy się zająć w niedalekiej przyszłości, to m.in.:

- rosnąca liczba przestępstw komputerowych popełnianych przeciw ochronie informacji, przeciw własności i bezpieczeństwu publicznemu związanych z gwałtownym rozwojem informatyki, oraz z szerokim jej wykorzystywaniem w prawie każdej sferze życia;
- spodziewana kontynuacja działalności szpiegowskiej w sieci skierowanej przeciw kluczowym instytucjom i przedsiębiorstwom w sferze infrastruktury krytycznej;
- postępujące w ostatnich latach podwyższanie na światowym rynku telekomunikacji – w tym na rynku polskim – pozycji producentów sprzętu, w stosunku do którego istnieje racjonalne podejrzenie, że jest stosowany do celów wywiadowczych.

Ponadto, analizując szczególny charakter cyberprzestępczości, można założyć, że wspomniane zagrożenia będą też dotyczyć kradzieży tożsamości, naruszeń bezpieczeństwa ICT, wykorzystywania złośliwego oprogramowania do celów przestępczych, nabywania kart bankomatowych oraz kryptowaluty (pranie pieniędzy). Ponadto przestępcy w sieci częściej kierują swoje działania na sektor finansowy, zwłaszcza banki i ich klientów, na elektroniczne płatności i sklepy elektroniczne. Przestępcy stają się wyraźnie bardziej profesjonalni, a zorganizowane grupy przestępcze zaczynają odgrywać kluczową rolę. Miały także miejsce ataki typu DDoS i anonimowe zgłoszenia o ładunkach wybuchowych. Należy dodać, że szybki rozwój informatyki i najczęściej stosowanych technik inżynierii społecznej będzie się przyczyniać do wzrostu cyberprzestępczości.

3.3.2 Liczba zarejestrowanych przypadków cyberprzestępczości

Dane dotyczące cyberprzestępczości są gromadzone przez różne służby państwowe (Policję, prokuraturę oraz sądy podlegające Ministerstwu Sprawiedliwości) i odzwierciedlają różne etapy postępowań przygotowawczych w sprawie incydentów cybernetycznych.

Statystyki Prokuratury Generalnej ukazują liczbę wszczętych postępowań karnych oraz informacje o ich wynikach.

Dane sądowe są odrębne od statystyk organów ścigania. Dane zbierane przez Ministerstwo Sprawiedliwości (na podstawie sprawozdań statystycznych przekazywanych przez sądy) uwzględniają liczbę postępowań karnych, w których wniesiono akt oskarżenia, oraz wyniki tych spraw (liczbę skazanych osób i zasądzone kary).

Dane statystyczne o wykrytych przestępstwach, w tym cyberprzestępstwach, są zbierane i przetwarzane w Krajowym Systemie Informacyjnym Policji (KSIP). Dane zbierane są na podstawie przestępstw wymienionych w Kodeksie karnym i innych aktach prawnych zawierających przepisy karne, po czym dane te są zapisywane w KSIP, z uwzględnieniem różnych cech charakterystycznych dla każdego rodzaju przestępstwa.

Informacje o przestępstwie są zgłaszane po zakończeniu policyjnego postępowania przygotowawczego i w chwili gdy sprawa jest gotowa do przekazania prokuraturze, po tym jak sąd ds. nieletnich wyda decyzję o wszczęciu i zakończeniu postępowania w sprawie karnej, lub po tym gdy policja postanowi o przerwaniu postępowania przygotowawczego i sprawa jest wpisywana do rejestru przestępstw. Dopiero wtedy informacja ta jest wpisywana do KSIP.

Według polskich władz możliwe jest uzyskanie informacji o wstępnym postępowaniu przygotowawczym w sprawie cyberprzestępstwa (w odniesieniu do konkretnego artykułu Kodeksu karnego) tylko z wykorzystaniem Krajowego Systemu Informacyjnego Policji, poprzez uwzględnienie kategorii „modus operandi", np. „internet" lub „komputer". Należy jednak zauważyć, że przestępstwa są częściowo definiowane przez artykuły, których treść nie umożliwia ustalenia, czy przestępstwa te zostały popełnione w cyberprzestrzeni, ponieważ podawanie kontekstu danego przestępstwa (np. „sieć" czy „internet") nie jest obowiązkowe przy wypełnianiu formularzy w KSIP, chociaż kontekst ten może być podany w ramach „modus operandi".

Oprócz tego hakowanie komputerów, kradzież danych komputerowych, podsłuch komputerowy i ataki na urządzenia sieciowe są zgłaszane rzadko, co zwiększa liczbę przestępstw ukrytych. Przyczyny takiej sytuacji to m.in.: niska świadomość wśród użytkowników, którzy często są nieświadomi tego, że stali się ofiarą cyberprzestępstwa; niechęć do zgłaszania przestępstw związanych z nielegalnym posiadaniem danych na komputerze osobistym (np. pirackiego oprogramowania); lub, w przypadku przedsiębiorstw, z których skradziono dane komputerowe, pragnienie ukrycia tego faktu z obawy o utratę reputacji i klientów.

Krajowy System Informacyjny Policji nie jest zintegrowany z pozapolicyjną bazą danych.

W latach 2013–2015 zanotowano następujące dane statystyczne o liczbie zarejestrowanych spraw, postępowań przygotowawczych, wniesionych oskarżeń i wyroków skazujących:

Tabela 1: Dane Policji

Przestępstwa zgłoszone i wykryte w wybranych kategoriach prawnych w latach 2013–2015 – dane zestawione na podstawie modus operandi*:							
	Podstawa prawna (Zob. załącznik I)	2013		2014		2015	
		Przestępstwa zgłoszone	Przestępstwa wykryte	Przestępstwa zgłoszone	Przestępstwa wykryte	Przestępstwa zgłoszone	Przestępstwa wykryte
Kodeks karny	Art. 190a § 2	269	84	439	128	391	90
	Art. 200 § 1	10	8	7	6	26	24
	Art. 200a § 1	12	6	52	47	20	14
	Art. 200a § 2	88	78	57	45	176	159
	Art. 200b	1	0	3	2	1	0
	Art. 202 § 1	10	9	23	16	20	11
	Art. 202 § 2 (uchylony)[14]	35	29	66	58	8	7
	Art. 202 § 3	1 823	1 793	2 160	2 136	272	254
	Art. 202 § 4	23	22	19	14	6	5
	Art. 202 § 4a	242	220	120	106	54	46
	Art. 202 § 4b	7	6	8	6	2	2
	Art. 256 § 1	83	7	205	27	132	50
	Art. 256 § 2	1	0	8	6	4	3
	Art. 267 § 1	1 070	335	1 274	198	1 171	177
	Art. 267 § 2	61	18	74	9	75	10
	Art. 267 § 3	31	5	28	8	31	3
	Art. 267 § 4	1	1	4	1	7	4

[14] Art. 202 § 2 stanowił, że „Kto małoletniemu poniżej lat 15 prezentuje treści pornograficzne lub udostępnia mu przedmioty mające taki charakter albo rozpowszechnia treści pornograficzne w sposób umożliwiający takiemu małoletniemu zapoznanie się z nimi, podlega grzywnie, karze ograniczenia wolności lub pozbawienia wolności do lat 2". Artykuł ten uchylono nowelizacją Kodeksu karnego z dnia 4 kwietnia 2014 r. (która, po okresie *vacatio legis*, obowiązuje od dnia 26 maja 2014 r.) i tą samą nowelizacją wprowadzono go jako nowy art. 200 § 3, ze zmienionym wymiarem kary:

	Art. 268 § 1	112	20	84	21	54	6
	Art. 268 § 2	43	9	38	7	18	2
	Art. 268a § 1	329	72	374	79	286	58
	Art. 268a § 2	3	2				
	Art. 269a	27	2	23	4	23	2
	Art. 269b § 1	28	7	34	10	29	2
	Art. 271 § 1	117	117	7	5	102	102
	Art. 271 § 2			1	1	1	1
	Art. 271 § 3	27	27	1	1	54	54
	Art. 286 § 1	30 784	23 844	35 987	27 008	31 735	23 537
	Art. 286 § 1 w związku z art.294 § 1	17	14	28	11	34	8
	Art. 286 § 2	2	0	3	1	5	1
	Art. 286 § 3	174	134	335	257	172	106
	Art. 287 § 1	1 312	316	1 638	195	1 760	261
	Art. 287 § 1 w związku z art.294 § 1	2	1	2	2	7	0
	Art. 287 § 2	6	0	2	0	3	1
	Art. 310 § 1	117	19	90	16	59	16
	Art. 310 § 2	8	4	6	3	14	1
	Art. 310 § 4	5	5	2	2	3	2

* Zachowanie sprawcy w stosunku do ofiar: kontakt. Inne cechy zachowania: dokonywanie bezprawnych zmian w danych komputerowych; używanie na miejscu specjalnego oprogramowania komputerowego; łączenie się z siecią dostawcy usług internetowych; umieszczanie fałszywej strony internetowej podszywającej się pod istniejącą stronę internetową, by uzyskać dane w sposób nieupoważniony (phishing); łamanie lub omijanie zabezpieczeń serwera komputerowego; włamanie się do systemu komputerowego (haking); pogróżki przez internet lub telefon.

** Dane za rok 2015 odnoszą się do okresu od 1 stycznia do 30 września.

Tabela 2: Dane z Ministerstwa Sprawiedliwości

Rodzaj przestępstwa / przepis (artykuł kodeksu karnego)	Liczba skazanych osób	
Rok	2013	2014
Art. 200a (1)	2	3
Art. 200a (2)	13	24
Art. 202 (1)	1	-
Art. 202 (3)	55	38
Art. 202 (4a)	82	79
Art. 202 (4b)	3	1
Art. 267 (1)	47	44
Art. 268a	22	18
Art. 269a	4	1
Art. 269b (1)	1	1
Art. 270 (1)	6 482*	5 920*
Art. 271 (1)	491*	359*
Art. 287 (1)	42	48
Art. 287 (2)	1	4

* Całkowita liczba osób skazanych za dane przestępstwo bez konkretnego odniesienia do przestępstw związanych z komputerami

Analiza skali występowania zjawiska oszustw z wykorzystaniem kart płatniczych (najpowszechniej występującego rodzaju przestępstwa w obszarze elektronicznych instrumentów płatniczych) została przeprowadzona na podstawie danych uzyskanych z Systemu Elektronicznej Sprawozdawczości w Policji (SESPol) za lata 2013–2014.

Tabela 3: Przestępstwa związane z kartami płatniczymi (kartami, o których mowa w postępowaniach) w latach 2013–2014*

Rodzaj przestępstwa / zdarzenia		Karty kredytowe		Karty debetowe (w tym karty wydawane przez sklepy i stacje benzynowe)	
Okres		2013	2014	2013	2014
Podrobione karty	oszustwo z wykorzystaniem kart płatniczych (biały plastik)	221	226	23	31
	przetworzona karta	4	64	5	5
Karty	karty skradzione	7.792	8.044	8.106	7.582
	karty zgubione	679	895	734	698
Transakcje internetowe		912	1199	55	97
Karty niedoręczone		5	1	1	16
Transakcje przeprowadzone na podstawie aplikacji wykorzystujących fałszywe dane		74	22	15	7
Oszustwa z wykorzystaniem kart	nielegalne pozyskiwanie danych z kart w bankomatach	496	375	362	3.835
	nielegalne pozyskiwanie danych z kart	425	355	41	120
Inne (przestępstwo niewymienione, np. wykorzystanie danych karty płatniczej bez jej rzeczywistego posiadania)		182	468	68	225

* Dane z SESPol.

Tabela 4: Przestępstwa związane z kartami płatniczymi (kartami, o których mowa w postępowaniach) w roku 2015 (1 stycznia–30 września)*

Rodzaj przestępstwa / zdarzenia		Karty kredytowe	Karty debetowe (w tym karty wydawane przez sklepy i stacje benzynowe)
Okres		2015	2015
Podrobione karty	oszustwo z wykorzystaniem kart płatniczych (biały plastik)	8	23
	przetworzona karta	6	5
Karty	karty skradzione	2.512	8.106
	karty zgubione	270	734
Transakcje internetowe		221	55
Karty niedoręczone		1	1
Transakcje przeprowadzone na podstawie aplikacji wykorzystujących fałszywe dane		13	15
Oszustwa z wykorzystaniem kart	nielegalne pozyskiwanie danych z kart w bankomatach	180	362
	nielegalne pozyskiwanie danych z kart	174	41
Inne (przestępstwo niewymienione, np. wykorzystanie danych karty płatniczej bez jej rzeczywistego posiadania)		70	68

* Dane z SESPol.

Pomimo statystyk oceniający nie stwierdzili, by istniała jakakolwiek wymiana ustrukturyzowanych danych między Policją a prokuratorami lub sądami, umożliwiająca prześledzenie historii danej sprawy. W związku z tym istnieją znaczne trudności w rejestrowaniu statystyk dotyczących cyberprzestępczości od początku do końca. Zdaniem oceniających dzielenie się danymi statystycznymi między organami ścigania a organami wymiaru sprawiedliwości mogłoby mieć istotne znaczenie dla mechanizmu monitorowania, a także ustalania priorytetowych celów podczas zwalczania tego zjawiska.

3.4 Budżet krajowy przeznaczony na zapobieganie cyberprzestępczości i na jej zwalczanie oraz wsparcie ze strony funduszy unijnych

Uznaje się, że zapobieganie cyberprzestępczości i jej zwalczanie należą do ogólnych działań prokuratury i sądów karnych. Zgodnie z polskim prawem budżetowym wydatki tych służb nie są związane z poszczególnymi rodzajami przestępczości, lecz są pokrywane z odpowiednich części budżetów tych służb.

Plan wydatków budżetowych dla jednostek Policji opracowywany jest zgodnie z *rozporządzeniem Ministra Finansów z 2010 r. w sprawie szczegółowej klasyfikacji dochodów, wydatków, przychodów i rozchodów oraz środków pochodzących ze źródeł zagranicznyc*h. Podczas planowania budżetu na 2015 r. środki na wydatki materialne zostały podzielone na podstawie decyzji komendantów wojewódzkich (regionalnych) policji (dysponentów środków budżetowych trzeciego stopnia) zgodnie z priorytetami i potrzebami podlegających im jednostek Policji. Oznacza to, że budżet Policji nie zawiera środków specjalnie przeznaczonych na zapobieganie cyberprzestępczości i jej zwalczanie. Jedyne środki finansowe przeznaczone na ten cel znajdują się w planie wydatków Biura Łączności i Informatyki Komendy Głównej Policji, gdyż wykonuje ono zadania związane z ochroną cyberprzestrzeni zawierającej infrastrukturę policji.

W 2014 r. Biuro Łączności i Informatyki Komendy Głównej Policji wydało na ten cel 2 132 217 PLN (488 984 EUR); wydatki planowane na ten cel w 2015 r. wynosiły 4 925 300 PLN (1 129 526 EUR).
Wdrażanie projektów zwalczania cyberprzestępczości jest również finansowane przez Unię Europejską i Norweski Mechanizm Finansowy. Wspomniane zasoby finansowe wydawane są na szkolenie polskich funkcjonariuszy w zakresie szeregu aspektów dotyczących zwalczania przestępczości komputerowej.

Podczas konsultacji dotyczących Programu Krajowego Funduszu Bezpieczeństwa Wewnętrznego na lata 2014–2020, jeden z wniosków przedłożonych w trakcie procesu oceny potrzeb dotyczył zastąpienia istniejącej bazy operacyjnej (SIO) i utworzenia elektronicznej bazy szkoleniowej. Celem tego projektu jest ułatwienie szybkiego i sprawnego funkcjonowania nowoczesnej i niezawodnej policyjnej bazy operacyjnej poprzez wyszkolenie profesjonalnej kadry, wymianę stacji dostępu, serwerów i oprogramowania oraz polepszenie wymiany informacji między służbami zajmującymi się zapobieganiem przestępczości, w tym cyberprzestępczości, i terroryzmowi oraz ich zwalczaniem.

3.5 Wnioski

- Od 2014 r. obowiązuje w Polsce krajowa strategia cyberbezpieczeństwa, której celem jest zapewnienie bezpieczeństwa cyberprzestrzeni kraju, w szczególności, jeśli chodzi o publiczną infrastrukturę krytyczną ICT uważaną za mającą podstawowe znaczenie dla funkcjonowania usług publicznych, takich jak usługi energetyczne i opieka zdrowotna, a także prywatnych przedsiębiorstw, w tym sektora finansowego. Strategia ta jest jednak fragmentaryczna i uzupełniają ją dwa inne dokumenty: *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* określająca wytyczne, którymi kierować się mają organy publiczne i organy ścigania; oraz *Doktryna cyberbezpieczeństwa RP* zawierająca cele odnoszące się do bezpiecznego funkcjonowania państwa jako całości w cyberprzestrzeni.

- Polska jasno zdefiniowała swoje priorytety krajowe, jeśli chodzi o cyberprzestępczość i cyberbezpieczeństwo. Priorytety te obejmują cyberobronę, cyberbezpieczeństwo, cyberprzestępczość, świadomość i szkolenie. Priorytety Policji są ponadto jasno opisane i obejmują aspekty operacyjne, potrzeby szkoleniowe, aspekty dotyczące usprawnienia sprzętu i oprogramowania, świadomości i bezpieczeństwo.

- Zdaniem oceniających opracowana przez Polskę strategia i zdefiniowane priorytety stanowią solidną podstawę zwalczania cyberprzestępczości. Jednakże istnienie różnych dokumentów dotyczących bezpieczeństwa cybernetycznego wydaje się utrudniać Ministerstwu Cyfryzacji koordynowanie wdrażania strategii, ponieważ nie ma ono niezbędnych uprawnień. Dlatego też oceniający uważają, że Polsce brakuje organu koordynującego podmioty faktycznie zajmujące się zwalczaniem cyberprzestępczości i jednego nadrzędnego dokumentu ustanawiającego krajową strategię cyberbezpieczeństwa na szczeblu centralnym.

- Ponadto, mimo informacji przekazanych przez władze polskie, oceniający nie znaleźli wystarczających informacji dotyczących zaangażowania sądownictwa (sędziów i prokuratorów) w opracowanie strategii cyberbezpieczeństwa kraju. Dlatego też, biorąc pod uwagę niezmiernie ważną rolę, jaką odgrywają sędziowie i prokuratorzy, oceniający odnotowują pewien brak proaktywnej postawy z ich strony przy ustalaniu własnych priorytetów. Zdaniem oceniających taka proaktywna postawa mogłaby zwiększyć kompetencje zawodowe sędziów i prokuratorów oraz skuteczność zwalczania cyberprzestępczości.

- Uregulowanie partnerstw publiczno-prywatnych (w tym obejmujących organizacje pozarządowe i zespoły reagowania), a także wyposażenie operatorów infrastruktury krytycznej w ramy ustanawiające obowiązki i przepisy mogłoby usprawnić przepływ informacji i zarządzanie.

- Główny Urząd Statystyczny Rzeczypospolitej Polskiej odpowiada za gromadzenie i rozpowszechnianie danych statystycznych. Istnieje wiele źródeł gromadzenia danych statystycznych dotyczących cyberprzestępczości i cyberbezpieczeństwa, głównymi źródłami tych statystyk są jednak Krajowy System Informacyjny Policji (KSIP) i CERT POLSKA.

- W KSIP odnotowywane są informacje na temat liczby zgłoszonych i wykrytych przestępstw oraz rozpoczętych i zakończonych śledztw. CERT POLSKA odnotowuje liczbę zdarzeń zgłoszonych mu przez społeczeństwo lub wykrytych przez samą organizację. Ponieważ nie ma jednolitej definicji cyberprzestępczości ustalonej w ustawodawstwie, wydaje się, że bardzo trudno jest wyliczyć wszystkie zdarzenia, które wchodzą w zakres cyberprzestępczości. Wydaje się ponadto, że sposoby, za pomocą których KSIP i CERT POLSKA gromadzą dane statystyczne wzajemnie się pokrywają; jest to spowodowane tym, iż zdarzenia zgłaszane CERT POLSKA mogą stanowić część zdarzeń zgłaszanych w rejestrze KSIP.

- Statystyki dotyczące cyberprzestępczości są niskie. Wydaje się, że gdyby kk uznał przestępstwa związane z cyberprzestępczością za odrębne przestępstwa kryminalne, można by umocnić organy ścigania zaangażowane w zwalczanie cyberprzestępczości. Brakuje niektórych statystyk, gdyż nie odróżnia się przestępstw popełnionych z wykorzystaniem środków elektronicznych od innych przestępstw, np. tradycyjnego oszustwa lub fałszerstwa od oszustwa lub fałszerstwa komputerowego. Oceniający mają zatem pewne wątpliwości, czy wszystkie zainteresowane strony zajmujące się zwalczaniem cyberprzestępstw rozumieją to pojęcie w ten sam sposób.

- Ponieważ nie można prześledzić powiązania między zgłoszonymi przestępstwami, wniesionymi oskarżeniami i wyrokami skazującymi, istnieją znaczne trudności w rejestrowaniu statystyk dotyczących cyberprzestępczości od jej początku do końca. Częściowym rozwiązaniem mogłoby być ustanowienie przez organy ścigania i organy sądowe wspólnych definicji.

- Ani Policja ani też rząd nie mają budżetu przeznaczonego specjalnie na podnoszenie świadomości w odniesieniu do cyberprzestępczości i bezpieczeństwa cybernetycznego. Jednak w ramach ogólnego budżetu Policji dostępne są środki na ten cel. Ponadto zauważono, że organizacje pozarządowe i sektor rządowy skutecznie współpracują przy występowaniu o środki europejskie w celu zwiększenia świadomości w dziedzinie cyberprzestępczości i bezpieczeństwa cybernetycznego i przy ich przyznawaniu. Ministerstwo Cyfryzacji dokonuje przeglądu wszystkich wniosków o dotacje przed ich przedłożeniem.

4 STRUKTURY KRAJOWE

4.1 Wymiar sprawiedliwości (prokuratura i sądy)

4.1.1 Struktura wewnętrzna

W Polsce prowadzenie postępowań przygotowawczych leży w gestii prokuratorów.
W ramach prokuratury nie ma specjalnych struktur, których zadaniem byłoby ściganie cyberprzestępczości ani wyznaczonych sądów, które zajmowałyby się wyłącznie tego rodzaju sprawami. Z drugiej strony takie struktury stworzono na szczeblu regionalnym w Policji.

Jednak na poziomie Prokuratury Krajowej wyznaczono kilku prokuratorów w celu zapewnienia koordynacji i wsparcia na niższych szczeblach prokuratury w sprawach dotyczących ataków cybernetycznych (ataków na systemy komputerowe), przestępstw z nienawiści oraz wykorzystywania seksualnego dzieci. Na szczeblu regionalnym wyznaczono ponadto prokuratorów w celu koordynacji spraw związanych z wykorzystywaniem seksualnym dzieci. Prokuratorzy ci ściśle współpracują z funkcjonariuszami Policji, zapewniając doradztwo w najtrudniejszych sprawach.

Zdaniem oceniających wyraźna specjalizacja Policji nie miała odpowiednika w ramach prokuratury.

Po wizycie na miejscu poinformowano zespół oceniający, że w kwietniu 2016 r. w Prokuraturze Krajowej w Departamencie do Spraw Przestępczości Gospodarczej została utworzona wyspecjalizowana jednostka do spraw cyberprzestępczości. W maju 2016 r. we wszystkich prokuraturach regionalnych powołano koordynatorów do spraw cyberprzestępczości.

4.1.2 Zdolności w sferze skutecznego ścigania i przeszkody w tej dziedzinie

Do wymienionych przez polskie władze głównych przeszkód w ściganiu cyberprzestępstw należą:

- W ujęciu krajowym: brak wystarczających zasobów (ludzkich i technicznych) oraz ograniczenia w gromadzeniu danych związane z poufnością informacji bankowych.
- W ujęciu międzynarodowym: długie i złożone procedury wzajemnej pomocy prawnej, różnice między systemami prawnymi (istnienie bezpiecznych przystani w cyberprzestrzeni), serwery umiejscowione w krajach, w których nie ma polskiej ani unijnej jurysdykcji, złożona sytuacja prawna dotycząca zatrzymywania danych w UE i w krajach trzecich (np. różne okresy zatrzymywania danych), brak legalnej bazy danych na temat urządzeń do kradzieży danych zawartych na pasku magnetycznym kart płatniczych (skimming), długi okres oczekiwania na międzynarodową pomoc prawną oraz wybór sądu pod kątem własnego interesu.

Jako główne przeszkody w wykrywaniu i zwalczaniu cyberprzestępczości wymieniono ponadto niezarejestrowane przedpłacone karty telefoniczne, trudności w identyfikowaniu użytkowników anonimowych sieci (sieci Tor) oraz fakt, że dostawcy internetu nie mają obowiązku nieodpłatnego reagowania na wnioski organów ścigania[15].

[15] Wydaje się, że rozwiązano niektóre z kwestii zasygnalizowanych podczas wizyty na miejscu jako przeszkody. Ustawa antyterrorystyczna z 10 czerwca 2016 r., przyjęta po wizycie na miejscu, wymaga, by użytkownicy kart przedpłaconych rejestrowali swoje karty sim. Abonenci będący stroną umowy o świadczenie usług telekomunikacyjnych, w tym usług przedpłaconych, muszą podać dostawcy usług swoje dane. W przypadku abonenta będącego osobą fizyczną musi on podać przynajmniej imię i nazwisko oraz numer PESEL, jeśli go posiada, albo nazwę, serię i numer dokumentu potwierdzającego tożsamość. W przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej – numer paszportu lub karty pobytu. W przypadku abonenta niebędącego osobą fizyczną musi on podać nazwę i numer identyfikacyjny REGON lub NIP lub numer w Krajowym Rejestrze Sądowym albo ewidencji działalności gospodarczej, lub innym właściwym rejestrze. Dostawca usług może rozpocząć świadczenie usług telekomunikacyjnych nie wcześniej niż po potwierdzeniu zgodności podanych przez abonenta danych. Rejestracja kart przedpłaconych zmniejsza anonimowość sprawców różnych przestępstw i pomaga zapobiegać przestępstwom. Ponadto zgodnie z ustawą o zmianie ustawy o Policji oraz niektórych innych ustaw z 15 stycznia 2016 r. obowiązek nieodpłatnego udostępniania danych Policji został rozszerzony z przedsiębiorstw telekomunikacyjnych również na operatorów świadczących usługi drogą elektroniczną.

Nie ma również ustawodawstwa dotyczącego możliwości monitorowania szyfrowanych sieci łączności[16].

Ponadto w oparciu o *Ustawę* o *świadczeniu usług drogą elektroniczną* niektórzy dostawcy usług internetowych nie dostarczają nieodpłatnie danych, o które zwraca się Policja. W dodatku przedsiębiorstwa globalne, takie jak Google czy Facebook, mają swoje własne określone procedury i współpraca z nimi nie podlega prawu krajowemu. Przedsiębiorstwa te wprawdzie podejmują w konkretnych przypadkach decyzje o dostarczeniu danych, lecz przypadki te nie odpowiadają wszystkim przestępstwom skutkującym karą na podstawie polskich przepisów. Nie ma w tej dziedzinie wspólnych uregulowań międzynarodowych.

Aby zwiększyć zdolności prokuratorów i sędziów, władze polskie planują zwiększyć liczbę kursów dotyczących cyberprzestępczości organizowanych przez Krajową Szkołę Sądownictwa i Prokuratury i włączyć ten temat do innych programów szkoleniowych (dotyczących prawa dowodowego, praw ofiar itd.).

4.2 Organy ścigania

Dochodzenia wstępne prowadzone są przez jednostki Policji usytuowane w komendach wojewódzkich (regionalnych) Policji.

Na szczeblu centralnym w ramach Biura Kryminalnego KGP utworzono Wydział do walki z Cyberprzestępczością (25 funkcjonariuszy). Jego główne zadania obejmują:

1) koordynowanie i inicjowanie działań policyjnych w celu identyfikowania zagrożeń przestępczością internetową;
2) rozwijanie współpracy z sektorem publicznym, prywatnym i z jednostkami akademickimi w celu określenia sposobu gromadzenia i wymiany informacji na temat przestępczości w cyberprzestrzeni;
3) przeprowadzanie technicznych konsultacji oraz współpraca z krajowymi i zagranicznymi jednostkami w celu określenia i wdrożenia najnowocześniejszych rozwiązań w walce z przestępczością w cyberprzestrzeni;

[16] Polskie władze poinformowały po wizycie na miejscu, że monitorowanie szyfrowanych sieci łączności opiera się na ogólnych zasadach nadzoru, lecz dostęp do przedmiotowych danych zależy od możliwości technicznych, które wciąż ulegają zmianom.

4) rozmieszczanie i utrzymywanie specjalnych systemów informatycznych w celu wykonywania zadań, takich jak monitorowanie internetu, aby wykryć przestępstwa lub nielegalną treść, wykrywanie użytkowników anonimowej sieci, zapewnianie zdalnego dostępu na rzecz wydzielonych komórek powołanych w strukturach komend wojewódzkich policji;
5) przygotowywanie opinii na temat ustawodawstwa w dziedzinie bezpieczeństwa informatycznego i zmian tego ustawodawstwa;
6) organizowanie szkoleń w miejscu pracy dla funkcjonariuszy policji pod kierownictwem wspomnianego wydziału.

W październiku 2014 r. w każdej komendzie wojewódzkiej (regionalnej) Policji stworzono specjalną strukturę ds. zwalczania cyberprzestępczości. Obecnie działa 19 jednostek w komendach wojewódzkich Policji, Komendzie Stołecznej Policji, w tym Centralne Biuro Śledcze Policji i Wydział do walki z Cyberprzestępczością w Biurze Kryminalnym Komendy Głównej Policji; pracuje w nich sumie 240 pracowników zatrudnionych na czas nieokreślony. Jednostki te są ciągle wyposażane w sprzęt i szkolone, aby polepszyć kwalifikacje funkcjonariuszy. policyjne czynności operacyjne, forensyka, współpraca międzynarodowa prowadzona bezpośrednio lub poprzez Biuro Międzynarodowej Współpracy Policji, współpraca z dostawcami treści internetowych, ICT, koordynacja zadań i wdrażanie nowych narzędzi.

W ramach tej struktury Wydział do walki z Cyberprzestępczością jest również całodobowym punktem kontaktowym dla funkcjonariuszy Policji i obywateli; można się z nim kontaktować przy pomocy poczty elektronicznej lub telefonicznie, aby przekazać informacje o wszelkiego rodzaju zdarzeniach związanych z internetem, komputerami oraz inne istotne kwestie. W przypadku wniosków międzynarodowych za koordynację zadań odpowiada głównie Biuro Międzynarodowej Współpracy Policji KGP.

W ramach Centralnego Biura Śledczego Policji został również utworzony Wydział ds. Zwalczania Cyberprzestępczości (15 pracowników). Głównym zadaniem wydziału jest zwalczanie cyberprzestępstw popełnianych przez zorganizowane grupy przestępcze. Wydział jest wyposażony w bardzo zaawansowane laboratorium, które oferuje szeroki wachlarz narzędzi i rozwiązań, w tym komorę laminarną (dla bezpiecznej ekstrakcji danych ze zniszczonych nośników elektronicznych) oraz sprzęt do łamania haseł w zaszyfrowanych plikach.

Wydział stale oferuje swoje wsparcie wydziałom ds. zwalczania cyberprzestępczości w komendach wojewódzkich Policji oraz Wydziałowi do walki z Cyberprzestępczością w KGP.

Ponadto przestępstwami takimi jak pedofilia, wykorzystywanie seksualne dzieci i pornografia dziecięca, a także przestępstwami z wykorzystaniem kart płatniczych, zajmują się różne jednostki w ramach KGP (Biuro Kryminalne) i wojewódzkich (regionalnych) komend policji.

W Biurze Łączności i Informatyki KGP są jednostki specjalne skupiające się na atakach cybernetycznych i cyberprzestrzeni. Istnieje również specjalne stanowisko ds. bezpieczeństwa cyberprzestrzeni: *pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni*, który zajmuje się głównie koordynacją działań w ramach infrastruktury sieci policyjnej zgodnie z decyzją Komendy Głównej Policji nr 415/2014.

Na polu pracy operacyjnej policja współpracuje z Agencją Bezpieczeństwa Wewnętrznego i ze Służbą Kontrwywiadu Wojskowego. Aby zapobiegać cyberprzestępstwom i je zwalczać, z Policją i z innymi instytucjami współpracuje ponadto Straż Graniczna.

Policja zajmuje się również stałym monitorowaniem internetu, ze szczególnym naciskiem na obszary kryminogenne; podejmuje również inicjatywy w celu zwiększenia świadomości i bezpieczeństwa użytkowników internetu. Policja współpracuje również z operatorami telefonicznymi, dostawcami usług internetowych oraz z ekspertami w dziedzinie zwalczania cyberprzestępczości z innych krajów. Wydział do walki z Cyberprzestępczością współpracuje ponadto na szczeblu krajowym i międzynarodowym z instytucjami państwowymi oraz z sektorem prywatnym i publicznym w celu uzyskiwania informacji na temat metod i form przestępstw popełnianych w cyberprzestrzeni.

4.3 Inne władze/instytucje/partnerstwo publiczno-prywatne

Polska posiada zdecentralizowany system ochrony cyberprzestrzeni. Kompetencje dotyczące bezpieczeństwa w cyberprzestrzeni dzielone są między innymi pomiędzy Ministerstwem Cyfryzacji, Ministerstwem Spraw Wewnętrznych i Administracji, Ministerstwem Obrony Narodowej, Ministerstwem Sprawiedliwości, Rządowym Centrum Bezpieczeństwa, Urzędem Komunikacji Elektronicznej, Generalnym Inspektorem Ochrony Danych Osobowych, Ministerstwem Rozwoju, Ministerstwem Spraw Zagranicznych, Agencją Bezpieczeństwa Wewnętrznego, Policją, Agencją Wywiadu, Służbą Kontrwywiadu Wojskowego oraz Narodowym Bankiem Polskim, a także CERT POLSKA będące częścią polskiej Naukowej i Akademickiej Sieci Komputerowej (NASK).

Oprócz tego Polska ma publiczne i prywatne zespoły reagowania na incydenty związane z bezpieczeństwem komputerowym (CSIRT) obejmujące, między innymi, administrację rządową, administrację wojskową oraz Policję, a także zespoły utworzone przez operatorów telekomunikacyjnych i środowiska naukowe i badawcze. Wyżej wymienione instytucje pracują nad zadaniami dotyczącymi bezpieczeństwa cybernetycznego, zapobiegania cyberprzestępczości oraz cyberobrony.

Ministerstwo Cyfryzacji

Ministerstwo Cyfryzacji odpowiada za:

- polityczną i strategiczną koordynację cyberprzestrzeni na rzecz bezpieczeństwa cybernetycznego w Polsce;
- zapewnienie minimalnych wymogów w zakresie bezpieczeństwa ICT w administracji publicznej
- określanie minimalnych wymogów dla rejestrów publicznych i wymiany informacji elektronicznych, a także minimalnych wymogów dla systemów ICT (w oparciu o ustawę z 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne oraz rozporządzenie Rady Ministrów z 2012 r. w sprawie Krajowych Ram Interoperacyjności);

– nadzorowanie Urzędu Komunikacji Elektronicznej, do którego operatorzy telekomunikacyjni zgłaszają najważniejsze incydenty cybernetyczne dotyczące sieci telekomunikacyjnych (zgodnie z ustawą z 2004 r. Prawo telekomunikacyjne);
– nadzorowanie NASK jako instytutu badawczego i operatora sieci transmisji danych oraz Narodowego Centrum Cyberbezpieczeństwa, które jest częścią wspomnianego instytutu.

Agencja Bezpieczeństwa Wewnętrznego (ABW)

Działania ABW w odniesieniu do zagrożeń w cyberprzestrzeni skupiają się na:

– - koordynowaniu w odpowiedzi na incydenty zagrażające bezpieczeństwu systemów i sieci ICT wykorzystywanych przez organy państwowe (zadanie CERT.GOV.PL);
– - rozwijaniu zdolności administracji publicznej do ochrony zasobów ICT;
– - nadzorowaniu systemu wczesnego ostrzegania o zagrożeniach w sieciach administracji publicznej (ARAKIS-GOV);
– - zwalczaniu cyberterroryzmu (nielegalnych ataków lub groźby ataku na komputery, sieci lub systemy informatyczne w wyniku działań grup terrorystycznych lub zagranicznych służb wywiadowczych).

Rządowy Zespół Reagowania na Incydenty Komputerowe (CERT.GOV.PL)

CERT.GOV.PL został utworzony 1 lutego 2008 r. w ramach ABW; zapewnia i rozwija zdolności jednostek administracji publicznej w zakresie ochrony przed zagrożeniami cybernetycznymi, w szczególności atakami na infrastrukturę obejmującą systemy i sieci informatyczne, których zniszczenie lub zakłócenie może znacząco zagrozić życiu i zdrowiu ludności, dziedzictwu narodowemu lub środowisku, lub prowadzić do

znacznych strat finansowych lub zakłócić funkcjonowanie podmiotów sektora publicznego. Zgodnie z tą polityką CERT.GOV.PL pełni zasadniczo rolę zespołu reagowania na incydenty komputerowe (CERT) w dziedzinie administracji rządowej. Publikuje roczne sprawozdania na temat stanu bezpieczeństwa cybernetycznego w Polsce.

Zespoły reagowania na incydenty komputerowe (CERT)

Nie ma jednego zespołu reagowania na incydenty komputerowe, lecz wiele zespołów CERT zajmujących się zagadnieniem ogólnie zdefiniowanym jako bezpieczeństwo ICT. Oprócz CERT.GOV.PL istnieje również Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych w ramach Ministerstwa Obrony Narodowej zajmujące się zapobieganiem incydentom, które mogłyby mieć skutki dla obronności Polski, oraz zespoły utworzone przez środowisko telekomunikacyjne, w tym CERT OPL i PIONIERCERT, a także CERT POLSKA (CERT.pl), który funkcjonował w czasie wizyty na miejscu w ramach Naukowej i Akademickiej Sieci Komputerowej (NASK)[17]. Równocześnie Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych odgrywa podobną rolę w siłach zbrojnych.

NASK

NASK to instytut badawczy i operator sieci transmisji danych uprzednio nadzorowany przez Ministerstwo Nauki i Szkolnictwa Wyższego. Zgodnie z nowym rozporządzeniem przyjętym przez Radę Ministrów od 1 stycznia 2016 r. NASK podlega nadzorowi Ministerstwa Cyfryzacji. Prowadzone przez NASK badania mają na celu rozwijanie rozwiązań zwiększających skuteczność, niezawodność i bezpieczeństwo sieci informatycznych. NASK prowadzi również działania związane ze zwiększaniem bezpieczeństwa internetu i reagowaniem na incydenty, które naruszają bezpieczeństwo sieci. Odpowiada za to CERT POLSKA, a inny zespół – Dyżurnet.pl – przyjmuje sprawozdania dotyczące nielegalnych działań w internecie i przekazuje je policji. NASK oferuje innowacyjne rozwiązania IT dla klientów biznesowych, rządu i sektora naukowego. CERT POLSKA został założony w 1997 r. jako pierwszy zespół CERT w Polsce. CERT POLSKA funkcjonuje w ramach struktury NASK, wiodącego krajowego rejestratora domen. CERT POLSKA pełni de facto rolę krajowego CERT (i jako taki jest umieszczony w dokumentach ENISA).

[17] Po wizycie na miejscu poinformowano zespół oceniający, że w ramach Naukowej i Akademickiej Sieci Komputerowej (NASK), której częścią jest CERT.POLSKA, utworzono Narodowe Centrum Cyberbezpieczeństwa (NC Cyber). Głównym zadaniem Narodowego Centrum Cyberbezpieczeństwa jest gromadzenie informacji o incydentach z kluczowych sektorów i współpraca z policją w dziedzinie cyberprzestępczości.

Policja prowadzi projekty naukowe we współpracy z sektorem prywatnym (badacze z dziedziny wdrażania oprogramowania i narzędzi w celu zwalczania cyberprzestępczości z Akademii Górniczo-Hutniczej i Politechniki Warszawskiej) w ramach Polskiej Platformy Bezpieczeństwa Wewnętrznego. Przykłady współpracy policyjnej z sektorem prywatnym:

- Wyższa Szkoła Policji w Szczytnie jest członkiem konsorcjum w siódmym programie ramowym: Comprehensive approach to cyber roadmap coordination and development (CAMINO) – 2014-2016 O ROB 0003 03 001.
- Funkcjonariusze Policji byli członkami konsorcjum w projekcie CIPS/ISEC: Creation of a Polish Centre of Excellence for Research on Cybercrime - 2013-2014 HOME / 2012 / ISEC / INT / 4000003858.

W ramach współpracy z sektorem prywatnym, który odpowiada za bezpieczeństwo w niedawno stworzonych urządzeniach do programowania, planuje się, by Policja uczestniczyła w tworzeniu nowych technologii dla sektora finansów. Wspólnie ze Związkiem Banków Polskich zostaną przeprowadzone testy, by zapewnić, że rozwiązania IT będą odporne na przestępstwa.
Warto również wspomnieć o współpracy ze Związkiem Banków Polskich i z Fundacją Dzieci Niczyje (zob. rozdziały 6.2.3, 6.3.2 i 8.2).

4.4 Współpraca i koordynacja na szczeblu krajowym

4.4.1 Obowiązki z tytułu przepisów prawa lub prowadzonej polityki

Na podstawie Polityki ochrony cyberprzestrzeni Rzeczypospolitej Polskiej minister cyfryzacji pełni rolę koordynatora ochrony cyberprzestrzeni w odniesieniu do urzędów administracji rządowej na szczeblu strategicznym i politycznym. Komitet Rady Ministrów ds. Cyfryzacji 13 kwietnia 2015 r. uzgodnił i przyjął Plan działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP. Plan działań jest obecnie wdrażany i zawiera zalecenia dotyczące bezpieczeństwa cyberprzestrzeni dla

całej administracji rządowej. Celem strategicznym polityki jest osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni. Należy sprecyzować, że termin „akceptowalny” jest używany w sensie standardów zarządzania ryzykiem, ponieważ na tym podejściu opiera się przedmiotowa polityka. Działania i środki, które należy przedsięwziąć w celu osiągnięcia tego celu są wynikiem ocen zagrożeń bezpieczeństwa cybernetycznego przeprowadzanych przez odnośne organy publiczne.

Głównym zadaniem Rządowego Zespołu Reagowania na Incydenty Komputerowe (CERT.GOV.PL), będącego częścią Agencji Bezpieczeństwa Wewnętrznego, jest wykonywanie zadań operacyjnych związanych z bezpieczeństwem systemów informatycznych organów publicznych. Jego głównym zadaniem jest zapewnienie i rozwijanie zdolności organów administracji publicznej do ochrony przed zagrożeniami cybernetycznymi, w szczególności przed atakami wymierzonymi w infrastrukturę ICT. CERT.GOV.PL zajmuje się przede wszystkim incydentami cybernetycznymi w sektorze publicznym, a jego działania obejmują koordynację procesu reagowania na incydenty, rozwiązywanie incydentów i ich analizę oraz koordynację reagowania na naruszenia bezpieczeństwa. W przypadku incydentów o szerokich skutkach oddziaływania, zespół koordynuje działania w związku z danym incydentem i na niego reaguje oraz wymienia informacje z instytucjami, których bezpośrednio dotknął atak cybernetyczny. Ponadto zespół wykorzystuje doświadczenie zdobyte podczas poprzednich incydentów, przygotowuje ostrzeżenia zawierające informacje techniczne i zalecenia dotyczące dalszych działań oraz przekazuje je jednostkom administracji rządowej. Proces ten ma na celu uniknięcie podobnych ataków na inne instytucje lub zmniejszenie możliwości ich wystąpienia.

Nadzwyczaj istotną rolę odgrywa CERT POLSKA, którego zadania obejmują reagowanie na zagrożenia i incydenty w polskiej domenie internetowej (.pl), publikowanie rocznych sprawozdań na temat zagrożeń cybernetycznych oraz tworzenie narzędzi i systemów informatycznych w celu zwiększenia potencjału kraju w zakresie cyberbezpieczeństwa, np. systemu wczesnego ostrzegania, oraz platformy wymiany wiedzy i informacji znanej jako ARAKIS.

W 2015 r. decyzją Komendanta Głównego Policji w ramach KGP powołano zespół reagowania na incydenty komputerowe (POL-CERT).

Zespół wykonuje zadania związane z koordynacją procesu reagowania na incydenty komputerowe w policyjnych systemach teleinformatycznych i sieciach teleinformatycznych. W wojewódzkich (regionalnych) komendach policji oraz w szkołach policyjnych ustanowiono punkty kontaktowe do spraw cybernetycznych, z myślą o uproszczeniu przepływu informacji o wydarzeniach. W przyszłości zespół reagowania na incydenty komputerowe POL-CERT będzie stanowić element polskiego systemu reagowania na incydenty komputerowe w cyberprzestrzeni.

4.4.2 Zasoby przeznaczone na polepszenie współpracy

Obecnie polska Policja jest w trakcie wyposażania niedawno utworzonych jednostek do zwalczania cyberprzestępczości. Planuje się stworzenie nowoczesnych narzędzi, które usprawnią pracę i pomogą zidentyfikować cyberprzestępstwa popełniane w nowym medium – internecie. Jednostki zwalczające cyberprzestępczość mają wyspecjalizowane oprogramowanie i narzędzia umożliwiające ujawnianie i zabezpieczanie dowodów elektronicznych.

Sprzęt i oprogramowanie wykorzystywane w walce z cyberprzestępczością, w szczególności w dziedzinie informatyki śledczej, należą do licencjonowanych narzędzi wykorzystywanych przez organy ścigania na całym świecie. W 2016 r. planowano zbudowanie platformy sprzętowej do studiowania złośliwego oprogramowania, aby znacząco przyspieszyć działania Policji podczas ścigania tego typu przestępstw i zwiększyć skuteczność tych działań.

4.5 Wnioski

- Za ściganie przestępstw i sądownictwo odpowiada Ministerstwo Sprawiedliwości. Nie ma sędziów zajmujących się wyłącznie sprawami związanymi z cyberprzestępczością. W praktyce jednak do zajmowania się tego rodzaju sprawami, przynajmniej o większym ciężarze gatunkowym, zazwyczaj wyznaczani są sędziowie zaznajomieni z kwestiami z zakresu cyberprzestępczości.

- Na szczeblu prokuratury nie ma wyspecjalizowanych jednostek do spraw cyberprzestępczości. Jednak w Prokuraturze Krajowej utworzono grupę wyznaczonych prokuratorów. Jej zadaniem jest koordynowanie i wspieranie przeprowadzanych na szczeblu regionalnym postępowań przygotowawczych dotyczących cyberprzestępczości, przestępstw z nienawiści oraz wykorzystywania seksualnego dzieci. Po wizycie na miejscu poinformowano zespół oceniający, że w kwietniu 2016 r. w Prokuraturze Krajowej w Departamencie do Spraw Przestępczości Gospodarczej została utworzona wyspecjalizowana jednostka do spraw cyberprzestępczości. W maju 2016 r. we wszystkich prokuraturach regionalnych powołano koordynatorów do spraw cyberprzestępczości.

- Policja jest faktycznie podporządkowana Ministerstwu Spraw Wewnętrznych i Administracji i sprawia wrażenie dobrze uporządkowanej organizacji o jasnym mandacie i wyraźnym zakresie odpowiedzialności. W Komendzie Głównej Policji działa wyspecjalizowana jednostka – Wydział do walki z Cyberprzestępczością, który zajmuje się pornografią dziecięcą, cyberatakami i oszustwami w sieci. Wydział ten składa się z 25 dobrze wyszkolonych funkcjonariuszy, do których obowiązków należy m.in. monitorowanie i doradzanie śledczym z Policji na szczeblu regionalnym zajmującym się sprawami z zakresu cyberprzestępczości. Wydział do walki z Cyberprzestępczością zapewnia wsparcie jednostkom Policji ds. zwalczania cyberprzestępczości na szczeblu województw/regionów.

- Ponadto na szczeblu regionalnym (województw) utworzono wyspecjalizowane jednostki do zwalczania cyberprzestępczości; każda jednostka liczy przeciętnie 10 funkcjonariuszy. Postępowania przygotowawcze w sprawie przestępstw, takich jak pedofilia, wykorzystywanie seksualne dzieci i pornografia dziecięca, mogą w związku z tym prowadzić różne jednostki: na szczeblu centralnym – Centralne Biuro Śledcze Policji lub na szczeblu regionalnym – komendy wojewódzkie policji. W razie konieczności polska Policja prowadzi współpracę operacyjną z Agencją Bezpieczeństwa Wewnętrznego i ze Służbą Kontrwywiadu Wojskowego. Jako przykłady optymalnych rozwiązań można by wymienić wewnętrzną strukturę Policji oraz wyznaczenie wyspecjalizowanych funkcjonariuszy Policji do zajmowania się cyberprzestępczością.

- Na szczeblu Komendy Głównej Policji w ramach Centralnego Biura Śledczego Policji jest ponadto wydzielony wydział złożony z 15 dobrze wyszkolonych funkcjonariuszy, którzy odpowiedzialni są na szczeblu operacyjnym za wspomaganie dochodzeń swoją wiedzą fachową w dziedzinie informatyki śledczej oraz w dziedzinie dochodzeń i forensyki na podstawie danych bieżących.

- Ponieważ wstępne dochodzenia prowadzone są przez Policję, cała istniejąca struktura zwalczania cyberprzestępczości opiera się na zasobach technicznych Policji i na jej zasobach ludzkich. Ten fakt, w połączeniu z brakiem potencjału technicznego i odpowiedniego przeszkolenia sędziów i prokuratorów, zwraca uwagę na to, czy nadzór ze strony sędziów i prokuratorów nad dochodzeniami Policji jest skuteczny i stały. Dlatego też zdaniem oceniających potrzebni są wyspecjalizowani prokuratorzy na szczeblu regionalnym posiadający wiedzę o cyberprzestępczości, tak by mogli wspierać kolegów na szczeblu rejonowym w prowadzeniu lub nadzorowaniu postępowań przygotowawczych. Należy ponadto zorganizować szkolenie prokuratorów; kursy powinny być regularne i mieć charakter obowiązkowy.

- W zapobieganiu cyberprzestępczości i w jej zwalczaniu bierze udział szereg innych władz i organizacji. Wydaje się, że interakcja i współpraca między sektorem publicznym i prywatnym w Polsce jest skuteczna i produktywna. NASK i Bankowe Centrum Cyberbezpieczeństwa (utworzone przez Związek Banków Polskich) dostarczają dobrych przykładów współpracy między administracją publiczną a społeczeństwem obywatelskim.

- Z drugiej strony podczas wizyty na miejscu zauważono, że nie ma krajowego zespołu CERT pełniącego rolę centralnego punktu koordynacji, współpracy, wymiany informacji i rejestrowania dla potrzeb statystyki incydentów z zakresu cyberbezpieczeństwa. Główne zespoły CERT w Rzeczypospolitej Polskiej to: CERT.GOV.PL, które odpowiada za ICT rządu, oraz CERT POLSKA obsługiwane przez NASK i działające jako podmiot naukowy; POL-CERT działa na rzecz policji, MIL-CERT – wojska oraz podmiotów, takich jak Alior Bank, z CSIRT. Zdaniem oceniających, obecna struktura sprawia wrażenie, że potrzebne jest stworzenie jednego punktu kontaktowego. Wyznaczenie krajowego CERT mającego uprawnienia koordynacyjne wobec innych zespołów CERT mogłoby zwiększyć odporność polskiego systemu cyberbezpieczeństwa[18].

- Polskie władze administracyjne i rządowe traktują cyberbezpieczeństwo z należytą powagą. Jednak wspomniane, bardzo zdecentralizowane podejście (wspomnianą problematyką zajmuje się wiele różnych podmiotów, m.in. kilka ministerstw oraz Służba Kontrwywiadu Wojskowego, Narodowy Bank Polski czy NASK) może skutkować pewnym brakiem koordynacji. Dlatego zdaniem oceniających należy wzmocnić koordynację różnych organów zaangażowanych w zwalczanie cyberprzestępczości. Byłoby zatem bardzo wskazane wyznaczenie jednego organu mającego uprawnienia do wydawania poleceń władzom odpowiedzialnym za cyberbezpieczeństwo i ich wykonywanie.

[18] Po wizycie na miejscu poinformowano zespół oceniający, że NC Cyber i jego część CERT POLSKA pełnią rolę krajowego CERT – centralnego punktu koordynacji, współpracy, wymiany informacji i rejestrowania dla potrzeb statystyki. Oczekuje się, że w obecnie przygotowywanej nowej ustawie o cyberbezpieczeństwie NC Cyber zostanie wyznaczone jako krajowy CERT.

- Z drugiej strony roczne sprawozdania przygotowywane przez NASK i Agencję Bezpieczeństwa Wewnętrznego (CERT.GOV.PL) wyraźnie opisują sytuację Polski pod względem cyberbezpieczeństwa. Opisują one ogólną sytuację w Polsce w odniesieniu do administracji publicznej i sektora prywatnego, a także incydenty dotyczące obywateli. Zdaniem oceniających, warto mierzyć postępy cyberprzestępczości w oparciu o zróżnicowane zasoby wykorzystywane przez organy rządowe i pozarządowe, tak jak corocznie robi się to w Polsce.

5 ASPEKTY PRAWNE

5.1 Prawo karne materialne dotyczące cyberprzestępczości

5.1.1 Konwencja Rady Europy o cyberprzestępczości 47

Konwencja Rady Europy o cyberprzestępczości, która weszła w życie 1 czerwca 2015 r.

5.1.2 Opis krajowego ustawodawstwa

A. Decyzja ramowa Rady 2005/222/WSiSW dotycząca ataków na systemy informatyczne oraz dyrektywa 2013/40/UE w sprawie ataków na systemy informatyczne

Polska dokonała transpozycji decyzji ramowej Rady 2005/222/WSiSW dotyczącej ataków na systemy informatyczne oraz dyrektywy 2013/40/UE w sprawie ataków na systemy informatyczne. Polskie władze powiadomiły, że ponieważ wszystkie wymogi tej dyrektywy są spełnione przez obowiązujące przepisy prawa polskiego, jej transpozycja nie przysporzyła trudności.

W polskim prawie istnieje obszerne ustawodawstwo dotyczące cyberprzestępczości[19]. Zgonie z polskim kodeksem karnym (kk) kryminalizacji podlegają następujące czyny: nielegalny dostęp do systemów informatycznych (art. 267), niezgodna z prawem ingerencja w system (art. 269a), niezgodna z prawem ingerencja w dane (art. 268a), nielegalne przechwytywanie danych komputerowych (art. 267), niewłaściwe użycie urządzeń (art. 269b), fałszerstwo komputerowe (art. 270 i 271), oszustwo (art. 287), przestępstwo komputerowe dotyczące tożsamości (mieści się w definicji fałszerstwa lub oszustwa), wysyłanie lub kontrolowanie wysyłania spamu (czyn popełniany w stosunku do usług dostarczanych poprzez ICT). W kk nie ma definicji cyberprzestępstwa.

[19] W sprawozdaniu nie zawarto jego opisu ze względu na dużą liczbę odnośnych stron. Więcej informacji znajduje się w załączniku D.

Kk nie zawiera żadnego katalogu okoliczności obciążających lub łagodzących wpływających na decyzję sądu. Niektóre przepisy kk wskazują jednak okoliczności, które musi uwzględnić sąd, oceniając społeczne szkody spowodowane przez popełnione przestępstwo, podejmując decyzję dotyczącą winy sprawcy i nakładając karę. Trzeba również odnotować, że przepisy ogólne określone w art. 53 kk (wytyczne odnośnie do nakładania kar) mają zastosowanie do wszystkich przestępstw.

Prawo stanowi, że karalna jest również próba popełnienia tych przestępstw. Na mocy prawa polskiego kryminalizacji podlegają również podżeganie oraz pomocnictwo.

Stopień społecznej szkody związanej z danym przestępstwem zależy między innymi od skutków i od sposobu, w jaki zostało ono popełnione. Mniej szkodliwy charakter przestępstwa będzie pociągał za sobą łagodniejszy wyrok.

Podmioty prawne mogą zostać pociągnięte do odpowiedzialności za przestępstwa określone w dyrektywie 2011/93/UE Parlamentu Europejskiego i Rady w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej oraz w dyrektywie 2013/40/UE w sprawie ataków na systemy informatyczne, a także w Konwencji o cyberprzestępczości. Uregulowania dotyczące tej odpowiedzialności zawarte są w Ustawie z 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary. W ustawie tej ustanawia się przepisy o odpowiedzialności podmiotów zbiorowych za przestępstwa i określa się katalog tych przestępstw (obejmuje on wszystkie z przestępstw, o których mowa w konwencji budapeszteńskiej) oraz sankcje nakładane na podmioty prawne.

Zgodnie z art. 7 i 9 wyżej wymienionej ustawy wobec podmiotu zbiorowego sąd może orzec karę pieniężną w wysokości od 1000 do 5 000 000 PLN (EUR 250 – 1 250 000), do wysokości 3% dochodu w roku obrotowym, w którym popełniono dane przestępstwo skutkujące odpowiedzialnością danego podmiotu zbiorowego i zastosowaniem innych środków wyraźnie wymienionych w ustawie.

Przestępstwa i wykroczenia dotyczące cyberprzestępczości (lub wykorzystania ICT) zdefiniowane są w różnych aktach prawnych. Najważniejsze z nich to:

- w odniesieniu do danych osobowych: *Ustawa o ochronie danych osobowych*, która zawiera definicje szeregu przestępstw związanych z gromadzeniem i przetwarzaniem danych osobowych, w tym ewentualne sankcje w przypadku braku właściwych środków bezpieczeństwa (niedbałego zarządzania danymi osobowymi),
- w odniesieniu do spamu: Ustawa o świadczeniu usług drogą elektroniczną, która w art. 24 ust. 1 przewiduje karę grzywny w przypadkach przesyłania za pomocą środków komunikacji elektronicznej niezamówionych informacji handlowych.

B. Dyrektywa 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej

Polska dokonała pełnej transpozycji do prawa krajowego dyrektywy 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej oraz ratyfikowała Konwencję Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych (tzw. Konwencję z Lanzarote). W Polsce istnieje obszerne ustawodawstwo dotyczące, między innymi, komputerowego wytwarzania, rozpowszechniania lub posiadania pornografii dziecięcej (art. 202) i komputerowego nagabywania dzieci w celach seksualnych[20].

C. Oszustwa internetowe z wykorzystaniem kart płatniczych

Prawo polskie zawiera środki przeciwdziałania oszukańczym operacjom finansowym z wykorzystaniem internetu. Zachowanie opisane jako „komputerowe oszustwo lub fałszerstwo" mieści się w definicji fałszerstwa określonej w art. 270 ust. 1 kk (fałszerstwo materialne) oraz w art. 271 ust. 1 (fałszerstwo intelektualne).

[20] W sprawozdaniu nie zawarto jego opisu ze względu na dużą liczbę odnośnych stron. Więcej informacji znajduje się w załączniku D.

Art. 270 § 1 przewiduje, że kto, w celu użycia za autentyczny, podrabia lub przerabia dokument lub takiego dokumentu jako autentycznego używa, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności od trzech miesięcy do lat pięciu.

Art. 271 § 1 stanowi, że funkcjonariusz publiczny lub inna osoba uprawniona do wystawienia dokumentu, która poświadcza w nim nieprawdę co do okoliczności mającej znaczenie prawne, podlega karze pozbawienia wolności od trzech miesięcy do lat pięciu.

Przestępstwa te mogą jedynie zostać popełnione celowo (na mocy art. 270 ust. 1 kk wymagana jest bezpośrednia intencja – cel wykorzystania sfałszowanego dokumentu, tak jakby był on autentyczny). Karalna jest również próba popełnienia wyżej wymienionych przestępstw. Termin „dokument" (używany w art. 270 i 271 kodeksu) został zdefiniowany w art. 115 § 14 jako każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne.

Art. 287 § 1 kk przewiduje, że kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od trzech miesięcy do lat pięciu. Przestępstwo to może jedynie zostać popełnione celowo (bezpośrednia intencja – wymagany jest cel uzyskania korzyści materialnych). Zachowania opisane jako „przestępstwa komputerowe dotyczące tożsamości" mieszczą się w definicji fałszerstwa lub oszustwa.

5.2 Kwestie proceduralne

5.2.1 Techniki śledcze

Szukanie i gromadzenie danych z systemu informacyjnego/komputera

W przypadku przestępstwa związanego z urządzeniami elektronicznymi i z elektronicznymi nośnikami danych można przeprowadzić dochodzenie w celu zdobycia danych w formie elektronicznej, jeśli są uzasadnione przesłanki pozwalające przypuszczać, że zostało popełnione przestępstwo i jeżeli istnieje prawdopodobieństwo, że dane urządzenie elektroniczne zawiera dane elektroniczne, na podstawie których można zidentyfikować, wykryć lub aresztować podejrzanego lub oskarżonego lub wykryć istotne dla danego postępowania karnego ślady przestępstwa lub ślady, które mogą być wykorzystane jako dowód w tym postępowaniu.

Szukania, gromadzenia i zabezpieczenia danych elektronicznych dokonuje się na podstawie ogólnych przepisów Kodeksu postępowania karnego (kpk) w odniesieniu do gromadzenia i zabezpieczenia dowodów.

Przechwytywanie/gromadzenie danych o ruchu/treści w czasie rzeczywistym

Możliwe jest przechwytywanie /gromadzenie w czasie rzeczywistym treści komunikacji (niezależnie czy ma ona postać rozmowy telefonicznej, wiadomości e-mail, sms-a lub inną formę); uważa się je jednak za specjalną technikę śledczą i dlatego konieczny jest nakaz sądowy. Policja może podejmować takie działanie jedynie w pilnych przypadkach (gdy istnieje zagrożenie utraty dowodów) i musi równocześnie zwrócić się do sądu o wydanie zezwolenia. Dowody zebrane bez takiego zezwolenia nie mogą być wykorzystane w postępowaniach karnych i muszą zostać zniszczone.

Wyżej wymienione ograniczenia nie mają zastosowania do działań związanych z danymi o ruchu. Na mocy art. 218 kpk prokurator lub sąd mają prawo do uzyskiwania danych o ruchu od przedsiębiorstw telekomunikacyjnych i transportowych. Obejmuje to tak zwane billingi (wykazy połączeń, ich czas i długość trwania), jak również informacje na temat umiejscowienia danego urządzenia telekomunikacyjnego.

Zabezpieczanie danych komputerowych

Podczas postępowania karnego dane zabezpieczone w trakcie dochodzenia są trzymane aż do czasu, gdy zakończy się dane postępowanie sądowe. Dane te mogą być przechowywane na oryginalnych nośnikach (dyskach komputerowych) lub (co jest najbardziej rozpowszechnione) można sporządzić cyfrową/forensyczną kopię tych danych.

Nakaz dotyczący przechowywania danych o ruchu/treści

Zgodnie z art. 218a kpk prokurator lub sąd mogą zarządzić, by dostawca usług telekomunikacyjnych przechował (zabezpieczył) wszelkie dane dotyczące dostarczonych usług, w tym dane dotyczące treści. Okres zabezpieczenia nie może jednak przekroczyć 90 dni.

Postępowania przygotowawcze związane z cyberprzestępczością prowadzone są zgodnie z taką samą procedurą, jak w odniesieniu do innych przestępstw. Zgodnie z art. 236a kpk przepisy dotyczące zatrzymania i przeszukania stosuje się odpowiednio do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną.

Ze względu na dynamiczny rozwój metod, technik i narzędzi popełniania cyberprzestępstw trudno jest stworzyć katalog dobrych praktyk w dziedzinie technik śledczych. Wszystkie działania przeprowadzane przez funkcjonariuszy Policji opierają się na ich własnym doświadczeniu i wymianie informacji. Innym źródłem informacji jest szkolenie organizowane dla funkcjonariuszy Wydziału do walki z Cyberprzestępczością np. przez Wyższą Szkołę Policji w Szczytnie. Na kursie tym kładzie się nacisk na szkolenie funkcjonariuszy w zakresie sposobów uzyskiwania informacji z internetu, tak by umożliwić im zwalczanie przestępstw komputerowych. Istnieje również specjalistyczny kurs dla funkcjonariuszy wykonujących zadania związane ze zwalczaniem cyberprzestępczości. Innym źródłem dobrych praktyk jest szkolenie w dziedzinie informatyki śledczej oferowane przez firmy zajmujące się dystrybucją wyspecjalizowanego sprzętu do ochrony, pozyskiwania i analizy danych. Również w ramach europejskiego programu wymiany policyjnej zorganizowanego przez Agencję Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (CEPOL)

funkcjonariusze mają możliwość wzbogacania i wymiany swoich doświadczeń z zakresu metod, technik i narzędzi potrzebnych do skutecznego zwalczania cyberprzestępczości. Spotkania punktów kontaktowych w ramach EC3 dają możliwość omawiania wspólnych kwestii i usprawniają wymianę informacji. W ramach współdziałania z sektorami publicznym i prywatnym na polu wymiany informacji funkcjonariusze policji zdobywają ponadto doświadczenie i wiedzę odnośnie do nowych technik wykorzystywanych przez sprawców przestępstw komputerowych.

Wydział do walki z Cyberprzestępczością wydał oprócz tego broszurę skierowaną do policyjnych jednostek zwalczania cyberprzestępczości, zawierającą informacje na temat dobrych praktyk w zakresie właściwego zabezpieczania dowodów elektronicznych.

Prokurator Generalny przygotował metodologię ścigania przestępstw z nienawiści, pedofilii i pornografii dziecięcej, obejmującą również aspekt cyberprzestępczości.

5.2.2 Forensyka i szyfrowanie

Kpk nie obejmuje pojęć, takich jak „ekspertyza elektroniczna lub zdalna". Jednak art. 193 ust. 1 kpk stanowi: „Jeżeli stwierdzenie okoliczności mających istotne znaczenie dla rozstrzygnięcia sprawy wymaga wiadomości specjalnych, zasięga się opinii biegłego albo biegłych".

Wojsko

Ministerstwo Obrony Narodowej uważa, że łączność za pośrednictwem sieci szyfrowanej (jak również monitorowanie takiej łączności) i zaszyfrowane urządzenia stanowią problem. Oświadczyło, że jeśli chodzi o łączność za pośrednictwem sieci szyfrowanej, potrzebne są serwery proxy, które potrafią deszyfrować i ponownie szyfrować ruch w sieci, aby poddawać go analizie i wykrywać możliwe zagrożenia (to podejście wymaga odpowiednich uregulowań prawnych i mocnego uzasadnienia).

Ministerstwo Obrony Narodowej twierdzi, że nie ma istotnych problemów, jeśli chodzi o współpracę w tej dziedzinie. W 2013 r. powołano Narodowe Centrum Kryptologii. Deszyfracji nie prowadzi się we współpracy z firmami prywatnymi. Podkreślono ponadto, że informatyka śledcza w zakresie zaszyfrowanych urządzeń jest dziedziną, w której nie było dotychczas możliwe skuteczne sprostanie czoła problemowi szyfrowania. Udało się wdrożyć filtrowanie ruchu i zwiększyć świadomość użytkowników w odniesieniu do internetu.

Policja

Do zadań Centralnego Laboratorium Kryminalistycznego Policji należy analizowanie zaszyfrowanych urządzeń cyfrowych w formie dysków twardych i woluminów odzyskanych z pamięci zarekwirowanych urządzeń cyfrowych. Podczas tych analiz eksperci komputerowi próbują złamać ochronę kryptograficzną, wykorzystując specjalne oprogramowanie działające na klastrze złożonym z komputerów dostępnych w jednostce IT Centralnego Laboratorium Kryminalistycznego. Obecnie największy problem w kryptografii dotyczy ograniczonej możliwości (zbyt mała moc przetwarzania) łamania ochrony kryptograficznej w przypadkach, gdy sprawcy korzystają z długich i skomplikowanych haseł.

5.2.3 Dowody elektroniczne

W różnych przepisach polskiego prawa kryminalnego, w tym w definicjach przestępstw kryminalnych, używane są terminy, takie jak: dane komputerowe, system informacyjny, system komputerowy, sieć. Nie ma jednak definicji prawnych wyżej wymienionych terminów ani definicji dowodu elektronicznego. Wynika to z tradycji definiowania w prawie jedynie terminów mających znaczenie inne niż w języku naturalnym.

Chociaż obecnie w polskim prawie nie ma definicji prawnej dowodu elektronicznego, praktycy rozumieją go jako informacje gromadzone na nośnikach elektronicznych. Tak zdefiniowany dowód elektroniczny jest dopuszczalny w procesie karnym i podlega opinii danego sądu jak jakikolwiek inny dowód, np. odnośnie do zasady swobodnej oceny dowodów. Procedura z wykorzystaniem dowodu elektronicznego jest taka sama jak w przypadku innych dowodów kryminalistycznych.

Jako zasada ogólna, art. 7 kodeksu postępowania karnego stanowi, że organy postępowania (prokuratorzy, sądy) kształtują swe przekonanie na podstawie wszystkich przeprowadzonych dowodów, ocenianych swobodnie z uwzględnieniem zasad prawidłowego rozumowania oraz wskazań wiedzy i doświadczenia życiowego (zasada swobodnej oceny dowodów). Art. 168a kpk stanowi ponadto, że niedopuszczalne jest przeprowadzenie i wykorzystanie dowodu uzyskanego do celów postępowania karnego za pomocą czynu zabronionego.

Wspomniane zasady mają także zastosowanie do dowodu elektronicznego (nie ma zasad dopuszczalności, które miałyby zastosowanie w szczególności w odniesieniu do tego rodzaju dowodu), tak jak mają zastosowanie do dowodów zebranych poza Polską (środkami pomocy prawnej).

Prawo polskie ma bardzo szerokie i elastyczne podejście do dowodów zebranych poza Polską. Art. 587 kpk stanowi, że takie dowody (protokoły oględzin, przesłuchań osób w charakterze oskarżonych, świadków, biegłych na wniosek polskiego sądu lub prokuratora lub protokoły innych czynności dowodowych, dokonanych przez sądy lub prokuratorów państw obcych albo organy działające pod ich nadzorem) mogą być odczytywane (wykorzystywane) na rozprawie. Dowody takie należy oddalić, jeśli sposób przeprowadzenia czynności (uzyskanie dowodów) jest sprzeczny z zasadami porządku prawnego w Polsce. Jednak zgodnie z orzecznictwem polskiego Sądu Najwyższego sam fakt, że gwarancje proceduralne (mające zastosowanie do zbierania niektórych rodzajów dowodów elektronicznych) w Polsce są bardziej rygorystyczne sam w sobie nie prowadzi do oddalenia takich dowodów.

Centralne Laboratorium Kryminalistyczne Policji, którego obowiązki obejmują badanie sprzętu komputerowego i analizę danych zachowanych na różnych urządzeniach cyfrowych (takich jak dyski twarde, pamięci Flash USB DVD itd.). Eksperci z zakresu informatyki śledczej odzyskują/ujawniają jedynie te dane, które wskazano we wniosku o zbadanie.

5.3 Ochrona praw człowieka/podstawowych wolności

Prawa podstawowe i podstawowe wolności są chronione przez polski porządek prawny zarówno w odniesieniu do sfery offline, jak i online. Są one określone w następujących aktach prawnych:

a) Konstytucja Rzeczypospolitej Polskiej, która gwarantuje prawo do prywatności, ochronę danych osobowych, wolność wyrażania poglądów, a także prawo wszystkich obywateli do pozyskiwania i rozpowszechniania informacji. Polska konstytucja zawiera również gwarancje regulujące przestrzeganie praw i wolności obywatelskich podczas prowadzenia postępowań karnych, w tym w dziedzinie cyberprzestępczości.

b) Ustawa o ochronie danych osobowych z 1997 r.[21], która zawiera dość rygorystyczne uregulowania wskazujące kiedy i w jaki sposób można przetwarzać dane osobowe. Art. 8 ustawy przewiduje powołanie Generalnego Inspektora Ochrony Danych Osobowych, do którego zadań należy, między innymi, wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych oraz prowadzenie rejestru zbiorów danych. Generalny Inspektor opiniuje również projekty ustaw i rozporządzeń dotyczących ochrony danych osobowych.

c) Prawo telekomunikacyjne, które zajmuje się ochroną prywatności w kontekście cyberprzestępczości, wraz z aktami prawnymi regulującymi działania związane ze świadczeniem poszczególnych usług. Określają one, które organy mogą mieć dostęp do danych osobowych abonentów przetwarzanych przez dostawców usług telekomunikacyjnych i w jaki sposób uzyskać taki dostęp.

[21] Dziennik Urzędowy z 2014 r., nr 1182, z późniejszymi zmianami.

d) Ustawa z 2002 r. o świadczeniu usług drogą elektroniczną[22], która powstała w następstwie dyrektywy 2000/31/WE i wprowadziła ochronę tzw. pośredników internetowych przed odpowiedzialnością prawną za treść generowaną, wymienianą i umieszczaną w internecie przez użytkowników. Wyłączenia odpowiedzialności umożliwiają dostarczanie takich usług elektronicznych, które pozwalają użytkownikom swobodnie wyrażać w internecie swoje myśli i opinie; jednocześnie procedura zgłaszania i usuwania treści umożliwia skuteczne usuwanie treści naruszających prawo ogólne, ponieważ odnosi się do internetu.

Wszystkie podmioty sektora publicznego (takie jak Policja, prokuratorzy i sędziowie) muszą ponadto działać w oparciu o prawo i w jego granicach. Dlatego też wszelkie działania ze strony organów publicznych, które mogą kolidować z gwarantowanymi konstytucyjnie prawami i swobodami wymagają wyraźnej podstawy prawnej zawartej w ustawie sejmowej.

Prawo do prywatności, ochrona danych osobowych i wolność słowa są uważane za prawa i swobody konstytucyjne. Dlatego też można nałożyć na nie ograniczenia jedynie, jeśli jest to konieczne: te ograniczenia nie mogą naruszać ich istoty i muszą mieć formę ustawy sejmowej.
Uznaje się, że właściwe jest powierzyć zapobieganie przestępstwom i prowadzenie śledztw, a także ściganie sprawców, pewnym państwowym służbom dysponującym specjalnymi uprawnieniami/technikami śledczymi. Przesłankami korzystania z takich technik są waga danego przestępstwa oraz konieczność działania (gdy nie istnieją inne, mniej inwazyjne środki). Korzystanie ze specjalnych technik śledczych pozostaje pod nadzorem sądów.

[22] Dziennik Urzędowy z 2013 r. nr 1422, tekst skonsolidowany.

Ustawa o Policji określa podstawowe zadania Policji, które obejmują:

- ochronę życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami;
- zapobieganie popełnianiu przestępstw i współdziałanie w tym zakresie z organami państwowymi, samorządowymi i organizacjami społecznymi;
- wykrywanie przestępstw i ściganie ich sprawców;
- gromadzenie, przetwarzanie i przekazywanie informacji kryminalnych;

Do celów realizacji swoich zadań statutowych Policja jest uprawniona, między innymi, do:

- korzystania z danych osobowych, w tym również w formie zapisu elektronicznego, uzyskanych przez inne organy, służby i instytucje państwowe w wyniku wykonywania czynności operacyjno-rozpoznawczych oraz ich przetwarzania w rozumieniu ustawy o ochronie danych osobowych, bez wiedzy i zgody osoby, której dane te dotyczą;
- przeszukiwania osób i pomieszczeń w trybie i przypadkach określonych w przepisach kpk i innych ustaw; dokonywania kontroli osobistej, przeglądania zawartości bagaży i sprawdzania ładunku w portach i na dworcach oraz w środkach transportu lądowego, powietrznego i wodnego, w przypadku istnienia uzasadnionego podejrzenia popełnienia czynu zabronionego pod groźbą kary;
- obserwowania i rejestrowania obrazu zdarzeń w miejscach publicznych oraz (działając w ramach czynności operacyjnych i administracyjnych) dźwięku towarzyszącego tym zdarzeniom.

W pewnych przypadkach (poważne przestępstwa, w tym cybersabotaż), jeśli inne środki okazały się nieskuteczne lub nieodpowiednie, Policja może korzystać ze specjalnych czynności w ramach postępowania przygotowawczego, w tym z kontroli operacyjnej i z przechwytywania komunikacji. Korzystanie z tych technik wymaga postanowienia sądu okręgowego wydanego na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, albo na pisemny wniosek komendanta wojewódzkiego Policji, złożony po uzyskaniu pisemnej zgody prokuratora okręgowego. W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować utratę dowodów, postanowienie sądu może zostać wydane ex post, lecz nie później niż 5 dni od dnia rozpoczęcia kontroli operacyjnej lub przechwytywania komunikacji.

Prawo o prokuraturze i kpk określają kompetencje i obowiązki prokuratury, w tym nadzór postępowań przygotowawczych w sprawach karnych oraz legalność wszczynania i przeprowadzania czynności operacyjnych przez organy ścigania w granicach przewidzianych w przepisach regulujących organizację tych organów i zakres ich działań. Należy zauważyć, że każdy wniosek o wykorzystanie kontroli operacyjnej i przechwytywanie komunikacji wymaga zgody odnośnego prokuratora.

5.4 Jurysdykcja

5.4.1 Zasady mające zastosowanie do dochodzeń z zakresu cyberprzestępczości

Przepisy w zakresie jurysdykcji w sprawach karnych zawarte są w art. 5 i w art. 109–113 kk. Przepisy te mają zastosowanie do przestępstw zdefiniowanych w samym kk, a także do wszelkich innych przestępstw zdefiniowanych w polskim prawie. Polska jurysdykcja w sprawach karnych ma zastosowanie do każdego sprawcy (niezależnie od jego obywatelstwa), który popełnił czyn zabroniony na terytorium Polski, jak również na polskim statku wodnym lub powietrznym, chyba że umowa międzynarodowa, której Polska jest stroną, stanowi inaczej (art. 5 kk).
Zgodnie z art. 111 kk jurysdykcja w odniesieniu do przestępstw popełnionych poza terytorium Polski podlega warunkowi podwójnej odpowiedzialności karnej. Jednak to ograniczenie nie ma zastosowania do przestępstw:

- wymienionych w art. 112 kk (przestępstwa przeciwko: bezpieczeństwu wewnętrznemu lub zewnętrznemu Polski; polskim urzędom lub funkcjonariuszom publicznym, polskim interesom gospodarczym, przestępstwa złożenia fałszywego oświadczenia wobec urzędu polskiego lub przestępstwa, z którego została osiągnięta, chociażby pośrednio, korzyść majątkowa w Polsce);
- określonych w umowach międzynarodowych, których stroną jest Polska.

Ponieważ Polska jest stroną Konwencji o cyberprzestępczości, dodatkowego protokołu do tej konwencji i Konwencji z Lanzarote, wymóg podwójnej odpowiedzialności karnej nie ma zastosowania do przestępstw, które są w nich zdefiniowane i które odpowiadają przestępstwom określonym w ustawodawstwie UE dotyczącym cyberprzestępczości.

5.4.2 Przepisy w przypadku konfliktów jurysdykcji i przekazywanie spraw Eurojustowi

Polskie władze nie miały do czynienia ze sprawami, w których występowałyby konflikty jurysdykcji. Jednak w szeregu spraw zidentyfikowano obywateli innych krajów jako sprawców czynów z zakresu cyberprzestępczości.

Polskie prawo materialne i prawo procesowe zawierają przepisy dotyczące osobistego i terytorialnego stosowania polskiego prawa karnego i instrumentów prawnych do współpracy międzynarodowej, w tym przekazywania ścigania, ekstradycji i wydawania; są one w pełni zgodne z mającymi zastosowanie uregulowaniami europejskimi, w szczególności z decyzją ramową Rady 2009/948/WSiSW z dnia 30 listopada 2009 r. w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów. Dlatego też ewentualne konflikty jurysdykcji mogłyby być rozwiązywane zgodnie z ustawodawstwem krajowym i z prawami organów innych państw członkowskich.

5.4.3 Jurysdykcja w odniesieniu do aktów cyberprzestępczości popełnionych w „chmurze”

Polskie władze nie doświadczyły dotąd problemów dotyczących sposobu gromadzenia danych określanego terminem „przetwarzanie w chmurze”. Jednak zdaniem polskich władz zjawisko to może w przyszłości prowadzić do poważnych problemów w miarę upowszechniania się tego typu rozwiązań, czego skutkiem może być gromadzenie poza jurysdykcją Polski i innych państw członkowskich UE większej ilości danych istotnych w dochodzeniach dotyczących przestępstw.

Należy wspomnieć, że procedury wykorzystywane do zdobywania takich danych są w większości długie i nieskuteczne, jedną z przyczyn jest to, że główni dostarczyciele zlokalizowani są poza UE.

5.4.4 Postrzeganie przez Polskę ram prawnych zwalczania cyberprzestępczości

Po podpisaniu przez Polskę Konwencji o cyberprzestępczości, dodatkowego protokołu do tej konwencji i Konwencji z Lanzarote, Polska zharmonizowała ustawodawstwo krajowe zarówno w odniesieniu do głównych aspektów cyberprzestępczości, jak też przestępstw najczęściej popełnianych z wykorzystaniem ICT. Jednak ustawodawstwa krajowe państw członkowskich UE wciąż są zróżnicowane, tak jak państw spoza Unii.

Zdaniem polskich władz skuteczne dochodzenia w dziedzinie cyberprzestępczości oraz identyfikacja sprawców zależą od dostępności danych będących w gestii operatorów telefonii komórkowej i dostawców usług internetowych (w szczególności danych dotyczących ruchu i dotyczących abonentów). Potrzebne jest europejskie prawodawstwo bardziej szczegółowo określające, które dane zdefiniowane są jako dane dotyczące ruchu, użytkownika oraz dane osobowe (adres IP, nazwa użytkownika, hasło itd.). Jest również miejsce na pewne uregulowania w odniesieniu do współpracy z państwami trzecimi, ze szczególnym naciskiem na państwa, w których mają swoją siedzibę najważniejsze firmy ICT.

5.5 Wnioski

- Polska jest stroną Konwencji Rady Europy o cyberprzestępczości, która weszła w życie 1 lipca 2015 r. Decyzja ramowa Rady 2005/222/WSiSW dotycząca ataków na systemy informatyczne oraz dyrektywa 2013/40/UE w sprawie ataków na systemy informatyczne zostały również przetransponowane do polskiego prawa.

- W pełni wdrożono dyrektywę 2011/93/UE Parlamentu Europejskiego i Rady w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej.

- W polskim kk określone są ogólne zasady dotyczące warunków wstępnych karania oraz elementów czynu przestępczego (zamiar, lekkomyślność, usiłowanie, itd.), jak też odpowiedzialności (w tym podżeganie i pomocnictwo); mają one zastosowanie do cyberprzestępczości. Jednak, tak jak w innych państwach członkowskich, Polska nie ma jednolitej definicji cyberprzestępczości. Zdaniem oceniających ten brak jednolitej definicji może prowadzić do nieprecyzyjnego rejestrowania do celów statystyki i nieprecyzyjnego przedstawiania cyberprzestępczości.

- Podmioty prawne mogą zostać pociągnięte do odpowiedzialności za wszystkie przestępstwa związane z postanowieniami konwencji budapeszteńskiej i za przestępstwa określone w dyrektywie 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej i w dyrektywie 2013/40/UE w sprawie ataków na systemy informatyczne.

- Jeżeli chodzi o techniki śledcze, jest szereg możliwości sprawiających wrażenie skutecznych z punktu widzenia zwalczania cyberprzestępczości, takich jak operacje specjalne, monitorowanie i zakładanie podsłuchów. Z proceduralnego punktu widzenia polskie prawo zezwala na najbardziej istotne techniki śledcze i środki dochodzeniowe właściwe dla tego obszaru przestępczości. W polskim prawie nie jest jednak przewidziane zdalne przeszukanie i zajęcie, np. przeprowadzanie przez organ ścigania włamania online do systemu komputerowego podejrzanego komputera zamiast jego fizycznego pozyskania. Zdaniem oceniających można by rozważyć przepisy zezwalające na taką operację, bez uszczerbku dla praw podejrzanego.

- Wyrok Europejskiego Trybunału Sprawiedliwości stwierdzający nieważność dyrektywy o zatrzymywaniu danych (dyrektywa 2006/24/WE) miał wpływ na niektóre przepisy prawa telekomunikacyjnego, które musiały zostać zmienione. Prokurator lub sędzia może zarządzić, by dostawcy usług telekomunikacyjnych zabezpieczyli dane dotyczące dostarczonych usług, w tym dane dotyczące treści. Okres zabezpieczenia nie może jednak przekroczyć 90 dni.

- Nie ma specjalnych przepisów dotyczących dopuszczalności i oceny dowodu elektronicznego. Dowód elektroniczny, jak większość tradycyjnych dowodów, jest dopuszczalny w sądzie i jest oceniany przez danego sędziego zgodnie z zasadą swobodnej oceny dowodów. Nie wymieniono żadnych trudności ani problemów odnośnie do dowodów elektronicznych uzyskiwanych za granicą.

- Polskie władze powiadomiły o trudnościach z zaszyfrowanymi komunikatami, z zaszyfrowanymi urządzeniami do przechowywania danych oraz z hostingiem w chmurze. W ramach Centralnego Biura Śledczego jest jednak wydzielone laboratorium kryminalistyczne, zdolne do przeprowadzania zaawansowanej deszyfracji. Hosting w chmurze i przechowywanie w chmurze to głównie zagadnienie prawne odnoszące się do jurysdykcji i własności.

- Centralne Laboratorium Kryminalistyczne Policji dysponuje ponadto szerokim spektrum materiałowym zaawansowanych narzędzi i rozwiązań, w tym do bezpiecznej ekstrakcji danych ze zniszczonych nośników elektronicznych oraz sprzętem do łamania haseł w zaszyfrowanych plikach lub urządzeniach. Zdaniem oceniających Centralne Laboratorium Kryminalistyczne Policji mogłoby dzielić się wiedzą fachową z innymi biurami terenowymi na terytorium kraju; polepszyłoby to umiejętności funkcjonariuszy i zagwarantowało pierwszą reakcję w sytuacjach kryzysowych lub gdy w pilnych przypadkach lub śledztwach wymagana jest szybka analiza.

- Główną zasadą ustalania polskiej jurysdykcji w odniesieniu do przestępstw jest zasada terytorialności. Do przestępstw popełnionych w Polsce (oraz na polskim statku wodnym lub powietrznym) zastosowanie ma polskie prawo. Jurysdykcja w odniesieniu do przestępstw popełnionych poza terytorium Polski podlega warunkowi podwójnej odpowiedzialności karnej, chyba że chodzi o żywotne interesy kraju lub wynika to ze zobowiązań określonych w instrumentach międzynarodowych. Ponieważ Polska jest stroną Konwencji Rady Europy o cyberprzestępczości, dodatkowego protokołu do tej konwencji i Konwencji z Lanzarote o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych, wymóg podwójnej odpowiedzialności karnej nie ma zastosowania do przestępstw w tych obszarach.

- Zdaniem oceniających konflikty jurysdykcji to bardzo istotny problem w najbardziej zaawansowanych sprawach z zakresu cyberprzestępczości. Wydaje się, że Polska pragmatycznie podchodzi do stawiania czoła tym problemom. W tym przypadku do rozwiązywania problemu należałoby wykorzystać Eurojust. Władze polskie nie miały dotąd do czynienia ze sprawami obejmującymi konflikty jurysdykcji w odniesieniu do cyberprzestępstw, przykładowo, gdy co najmniej dwa państwa członkowskie mogą prowadzić dochodzenie i ścigać tego samego sprawcę za cyberprzestępstwa popełnione poza ich terytorium lub gdy chodzi o czyny przestępcze popełnione w chmurze.

6 ASPEKTY OPERACYJNE

6.1 Ataki cybernetyczne

6.1.1 Charakter ataków cybernetycznych

W 2014 r. Agencja Bezpieczeństwa Wewnętrznego odnotowała 7 498 incydentów. Najczęściej występowały następujące kategorie incydentów: botnet (4 681 incydentów), nieprawidłowa konfiguracja urządzenia (2 213), skanowanie (132), inżynieria społeczna (119), błędy aplikacji sieciowych (101). Raporty na temat zagrożeń dla bezpieczeństwa cybernetycznego i incydentów cybernetycznych w polskiej domenie internetowej są przygotowywane przez CERT POLSKA[23].

6.1.2 Mechanizmy reagowania na ataki cybernetyczne

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej przewiduje trzypoziomowy Krajowy System Reagowania na Incydenty Komputerowe w cyberprzestrzeni:

1) Poziom I – poziom koordynacji – minister właściwy ds. informatyzacji;
2) Poziom II – reagowania na incydenty komputerowe;
a) Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL;
b) Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych realizujące zadania w sferze militarnej;
3) Poziom III – poziom realizacji – administratorzy odpowiadający za poszczególne systemy teleinformatyczne funkcjonujące w cyberprzestrzeni.

Zadania operacyjne w ramach ochrony cyberprzestrzeni są również wykonywane przez zespoły publiczne i prywatne powoływane przez operatorów telekomunikacyjnych i środowiska naukowo-badawcze.

[23] http://www.cert.pl/PDF/Report_CP_2014.pdf

Głównym zadaniem Rządowego Zespołu Reagowania na Incydenty Komputerowe (CERT.GOV.PL) jest wykonywanie zadań operacyjnych związanych z bezpieczeństwem systemów informatycznych organów publicznych. Jego głównym zadaniem jest zapewnienie i rozwijanie zdolności jednostek administracji publicznej w zakresie ochrony przed zagrożeniami cybernetycznymi, w szczególności przed atakami wymierzonymi w infrastrukturę ICT. CERT.GOV.PL przede wszystkim zajmuje się incydentami cybernetycznymi w sektorze publicznym, a jego działania obejmują koordynację procesu reagowania na incydenty, rozwiązywanie i analizę incydentów oraz koordynację reagowania na naruszenia bezpieczeństwa. CERT.GOV.PL publikuje katalogi zagrożeń dla bezpieczeństwa i biuletyny bezpieczeństwa oraz roczne raporty o stanie bezpieczeństwa cyberprzestrzeni w organach publicznych.

Ogromną wagę przykłada się do zespołu CERT POLSKA działającego w ramach struktury NASK (Naukowej i Akademickiej Sieci Komputerowej):

– reagowanie na zagrożenia i incydenty w polskiej domenie internetowej (.pl);
– publikowanie sprawozdań rocznych na temat zagrożeń cybernetycznych;
– tworzenie narzędzi i systemów informatycznych w celu zwiększenia potencjału kraju w zakresie cyberbezpieczeństwa, np. systemu wczesnego ostrzegania, oraz platformy wymiany wiedzy i informacji znanej jako ARAKIS;
– Platforma n6, system wymiany informacji NISHA;
– szkolenia specjalistyczne i organizacja konferencji SECURE.

Zgodnie z dokumentem *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* CERT.GOV.PL stanowi drugi poziom Krajowego Systemu Reagowania na incydenty komputerowe w polskiej cyberprzestrzeni. W przypadku incydentów o szerokich skutkach oddziaływania, zadaniem zespołu jest koordynacja i reagowanie na incydent oraz wymiana informacji pomiędzy instytucjami, których bezpośrednio dotyczy atak cybernetyczny. Ponadto zespół wykorzystuje doświadczenie zdobyte podczas poprzednich incydentów, przygotowuje ostrzeżenia zawierające informacje techniczne i zalecenia dotyczące dalszych działań oraz przekazuje je rządowym organom administracyjnym. Celem jest tutaj zapobieganie lub redukowanie możliwości przeprowadzenia podobnych ataków na inne instytucje.

CERT.GOV.PL jest odpowiedzialny za zajmowanie się incydentami, które dotyczą agencji rządowych. Zawarte są również porozumienia z operatorami IT dotyczące dobrowolnej sprawozdawczości. Dzięki temu zespół ma możliwość współpracy przy reagowaniu na incydenty występujące w sieciach danych danej instytucji. W przypadku incydentu, który wykracza poza zdolności zespołu, CERT.GOV.PL współpracuje z wszystkimi innymi polskimi zespołami reagowania na incydenty cybernetyczne, takimi jak CERT POLSKA lub MIL CERT.
W 2015 r. decyzją Komendanta Głównego Policji w ramach Komendy Głównej Policji powołano zespół reagujący na incydenty komputerowe (POL-CERT). Zespół wykonuje zadania związane z koordynacją reagowania na incydenty komputerowe w policyjnych systemach i sieciach teleinformatycznych. Z myślą o uproszczeniu przepływu informacji o wydarzeniach w wojewódzkich (regionalnych) komendach policji oraz w szkołach policyjnych ustanowiono punkty kontaktowe do spraw cybernetycznych. W przyszłości POL-CERT będzie stanowić element polskiego systemu reagowania na incydenty cybernetyczne w cyberprzestrzeni.

Operatorzy infrastruktury krytycznej uczestniczą w procesie redukowania ryzyka cyberataków i łagodzenia ich skutków poprzez ochronę zasobów swojej infrastruktury krytycznej i poprzez współpracę z administracją publiczną. Operatorzy ci w szczególności przygotowują i wdrażają plany ochrony tej infrastruktury. Ponadto projektują oni i wdrażają swoje własne systemy zabezpieczające wspierające tę infrastrukturę i zapewniające jej ciągłe funkcjonowanie. Wymogi i środki dotyczące zapewnienia bezpieczeństwa cybernetycznego i wymiany informacji są przedstawione w Narodowym Programie Ochrony Infrastruktury Krytycznej[24]. Przyjęte rozwiązania są poddawane przeglądowi podczas procesu konsultacji i zatwierdzania planów ochrony infrastruktury krytycznej. W ramach działań zespołu CERT. GOV.POL podpisano porozumienia z operatorami infrastruktury krytycznej zainteresowanymi współpracą z zespołem.

[24] http://rcb.gov.pl/?page_id=210

Ponadto, na mocy Ustawy o zarządzaniu kryzysowym z 2007 r., szef Agencji Bezpieczeństwa Wewnętrznego, w przypadku podjęcia informacji o możliwości wystąpienia sytuacji kryzysowej będącej skutkiem zdarzenia o charakterze terrorystycznym, zagrażającego infrastrukturze krytycznej, może udzielać zaleceń podmiotom zagrożonym tymi działaniami. Ustawa ma bezpośrednie skutki dla działalności CERT.GOV.PL.

Operatorzy infrastruktury krytycznej z sektora publicznego i prywatnego są zobowiązani, na mocy § 7 *Rozporządzenia Rady Ministrów w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej*[25] z 2007 r. i dokumentów dotyczących programu, dostarczać informacje na temat zagrożeń dla infrastruktury krytycznej i dla bezpieczeństwa państwa i obywateli mogących być skutkiem zakłócenia funkcjonowania tej infrastruktury. Istnieje obowiązek wymiany informacji na temat wszelkich okoliczności lub zdarzenia, które mogą mieć wpływ na bezpieczeństwo infrastruktury krytycznej, w tym na temat cyberataków. Procedura wymiany informacji z centrami zarządzania kryzysowego i innymi organami administracji publicznej na temat zagrożeń dla infrastruktury krytycznej jest jednym z wymogów dotyczących planów ochrony infrastruktury krytycznej – na mocy § 2 pkt 3 ust. *Rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytyczne*[26]j i musi być zawarta w tych planach, wraz ze wskazaniem środka komunikacji.

CERT.GOV.PL realizuje zadania związane z organami administracji publicznej. W ramach działalności zespołu podpisano porozumienia pomiędzy Agencją Bezpieczeństwa Wewnętrznego i innymi podmiotami, które są gotowe uczestniczyć w projektach ARAKIS-GOV i ARAKIS 2.0 GOV oraz z operatorami infrastruktury krytycznej, którzy są gotowi wymieniać się informacjami na temat incydentów. Ponadto CERT.GOV.PL współpracuje ze spółką Microsoft w dziedzinie profesjonalnych szkoleń dla administratorów systemów teleinformatycznych, którzy pracują dla administracji publicznej.

[25] Dziennik Urzędowy z 2010 r., nr 83, pozycja 541
[26] Dziennik Urzędowy z 2010 r., nr 83, pozycja 542

Głównym problemem zdiagnozowanym przez CERT.GOV.PL jest brak aktu prawnego regulującego reagowanie na incydenty cybernetyczne w kilku określonych dziedzinach. Brak jest instrumentu prawnego nakładającego na instytucje obowiązek składania sprawozdań z działań podjętych w przypadku przekazania im informacji przez CERT.GOV.PL.

6.2 Działania przeciw pornografii dziecięcej i wykorzystywaniu seksualnemu w internecie

6.2.1 Komputerowe bazy danych identyfikujące ofiary i środki na rzecz niedopuszczania do ponownej wiktymizacji

Policja dysponuje bazami danych zawierającymi między innymi dane o tożsamości sprawców. Nie dysponuje jednak bazą danych służącą specjalnie do identyfikacji ofiar. Sytuacja ta wynika z prawnych uregulowań w polskim prawie, m.in. z Ustawy o ochronie danych osobowych. Wynika również z braku ustawodawstwa umożliwiającego organom ścigania ustanowienie i wykorzystywanie bazy danych ściśle do identyfikacji ofiar.

Podczas wizyty na miejscu zauważono, że Policja nie dysponuje specjalną bazą danych wykorzystującą funkcje haszujące, która ułatwiałaby prowadzenie postępowania przygotowawczego i identyfikację dzieci będących ofiarami seksualnego wykorzystywania.

Polska Policja korzysta z wszystkich dostępnych sposobów prawnych, by usuwać z internetu treści prezentujące seksualne wykorzystywanie dzieci. Robi to przede wszystkim stosując procedurę powiadamiania i usuwania treści, często w ramach międzynarodowej współpracy policyjnej. Ponadto materiały prezentujące seksualne wykorzystywanie dzieci zabezpieczone w konkretnej sprawie (tj. w czasie realizacji nakazu przeszukania) są również usuwane po zamknięciu sprawy i zakończeniu procedury sądowej. Nie ma specjalnych procedur odnoszących się specjalnie do dzieci jako ofiar wykorzystywania seksualnego, których zdjęcia są rozpowszechniane w internecie. Takim ofiarom można jednak regularnie zapewniać pomoc, aby uniknąć szkód psychicznych i fizycznych oraz ponownej wiktymizacji (taką samą jak pomoc zapewniana dzieciom będącym ofiarami seksualnego wykorzystywania).

Podczas wizyty na miejscu zespół oceniający odwiedził organizację pozarządową Fundacja Dzieci Niczyje. Jej głównym zadaniem jest pomoc dzieciom, między innymi tym które padły ofiarą wykorzystywania seksualnego lub przemocy domowej. W siedzibie fundacji znajdują się specjalnie zaprojektowane pokoje, gdzie dzieci są przesłuchiwane przez przedstawicieli kompetentnych organów. W opinii oceniających przesłuchania młodych ofiar prowadzone we współpracy z Fundacją Dzieci Niczyje, a co za tym idzie korzystanie z nagrań wideo przesłuchań podczas postępowania sądowego stanowią przykład optymalnych rozwiązań, dzięki którym unika się ponownej wiktymizacji.

6.2.2 Środki służące przeciwdziałaniu wykorzystywaniu seksualnemu/niegodziwemu traktowaniu w celach seksualnych w internecie, sextingowi, cyberprzemocy

Przygotowano specjalną kampanię edukacyjną GADKI („Underwear Rule" www.gadki.fdn.pl) będącą polską wersją kampanii Rady Europy pt. „1 in 5". Realizuje ona zobowiązanie podjęte przez Polskę wskutek ratyfikacji Konwencji o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych. Celem kampanii jest nauczenie rodziców jak – prosto i naturalnie – przekazać dzieciom informacje, które mogą je ochronić przed wykorzystywaniem seksualnym i uświadomić je, że to one decydują o swoim ciele i że zawsze mogą powiedzieć „nie", jeśli czyjeś działanie narusza ich strefy intymne.

Ponadto zespół oceniający został poinformowany przez Ministerstwo Sprawiedliwości o pracach nad ustawą, która stworzy podstawę prawną do ustanowienia rejestru przestępców seksualnych, w szczególności tych, którzy zostali skazani za przestępstwa na tle seksualnym wobec dzieci.

6.2.3 Działania prewencyjne dotyczące turystyki seksualnej, uczestnictwa dzieci w pornografii i innych zjawisk

7 czerwca 2014 r. Komendant Główny Policji i przewodnicząca Fundacji Dzieci Niczyje podpisali roczne porozumienie, które w czerwcu 2015 r. przedłużono na kolejny rok. Celem tego porozumienia, będącego częścią międzynarodowej kampanii „Nie odwracaj wzroku" (Don't look away), jest zapobieganie turystyce seksualnej w celu wykorzystywania dzieci. Wspomniany dokument stanowi podstawę do zwiększenia skuteczności pracy policji poprzez utworzenie specjalnej strony internetowej (www.stopseksturystyce.fdn.pl), gdzie każdy może znaleźć formularz do zgłoszenia (anonimowo lub oficjalnie) informacji o przypadkach seksturystyki lub innych podejrzanych zachowaniach, które mogą być związane z seksualnym wykorzystywaniem dzieci.

Ponadto wszystkie takie zgłoszenia sprawdzane są przez odpowiednie jednostki Policji na szczeblu krajowym lub regionalnym (w zależności od tego, gdzie nastąpiło konkretne zgłoszenie) specjalizujące się w zwalczaniu seksualnego wykorzystywania dzieci. Po otrzymaniu danej informacji osoby prowadzące postępowanie mogą ją sprawdzić, a następnie podjąć stosowne działania operacyjne i dochodzeniowe.

Trwająca ponad dwa lata kampania przyciągnęła uwagę mediów, przedsiębiorstw turystycznych i użytkowników internetu. Strona kampanii została odwiedzona ponad 7 500 razy. W ramach wyżej wspomnianego polskiego projektu dotyczącego wykorzystywania seksualnego dzieci przeszkolono 750 funkcjonariuszy i cywilnych pracowników policji. W szkoleniu uczestniczyli również pracownicy hoteli i biur podróży oraz studenci turystyki. Od początku w tworzeniu projektu uczestniczy Policja, Fundacja Dzieci Niczyje i ECPAT International. Honorowy patronat nad projektem objęli: Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Sportu i Turystyki, Rzecznik Praw Obywatelskich i Rzecznik Praw Dziecka.

Z myślą o trzymaniu dzieci z dala od nielegalnych treści w internecie podjęto następujące działania prewencyjne:

Dyżurnet.pl

Od 2004 r. w NASK działa zespół Dyżurnet.pl, który w ramach programu Bezpieczniejszy internet (obecnie w ramach instrumentu „Łącząc Europę") zajmuje się zgłoszeniami otrzymywanymi od użytkowników internetu dotyczącymi nielegalnych lub szkodliwych treści (w szczególności materiałów prezentujących niegodziwe traktowanie dzieci). Ten punkt kontaktowy, działający w ramach NASK, jest częścią Polskiego Centrum Programu Safer Internet ustanowionego przez NASK i Fundację Dzieci Niczyje. Dyżurnet.pl jest członkiem stowarzyszenia INHOPE zrzeszającego podobne zespoły z całej Europy i spoza niej.

Zespół współpracuje z dostawcami treści, Policją i podobnymi zespołami na całym świecie, a forma współpracy w dziedzinie radzenia sobie z rozpowszechnianiem szkodliwych lub nielegalnych treści przypomina pracę zespołów CSIRT. Dyżurnet.pl i CERT POLSKA ściśle ze sobą współpracują w dziedzinie konsultacji na temat technologicznych aspektów tego problemu.

Policja utworzyła z Dyżurnet.pl partnerstwo, które obejmuje zgłaszanie niegodziwych zdjęć i treści znalezionych w internecie, w tym materiałów prezentujących niegodziwe traktowanie dzieci, specjalnej jednostce policji (Wydziałowi do walki z Cyberprzestępczością). Ponadto Fundacja Dzieci Niczyje prowadzi gorącą linię przeznaczoną dla dzieci i dorosłych, którzy chcą zgłosić przestępstwo seksualnego wykorzystywania dziecka lub podejrzaną sytuację, która może doprowadzić do takiego przestępstwa. Zgłoszenia takich sytuacji są przekazywane policji, tak by w razie potrzeby mogła ona podjąć stosowne działania prawne. Gorąca linia jest prowadzona wraz z policją.

Działania edukacyjne

Od 2013 r. Ministerstwo Cyfryzacji prowadzi działania służące ochronie dzieci i nastolatków przed niestosownymi treściami w internecie. Największy nacisk kładzie się na działania edukacyjne zwiększające świadomość niebezpieczeństw wywodzących się z internetu i umiejętności konieczne do bezpiecznego korzystania z internetu. Działania te są skierowane do różnych grup odbiorców, głównie dzieci i nastolatków, ale również do nauczycieli i rodziców. Na podstawie art. 13 ust. 1 ustawy o działalności pożytku publicznego i o wolontariacie realizacja tych działań, należących do zadań organów publicznych, jest przekazana organizacjom pozarządowym wybieranym w drodze konkursu. Jak dotąd Ministerstwo Cyfryzacji sfinansowało 11 projektów z tej dziedziny. Dotacje dla organizacji pozarządowych na działania służące ochronie dzieci i nastolatków w internecie wyniosły w 2013 r. 447 000 PLN (112 055 EUR), w 2014 r. – 838 925 PLN (210 304 EUR), a w 2015 r. – 1 000 000 PLN (250 683 EUR).

Na 2015 r. zaplanowano realizację trzech projektów tego rodzaju. Projekty te obejmują szkolenie około 6 000 uczniów w wieku 6–12 lat, około 4 500 uczniów w wieku 13–18 lat i około 2 000 nauczycieli, edukatorów i rodziców. W ramach finansowanych projektów opracowano – z udziałem ekspertów ds. bezpieczeństwa cybernetycznego (NASK i Uniwersytet Pedagogiczny im. Janusza Korczaka w Warszawie) – Standard bezpieczeństwa online placówek oświatowych. Standard ten obejmuje diagramy graficzne określające procedury interwencji np. w następujących przypadkach: cyberprzemoc, nagabywanie dzieci dla celów seksualnych, natknięcie się na nielegalne treści, sexting, czyny zabronione, nadmierne korzystanie z nowoczesnych technologii oraz sposób reagowania na zagrożenia i incydenty komputerowe. Przedstawiono również model profilaktyczny – zalecenia do przygotowania bezpiecznej i efektywnej infrastruktury internetowej dla szkół lub innych instytucji oświatowych.

Co roku minister edukacji narodowej wyznacza kierunek państwowej polityki edukacyjnej. Jej celem jest poprawa bezpieczeństwa w szkołach. W roku szkolnym 2014/2015 priorytetem nadal jest zapobieganie agresji i przemocy w szkołach. Określanie priorytetów oznacza, że w ciągu roku szkolnego dyrektor i nauczyciele powinni zwracać szczególną uwagę na tę kwestię, a instytucje wspierające szkołę, takie jak ośrodki psychologiczne i pedagogiczne, ośrodki kształcenia nauczycieli lub biblioteki pedagogiczne powinny wspierać dyrektorów w realizacji tych działań, np. poprzez przygotowywanie materiałów informacyjnych i edukacyjnych lub oferowanie szkoleń dla nauczycieli.

Ponadto toczą się prace nad drugim cyklem (na lata 2014–2016) programu Bezpieczna i przyjazna szkoła. Głównym założeniem programu jest zwiększenie efektywności działań edukacyjnych i prewencyjnych i stworzenie przyjaznego i bezpiecznego środowiska szkolnego. Program obejmuje m.in. następujące kwestie:

1) zapobieganie agresji i przemocy, również cyberprzemocy;
2) zapobieganie uzależnieniu się od gier komputerowych, internetu i hazardu;
3) rozwijanie umiejętności uczniów, uczenie ich poprawnych zachowań w środowisku nowych mediów;
4) przygotowywanie nauczycieli do prowadzenia lekcji na temat cyberprzemocy.

W ramach rządowego programu Bezpieczna i przyjazna szkoła utworzono telefon zaufania. Jest on przeznaczony dla uczniów, rodziców, nauczycieli i osób współpracujących ze szkołami.

1) Dla uczniów przeznaczony jest numer 116 111 i pomoc online. Czynne 10 godzin dziennie, 7 dni w tygodniu, oprócz świąt państwowych;
2) Inny numer telefonu – 800 100 100 – i pomoc online udostępniono rodzicom, nauczycielom i innym profesjonalistom przez 6 godzin dziennie od poniedziałku do piątku, oprócz świąt państwowych;
3) Strony internetowe www.116111.pl i www.800100.100.pl oferują darmowe wsparcie telefoniczne i online.

Strony te stanowią nieodłączną część pomocy telefonicznej i zawierają pakiet informacyjno-edukacyjny. Wysoką jakość oferowanej pomocy gwarantuje ciągłe monitorowanie pracy konsultantów przez przełożonych w godzinach pracy i organizowanie briefingów dla zespołów konsultantów każdorazowo przed rozpoczęciem dyżuru i po jego zakończeniu oraz comiesięczne kontrole. Organizacja składa miesięczne raporty z rozmów i interwencji.

Działania policji

CyberPol to program oparty na współpracy pomiędzy Policją a NASK, ukierunkowany na dzielenie się wiedzą i doświadczeniami dotyczącymi środków podejmowanych w odniesieniu do działań dzieci i nastolatków w internecie, zwalczania cyberprzestępczości i zwiększania świadomości ludzi korzystających z sieci. Głównym zadaniem CyberPol jest zwalczanie cyberprzestępczości i zwiększenie bezpieczeństwa dzieci i młodych ludzi w sieci.

Ministerstwo Spraw Wewnętrznych i Administracji uruchomiło gorącą linię, stronę internetową i adres mailowy. Dzięki temu możliwe jest natychmiastowe zgłaszanie nielegalnych i szkodliwych treści internetowych zagrażających dzieciom i młodym ludziom.

Dzięki współpracy pomiędzy Komendą Główną Policji, Fundacją Dzieci Niczyje, NASK, Rzecznikiem Praw Dziecka i Fundacją Orange, prowadzonej w ramach programu Komisji Europejskiej Bezpieczniejszy Internet, przygotowano kampanię Dziecko w sieci. Istotną częścią tej kampanii, poza działaniami w mediach, jest szeroki wachlarz oferowanych materiałów edukacyjnych. Zostały one przygotowane przez Fundację Dzieci Niczyje i są skierowane do dzieci, nastolatków, ich rodziców i profesjonalistów.

W ramach kampanii stworzono innowacyjny kurs o nazwie Dziecko w sieci. Pokazuje on różne aspekty seksualnego wykorzystywania dzieci w internecie i inne formy zagrożenia dla młodych użytkowników internetu (www.dzieckowsieci.pl). Kampania jest prowadzona pod patronatem Komendy Głównej Policji, Ministerstwa Edukacji, Pełnomocnika Rządu do Spraw Równego Traktowania i Urzędu Komunikacji Elektronicznej.

Działania są wspierane przez firmy Arcabit, Wirtualna Polska, VA Strategic Communications i kilku partnerów medialnych i są ukierunkowane na propagowanie możliwości oferowanych przez polski projekt Helpline.org.pl działający od lutego 2007 r. Konsultanci Helpline.org.pl udzielają pomocy online lub przez telefon w sytuacjach, gdy zagrożone jest bezpieczeństwo dziecka lub nastolatka w sieci.

Co roku Policja prowadzi krajowe, regionalne lub lokalne kampanie i inicjatywy – lub w nich uczestniczy – dotyczące bezpiecznego korzystania z internetu i zagrożeń, z którymi mogą się stykać dzieci i młodzież w internecie, w tym sytuacji związanych z różnymi formami wykorzystywania seksualnego dzieci lub materiałami prezentującymi niegodziwe traktowanie dzieci. Więcej informacji na temat projektów, programów i kampanii społecznych, które dotyczą działań prewencyjnych podejmowanych w tej dziedzinie, można również znaleźć pod adresem URL http://fdn.pl/en/social-campaigns.

W ocenie policji „live streaming" (transmisja strumieniowa na żywo) lub uczestniczenie dzieci w pornografii w internecie na żywo nie jest jeszcze w Polsce nasilającą się praktyką. Policja ma jednak świadomość, że te przestępcze działania mogą stanowić w przyszłości poważny problem.

Jak dotąd w Polsce było tylko kilka przypadków komercyjnego „live streamingu", przy czym większość z nich dotyczyła sytuacji, w których sprawcy z Polski próbowali oglądać na żywo pornografię z udziałem dzieci za pośrednictwem serwerów umieszczonych za granicą (np. na Filipinach), płacąc w zamian pewną kwotę pieniędzy. Inny rodzaj przestępstwa występujący w Polsce dotyczy sytuacji, w których dzieci dokonują seksualnych aktów przed kamerą internetową – nie otrzymując w zamian korzyści komercyjnej – podczas czatów z dorosłymi sprawcami. Oba te wyżej opisane czyny przestępcze są zakazane. W polskim kodeksie karnym „live streaming" lub, jak to jest określone, „uczestniczenie w prezentacji treści pornograficznych z udziałem małoletniego" jest karalne (art. 202§ 4a i 4c), a kara wynosi do dwóch lat pozbawienia wolności. Ponadto zachowanie sprawcy jest również traktowane jako element nagabywania dzieci dla celów seksualnych, które także jest karalne na mocy art. 200a kodeksu.

6.2.4 Podmioty i działania zwalczające strony internetowe zawierające lub rozpowszechniające pornografię dziecięcą

Polskie uregulowania dotyczące blokowania dostępu, usuwania treści i zamykania stron internetowych są oparte na normach określonych w dyrektywie 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informatycznego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym). *Ustawa o świadczeniu usług drogą elektroniczną z 2002 r.* stwierdza, że dostawca usług drogą elektroniczną jest odpowiedzialny za bezprawne treści, jeśli otrzymał wiarygodną wiadomość o bezprawnym charakterze tych treści. A zatem, żeby uniknąć takiej odpowiedzialności, dostawca usług drogą elektroniczną blokuje lub usuwa takie treści. Istotną rolę w tym względzie odgrywają organizacje pozarządowe, które informują dostawców.

Rozpowszechnianie materiałów prezentujących niegodziwe traktowanie dzieci jest zakazane na mocy art. 202 ust. 3 kodeksu karnego. A zatem, gdy takie materiały przechowywane na serwerach w Polsce zostają wykryte, Policja podejmuje wszelkie kroki konieczne do zidentyfikowania osoby odpowiedzialnej za ich umieszczenie i usuwa nielegalne treści z internetu. Jeśli do gorącej linii wpływa informacja o treściach prezentujących seksualne wykorzystywanie dzieci, to informacja ta jest przekazywana Policji (zazwyczaj Wydziałowi do walki z Cyberprzestępczością w Komendzie Głównej Policji), która następnie zajmuje się daną sprawą.

Gdy nastąpi wykrycie treści prezentujących niegodziwe traktowanie dzieci (niezależnie od tego, kto je znalazł w internecie) Policja, po otrzymaniu informacji, kontaktuje się z odpowiednim dostawcą usług internetowych lub dostawcą usług drogą elektroniczną w celu zidentyfikowania osoby, która umieściła te treści, a następnie dokonuje ich zajęcia (o ile jest to możliwe) i je usuwa. Następnie, po zidentyfikowaniu sprawcy, podejmowane są wobec niego kroki prawne i proceduralne.

Polskie prawo nie zezwala na stosowanie technik, które blokują dostęp do strony internetowej, nawet jeśli zawiera ona materiały prezentujące niegodziwe traktowanie dzieci. Policja usuwa wykryte treści o przedmiotowym charakterze, ale nie ma prawa blokować dostępu do stron internetowych zawierających takie materiały. W takich przypadkach ma zastosowanie procedura zgłaszania i usuwania treści. Zgodnie ze statystykami prezentowanymi w sprawozdaniach gorącej linii procedura ta przynosi dość dobre rezultaty i wspomniane materiały są szybko usuwane z internetu[27].

Nie ma konkretnej procedury blokowania dostępu/usuwania treści online, ale istnieje kilka sposobów zgłaszania znalezionych w internecie materiałów prezentujących niegodziwe traktowanie dzieci: głównie online za pomocą specjalnego formularza (jeśli zgłoszenie jest przesyłane do specjalnej gorącej linii lub za pośrednictwem takiej linii do policji) lub mailem, ale także listem lub, czasami, ustnie.

W Polsce dostępne są różne narzędzia filtrujące. Wiele z nich jest dostarczanych za darmo przez organizacje pozarządowe, firmy zajmujące się bezpieczeństwem internetu i niektórych dostawców usług internetowych (głównie firmy telekomunikacyjne). Dostawcy usług internetowych/usług drogą elektroniczną nie są jednak zobowiązani do oferowania takich narzędzi swoim klientom.

Nie ma jednego organu odpowiedzialnego za zajmowanie się nielegalnymi treściami online. W zależności od rodzaju treści (ich nielegalnego charakteru) decyzja o ich usunięciu (o ile nie usunął ich jeszcze dostawca usług internetowych/usług drogą elektroniczną) może być wydana przez sąd karny lub cywilny.

Każdy obywatel, instytucja lub organizacja w Polsce jest zobowiązana do informowania Policji o popełnionym przestępstwie. Dlatego Policja otrzymuje raporty o wykryciu takich materiałów, w tym o zawierających je stronach internetowych, od różnych podmiotów: obywateli, organizacji pozarządowych, instytucji publicznych i innych organów ścigania.

[27] Więcej informacji (po angielsku) dostępnych jest pod adresem internetowym: https://dyzurnet.pl/en/multimedia.html.

Zasada odpowiedzialności dostawców usług za dostarczanie usług drogą elektroniczną jest określona w Ustawie o świadczeniu usług drogą elektroniczną, która wdraża dyrektywę 2000/31/WE w sprawie e-handlu:

- art. 12 odnosi się do wyłączenia odpowiedzialności dostawcy usług w przypadku, gdy działanie dotyczy wyłącznie przeprowadzenia transmisji lub zapewnienia dostępu do sieci telekomunikacyjnej. Wyłączenie odpowiedzialności obejmuje również automatyczne i krótkotrwałe pośrednie przechowywanie transmitowanych danych, jeżeli działanie to ma wyłącznie na celu przeprowadzenie transmisji;
- art. 13 określa podstawy wyłączenia odpowiedzialności w przypadku usługi nazywanej caching. Oznacza to automatyczne i krótkotrwałe pośrednie przechowywanie danych, aby przyspieszyć ponowny dostęp do nich. Dostawca usług nie jest odpowiedzialny za przechowywane dane, jeśli nie modyfikuje danych, posługuje się uznanymi i stosowanymi zwykle technikami informatycznymi określającymi parametry techniczne dostępu do danych i ich aktualizowania i nie zakłóca posługiwania się technikami informatycznymi uznanymi i stosowanymi zwykle do zbierania informacji o korzystaniu ze zgromadzonych danych;

- art. 14 odnosi się do wyłączenia odpowiedzialności za tzw. hosting. Dostawca usług nie jest odpowiedzialny za przechowywane dane, jeśli nie ma wiedzy na temat ich bezprawnego charakteru. Gdy usługodawca otrzymuje urzędowe zawiadomienie lub wiarygodną wiadomość o bezprawnym charakterze danych lub związanej z nimi działalności, i uniemożliwia dostęp do tych danych, nie ponosi odpowiedzialności względem usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych (procedura zgłaszania i usuwania treści).

Na mocy art. 15 usługodawca nie jest zobowiązany do sprawdzania (monitorowania, kontrolowania, analizowania) danych przekazywanych, przechowywanych lub udostępnianych przez niego w związku z usługami, o których mowa w art. 12–14. Ma to szczególnie znaczenie w przypadku hostingu, gdy jedną z podstaw wyłączenia odpowiedzialności jest wiedza usługodawcy na temat bezprawnego charakteru przechowywanych danych.

Na mocy przepisów Ustawy o świadczeniu usług drogą elektroniczną dopuszczalne jest blokowanie dostępu do treści lub ich usuwanie, jeśli publikowane treści mają bezprawny charakter, a usługodawca jest o tym zawiadomiony. W tym celu usługodawca powinien otrzymać tzw. wiarygodną wiadomość. Może ona zostać przesłana przez kogokolwiek – zarówno stronę poszkodowaną, jak i stronę trzecią, nie mającą związku z przechowywanymi danymi. Możliwe jest otrzymanie wiarygodnej wiadomości od samego usługodawcy, np. w wyniku zaznajomienia się z komentarzami użytkowników na administrowanym forum internetowym. Usługodawca może zostać również powiadomiony przez organ publiczny, który przesyła mu tzw. urzędowe zawiadomienie.

W przypadku wykrycia treści prezentujących seksualne wykorzystywanie dzieci, które to treści umieszczone są na serwerach zagranicznych, Policja informuje stosowne organy ścigania w danym kraju i dostarcza im wszystkie zebrane materiały i dowody. W sferze międzynarodowych kanałów współpracy policyjnej w takich sprawach Policja korzysta z pomocy Europolu (jeśli sprawa dotyczy państwa członkowskiego UE lub ma związki z Europolem – kanał SIENA) i Interpolu oraz oficerów łącznikowych danych krajów. Jeśli materiały prezentujące niegodziwe traktowanie dzieci umieszczone na serwerach zagranicznych zostają wykryte przez pracowników gorącej linii, to informują oni swoich odpowiedników w danym kraju, jeśli działa w nim taka gorąca linia. Następnie pracownicy tej gorącej linii informują policję.

6.3 Oszustwa internetowe z wykorzystaniem kart płatniczych

6.3.1 Zgłaszanie online

Przestępstwa polegające na oszustwach z wykorzystaniem kart płatniczych są zazwyczaj zgłaszane bankom jako skargi przez obywateli i prywatne przedsiębiorstwa, a banki, jako ofiary, powiadamiają organy ścigania.

Według władz polskich współpraca pomiędzy branżą, bankami, sektorem prywatnym i organami ścigania w obszarze prewencji i zwalczania oszustw internetowych z wykorzystaniem kart płatniczych jest skuteczna. Wymogi dotyczące autoryzacji transakcji internetowych i potwierdzenia tożsamości klienta są coraz surowsze. Banki i sektor prywatny powiadamiają Policję, gdy dowiadują się o jakimkolwiek bezprawnym użyciu nowych narzędzi płatniczych. Policja nie jest informowana o strategiach banków w dziedzinie zwiększania bezpieczeństwa płatności bezgotówkowych.

Zgodnie z informacjami dotyczącymi kart płatniczych opublikowanymi przez Narodowy Bank Polski (NBP) w marcu 2015 r., 5% wszystkich kart płatniczych używanych w Polsce miało wyłącznie pasek magnetyczny. Ogromna większość kart płatniczych miała zarówno pasek magnetyczny, jak i mikroprocesor (94,6% wszystkich kart płatniczych). Całkowita liczba kart płatniczych wyposażonych wyłącznie w pasek magnetyczny stopniowo maleje. Rozwiązanie z wykorzystaniem mikroprocesora oparte na standardzie EMV zapewnia całkowicie bezpieczne korzystanie z karty.

Ponadto, zgodnie z Oceną funkcjonowania polskiego systemu płatniczego w Polsce opublikowaną przez NBP w drugiej połowie 2014 r. (na podstawie danych otrzymanych z banków), wielkość i wartość oszukańczych transakcji dokonanych z użyciem kart płatniczych w tym okresie wzrosła odpowiednio o 10,9% i 4,9%. Zgodnie z wyżej wymienionym dokumentem tendencja ta jest głównie spowodowana wzrostem liczby i wartości transakcji płatniczych z użyciem kart (wielkość i wartość oszukańczych transakcji w stosunku do wszystkich transakcji z wykorzystaniem karty płatniczej są wciąż na tym samym poziomie – oszukańcze transakcje stanowią tylko 0,003% wielkości i 0,006% całkowitej wartości transakcji płatniczych dokonanych z użyciem kart płatniczych wydanych przez banki).

Należy zauważyć, że 30 września 2013 r. organ doradczy NBP opublikował Rekomendacje w zakresie bezpieczeństwa kart zbliżeniowych. Rekomendacje zawierają zasady dotyczące wydawania, obsługi i przyjmowania kart zbliżeniowych. Mają one na celu ulepszenie procedur związanych z wydawaniem tego typu kart płatniczych. Według sprawozdania na temat wdrożenia rekomendacji, opublikowanego przez Związek Banków Polskich w kwietniu 2014 r., wszystkie banki – wydawcy kart płatniczych – stosują się do rekomendacji. Tylko dwa banki stwierdziły, że wdrożą je do końca 2014 r. Według polskiej Komisji Nadzoru Finansowego w styczniu 2015 r. oba banki zadeklarowały ich wdrożenie.

Ponadto dostawcy usług płatniczych podejmują działania ukierunkowane na zapewnienie bezpieczeństwa transakcji płatniczych. Banki, z myślą o zabezpieczeniu swoich bankomatów, instalują anty-skimmingowe czytniki kart, które rejestrują próby oszustw. Jednocześnie ogromna większość bankomatów jest monitorowana przez kamery. Aby zwiększyć bezpieczeństwo transakcji z użyciem kart utworzono specjalną linię telefoniczną ((+48) 828 828 828) dla tych użytkowników kart płatniczych, którym zginęła karta. To rozwiązanie umożliwia zablokowanie zaginionej karty, nawet jeśli użytkownik nie ma przy sobie numeru telefonu do banku. Najważniejszym elementem tego systemu jest w pełni zautomatyzowana linia telefoniczna IVR, w której stosuje się technologię rozpoznawania mowy.

Dochody z oszustw internetowych z wykorzystaniem karty płatniczej są często legalizowane w innych krajach niż kraj pochodzenia ofiary. Polska Jednostka Analityki Finansowej, odpowiedzialna za zwalczanie prania pieniędzy i finansowania terroryzmu, koncentruje się na zwiększaniu współpracy ze swoimi zagranicznymi odpowiednikami, aby sprawdzić, czy podejrzane transakcje objęte dochodzeniem są związane z legalizacją dochodów z oszustw internetowych z wykorzystaniem karty płatniczej.

Polska bierze udział w działaniach punktu kontaktowego AWF SOC FP TERMINAL. Współpraca przyczynia się do poprawy wymiany informacji w pracach nad daną sprawą. Krajowym koordynatorem pliku analitycznego na potrzeby AWF SOC FP TERMINAL jest wyznaczony funkcjonariusz policji w Wydziale do walki z Przestępczością Gospodarczą (Biuro Kryminalne Komendy Głównej Policji).

6.3.2 Rola sektora prywatnego

W obszarze oszustw z wykorzystaniem kart płatniczych policja współpracuje ze Związkiem Banków Polskich. Współpraca z bankami (wymiana informacji, wzajemne szkolenia) oparta jest na porozumieniu. Ewoluowała latami: z powodzeniem inicjowano i organizowano prace służące zapobieganiu popełnianiu przestępstw bankowych, w tym przestępstw popełnionych z nielegalnym wykorzystaniem kart płatniczych. Aktywne uczestnictwo przedstawicieli ZBP w wydarzeniach organizowanych przez Biuro Kryminalne KGP (specjalizujące się w szkoleniach dotyczących tego rodzaju przestępstw) przyczynia się do znaczącego poszerzenia wiedzy i umiejętności funkcjonariuszy policji w radzeniu sobie z wyżej wymienionymi kwestiami.
Ponadto w ramach wzajemnej współpracy, z udziałem przedstawicieli Związku Banków Polskich i Wydziału do walki z Przestępczością Gospodarczą BK KGP biorącego udział w zwalczaniu przestępstw z wykorzystaniem kart, opracowano algorytm dla organów ścigania w odniesieniu do wykrywania oszustw z użyciem kart. Celem tej strategii jest ułatwienie prowadzenia postępowania karnego w sprawie takich oszustw. Z myślą o realizacji tego celu temat ten został podzielony na 4 obszary: zgłaszanie kradzieży karty płatniczej, ujawnienie danych karty kredytowej przez osobę nieupoważnioną lub poprzez wykorzystanie okoliczności umożliwiających popełnienie przestępstwa (podejrzenie, że przestępstwo zostało popełnione w momencie przeprowadzania transakcji); skopiowanie danych karty płatniczej.

6.4. Wnioski

- Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej przewiduje trzypoziomowy Krajowy System Reagowania na Incydenty Komputerowe w cyberprzestrzeni: pierwszy poziom koordynacji na szczeblu ministerialnym; drugi poziom reagowania na incydenty komputerowe; trzeci poziom wdrażania odnosi się do administratorów odpowiedzialnych za poszczególne systemy ICT działające w cyberprzestrzeni.

- Głównym zadaniem CERT.GOV.PL jest zapewnienie bezpieczeństwa cybernetycznego na szczeblu rządowym (drugi poziom). CERT.GOV.PL zajmuje się incydentami cybernetycznymi w sektorze publicznym, a jego działania obejmują koordynację procesu reagowania na incydenty, rozwiązywanie problemów wywoływanych przez incydenty i ich analizę oraz koordynację reagowania na naruszenia bezpieczeństwa. W przypadku incydentu, który wykracza poza zdolności zespołu, CERT.GOV.PL współpracuje z wszystkimi innymi polskimi zespołami reagowania na incydenty cybernetyczne, takimi jak CERT POLSKA lub MIL-CERT.

- CERT POLSKA, którego działalność jest koordynowana przez Ministerstwo Cyfryzacji, jest wiodącą organizacją w zakresie zbierania i analizy informacji na temat cyberataków w Polsce. Podmioty zarządzające infrastrukturą krytyczną są zobowiązane do zgłaszania cyberataków do CERT POLSKA. CERT POLSKA działa jako centrum doskonałości i ma możliwość reagowania na zagrożenia, opracowywania oprogramowania do wczesnego ostrzegania i zapewniania specjalistycznych szkoleń na temat cyberprzestępczości i bezpieczeństwa cybernetycznego. Ponadto prowadzi badania w obszarze bezpieczeństwa cybernetycznego oraz gromadzi i publikuje coroczne statystyki na temat cyberataków. CERT POLSKA współpracuje ściśle i nieprzerwanie z CERT.GOV.PL i innymi zespołami CERT w celu zwalczania cyberataków.

- Polska stworzyła struktury do zajmowania się seksualnym wykorzystywaniem dzieci online. Realizowana jest efektywna współpraca z organami międzynarodowymi, takimi jak Europol, Interpol i NCMEC w odniesieniu do gromadzenia i analizy informacji związanych z seksualnym wykorzystywaniem dzieci. Ponadto podjęto inicjatywy i środki z myślą o zajęciu się zjawiskiem turystyki seksualnej, której ofiarami są dzieci. Prowadzonych jest również kilka publicznych kampanii i inicjatyw, które uruchomiono z myślą o zwiększeniu świadomości publicznej (np. na temat cyberprzemocy, nagabywania dzieci dla celów seksualnych, nielegalnych treści i sextingu). Nie ma jednak bezpośredniej łączności pomiędzy Wydziałem do walki z Cyberprzestępczością w Policji a bazą danych ICSE. Po wizycie na miejscu poinformowano zespół oceniający, że w 2016 roku zostały podjęte działania w celu przywrócenia bezpośredniego dostępu do bazy danych ICSE[28].

[28] Po wizycie na miejscu zespół oceniający poinformowano, że bezpośredni dostęp do bazy danych ICSE ma obecnie jeden specjalny funkcjonariusz w Komendzie Głównej Policji. Ten funkcjonariusz ma wkrótce przeszkolić innych, aby uzyskali oni dostęp do tej bazy. Baza danych ICSE jest wykorzystywana na co dzień przez wyspecjalizowany personel policyjny w sprawach dotyczących niegodziwego traktowania dzieci w celach seksualnych oraz we wspólnych działaniach międzynarodowych mających na celu identyfikację ofiar i sprawców.

- Stwierdzono, że w Policja nie dysponuje bazą danych wykorzystującą dedykowane funkcje haszujące, która ułatwiałaby prowadzenie postępowania przygotowawczego i identyfikację dzieci będących ofiarami seksualnego wykorzystywania. W opinii oceniających dużą przeszkodą jest brak krajowego rejestru plików z pornografią dziecięcą, który pozwalałby na identyfikację poszczególnych plików z użyciem funkcji haszującej. Taki rejestr pozwoliłby na zaoszczędzenie dużych zasobów, które można by wykorzystać do osiągania większych sukcesów w zwalczaniu cyberprzestępczości.

- Polsce udało się efektywnie zająć ponowną wiktymizacją dzieci dzięki wprowadzeniu specjalnie przystosowanych pokojów przesłuchań pod zarządem organizacji pozarządowej Fundacja Dzieci Niczyje. Fundacja dysponuje imponującymi, specjalnie zaprojektowanymi pomieszczeniami, wyposażonymi i urządzonymi tak, by przesłuchania dzieci i nastolatków w kontekście postępowań w sprawie wykorzystywania seksualnego były prowadzone w neutralnej i przyjaznej atmosferze, bez konfrontacji pomiędzy ofiarą i sprawcą. Fundacja oferuje również ofiarom tego typu przestępstw pomoc psychologiczną, medyczną i prawną. W opinii oceniających zadania realizowane przez fundację i profesjonalizm, jaki wypracowała, powinny być traktowane jako dobre praktyki. Ponadto oceniający uznają, że projekt prawa, które ustanawiałoby rejestr skazanych pedofilów, może jeszcze bardziej wzmocnić ochronę ofiar.

- Fundacja Dzieci Niczyje zapewnia również telefon zaufania oferujący wsparcie i doradztwo dzieciom w trudnych sytuacjach. Ten telefon zaufania odnosi ogromny sukces, ale z uwagi na problemy finansowe nie może działać 24 godziny na dobę. Z uwagi na fakt, że w opinii oceniających telefon zaufania odgrywa istotną i użyteczną rolę dla ofiar, można by rozważyć wsparcie fundacji, tak by działał on 24 godziny na dobę.

- Ponadto stwierdzono, że we współpracy z dostawcami usług drogą elektroniczną skutecznie stosowana jest procedura zgłaszania i usuwania treści. Wydaje się, że zatrzymywanie danych i współpraca z polskimi dostawcami usług internetowych działa z praktycznego punktu widzenia, choć w kilku państwach członkowskich brak jest wystarczającej współpracy z policją i organami sądowymi. Taka sytuacja raczej nie występuje w Polsce.

- Współpraca Policji ze Związkiem Banków Polskich stanowi tutaj przykład imponującego, a jednocześnie skutecznego współdziałania. Policja i zespoły reagowania na incydenty komputerowe należą do organu doradczego Związku Banków Polskich, dzięki czemu wymiana informacji jest skuteczna, a zwalczanie cyberataków przynosi efekty. Ten rodzaj współpracy z sektorem finansowym tworzy sytuację, w której wygrywają obie strony i która wg oceniających powinna być uznana za optymalne rozwiązanie.

7 WSPÓŁPRACA MIĘDZYNARODOWA

7.1 Współpraca z agencjami UE

7.1.1 Formalne wymogi współpracy z Europolem/EC3, Eurojustem, ENISA

Polscy prokuratorzy wypowiadają się pozytywnie na temat współpracy z Eurojustem. W większości przypadków kontakty takie były wykorzystywane do określenia właściwych organów, wyjaśnienia wymogów formalnych lub przyspieszenia przetwarzania wniosków.

Polska uczestniczy w działaniach dotyczących dwóch plików analitycznych: AWF SOC (poważna przestępczość zorganizowana) i AWF CT (zwalczanie terroryzmu). Polska jest zaangażowana w działania trzech punktów kontaktowych, które pomagają zwalczać cyberprzestępczość: Terminal, Cyborg i Twins. Aby utrzymać wysokie standardy koordynacji wymiany informacji w Polsce, wyznaczono krajowych koordynatorów każdego z tych punktów kontaktowych w oparciu o decyzję Komendanta Głównego Policji z 2014 r. w sprawie powołania ekspertów krajowych ds. realizowania działań związanych z plikami analitycznymi Europolu.

W związku ze zwalczaniem przestępczości z wykorzystaniem kart kredytowych Polska uczestniczy w działaniach AWF SOC FP TERMINAL. Współpraca w tym obszarze zasadniczo przybiera formę wymiany informacji w czasie prac nad daną sprawą na szczeblu krajowym (wkłady, wnioski) i międzynarodowym (odpowiedzi na wnioski, uczestnictwo w działaniach lub operacjach). Krajowym koordynatorem pliku analitycznego AWF SOC FP TERMINAL jest wyznaczony funkcjonariusz w Wydziale do walki z Przestępczością Gospodarczą (Biuro Kryminalne Komendy Głównej Policji). Tego typu przestępczość jest również zwalczana na szczeblu regionalnym. W każdej Komendzie Wojewódzkiej Policji jest wydział, który wyznacza koordynatora w obszarze zwalczania tego rodzaju przestępczości.

We wrześniu 2015 r. Wydział do Walki z Cyberprzestępczością został wyznaczony do uczestnictwa w platformie EMPACT w dziedzinie cyberataków. Ponadto wydział ten jest też członkiem punktu kontaktowego Europolu AWF SOC FP Cyborg. Z uwagi na jednak fakt, że Polska jest nowym członkiem wyżej wymienionych inicjatyw (FP Cyborg i platforma EMPACT w dziedzinie cyberataków), nie ma zbyt dużo doświadczenia we współpracy w konkretnych przypadkach, ale wspomniany wydział ma zamiar wzmocnić współpracę z Europolem w obszarze zwalczania cyberprzestępczości.

Obecnie Policja współpracuje ściśle z punktem kontaktowym Europolu FP Twins (jako członek tego punktu kontaktowego) w kilku przypadkach, w których konieczny jest udział Europolu, a także uczestniczy w operacjach międzynarodowych prowadzonych lub koordynowanych przez Europol, takich jak Downfall II, Daylight, Depletion, Lima Rhodes itd.

Ponadto Polska bierze udział w planowanych operacjach, np. w Dniu Przeciwdziałania Oszustwom przy Zakupie Biletów Lotniczych. Operacja ta jest organizowana raz w roku, a jej celem jest zapobieganie przestępstwom związanym z kupowaniem biletów lotniczych przez internet przy użyciu nielegalnie skopiowanych danych kart płatniczych. W operacji uczestniczą przedstawiciele największych linii lotniczych na świecie, wraz z Polskimi Liniami Lotniczymi LOT.
Od 2013 r. Polska jest członkiem zarządu Grupy Zadaniowej Unii Europejskiej ds. Zwalczania Cyberprzestępczości, w której skład wchodzą szefowie wyznaczonych w każdym z państw członkowskich zespołów ds. zwalczania cyberprzestępczości oraz Europol. Ta grupa o charakterze międzyagencyjnym powstała, by umożliwić szefom zespołów ds. zwalczania cyberprzestępczości, Europolowi, Komisji Europejskiej, CEPOL-owi i Eurojustowi, przy udziale obserwatorów: Interpolu, Norwegii, Szwajcarii i Islandii, omawianie kwestii strategicznych i operacyjnych związanych ze ściganiem cyberprzestępczości w UE i poza nią.

Ponadto we wrześniu 2014 r. Europol powołał w ramach swojego Europejskiego Centrum ds. Walki z Cyberprzestępczością Wspólną Grupę Zadaniową ds. Przeciwdziałania Cyberprzestępczości (J-CAT). Członkowie J-CAT byli zgromadzeni w kwaterze głównej Europolu i wspólnie prowadzili najważniejsze postępowania przygotowawcze i operacje z dziedziny cyberprzestępczości. Biuro Kryminalne i Centralne Biuro Śledcze zadeklarowały już chęć, by przyłączyć się do projektu.

Prowadzony przez Polskę projekt „Partnerstwo Wschodnie" wszedł w skład planu działań operacyjnych na rok 2016. Polska prowadzi aktywną współpracę z EC3 (punkt kontaktowy Terminal), aby zaangażować państwa Partnerstwa Wschodniego we wspólną walkę z oszustwami związanymi z kartami płatniczymi.

Co do współpracy z ENISA, to NASK i CERT POLSKA ściśle współpracują z agencją w formie uczestniczenia w jej organach zarządzających i grupach roboczych, rozwijając wiedzę fachową i realizując wytyczne opracowane przez ENISĘ. Możliwe było otrzymanie opinii ENISA zgodnie z art. 14 ust. 2 lit. d) rozporządzenia (UE) nr 526/2013 Parlamentu Europejskiego i Rady z dnia 21 maja 2013 r. w sprawie ENISA i uchylające rozporządzenie (WE) nr 460/2004; członkiem zarządu ENISA reprezentującym rząd polski jest pracownik NASK.

7.1.2 Ocena współpracy z Europolem/EC3, Eurojustem, ENISA

Polskie doświadczenia wskazują, że przy zaangażowaniu Eurojustu wnioski są zazwyczaj szybciej przetwarzane.

Ocena współpracy z Europolem jest również pozytywna. Europol zapewnia również dobre praktyki i informacje na temat narzędzi, które wspierają pracę funkcjonariuszy Policji zajmujących się przypadkami cyberprzestępczości. Podczas spotkań roboczych, które odbywają się w ramach działającej w ramach EC3 w Europolu grupy EUCTF (Europejska Grupa Zadaniowa ds. Cyberprzestępczości), przedstawiane są informacje na temat najnowszych zagrożeń związanych z cyberprzestępczością.

W odniesieniu do zwalczania seksualnego wykorzystywania dzieci i materiałów prezentujących niegodziwe traktowanie dzieci i podkreślono bardzo dobrą współpracę w ramach działań pliku analitycznego AWF SOC - FP Twins. Z uwagi na fakt, że wykorzystywanie seksualne dzieci (wiele różnych rodzajów tego zjawiska) ma charakter transgraniczny, kluczowa dla zwalczania tego typu przestępczości jest międzynarodowa współpraca organów ścigania. A zatem z uwagi na doświadczenia polskiej policji i wyniki prowadzonych wspólnie postępowań przygotowawczych i działań operacyjnych, pomoc Europolu, a zwłaszcza punktu kontaktowego Twins, w zwalczaniu seksualnego wykorzystywania dzieci i wizerunków przedstawiających takie wykorzystywanie, jest bardzo doceniane.

7.1.3 Działania operacyjne wspólnych zespołów dochodzeniowo-śledczych i cyber patrole

W 2015 r. Polska i Szwecja powołały wspólny zespół dochodzeniowo-śledczy do spraw oszustw internetowych. Policja nie uczestniczyła jak dotąd w operacyjnych fazach wielkoskalowych międzynarodowych operacji wymierzonych w seksualne wykorzystywanie dzieci i materiały prezentujące ich niegodziwe traktowanie (w tym w monitorowaniu konkretnych obszarów internetu, tj. pedofilskich „tablic ogłoszeniowych" w sieci TOR).

7.2 Współpraca pomiędzy władzami polskimi i Interpolem

Według władz polskich współpraca z Interpolem jest dobra, a w obszarze identyfikacji ofiar nawet doskonała.

Policja ściśle współpracuje z Interpolem w obszarze identyfikacji ofiar seksualnego wykorzystywania dzieci, w szczególności w korzystaniu z międzynarodowej bazy danych dotyczącej seksualnego wykorzystywania dzieci (ICSE). Za pośrednictwem kanału, jakim jest Interpol, policja otrzymuje z innych krajów – i przekazuje – informacje operacyjne/wywiadowcze i dowody przestępstw dotyczących seksualnego wykorzystywania dzieci i materiałów prezentujących takie wykorzystywanie potrzebne do podjęcia wszelkich, uznanych za konieczne, stosownych działań (zarówno w państwach członkowskich UE, jak i w państwach trzecich).

Obecnie Policja ma dostęp do bazy danych ICSE poprzez bezpośredni kontakt z odpowiednimi oficerami Interpolu i otrzymuje dostęp do bazy danych poprzez kanał I – 24/7. Jak dotąd, w oparciu o otrzymane w ten sposób informacje i materiały z ICSE, Policji udało się dokonać pozytywnej identyfikacji ofiar i sprawców zarówno w Polsce, jak i za granicą.

Jednak z uwagi na rosnąca liczbę prowadzonych przez Policję spraw dotyczących przestępstw przeciw dzieciom Komenda Główna Policji podjęła ostatnio działania w celu uzyskania bezpośredniego dostępu do bazy danych ICSE dla Komendy Głównej Policji i wybranych komend wojewódzkich. Obecnie Biuro Kryminalne Komendy Głównej Policji prowadzi badania, by stwierdzić ilu funkcjonariuszy ds. kryminalnych na szczeblu krajowym i regionalnym potrzebuje indywidualnego dostępu do ICSE. Następnym krokiem będzie organizacja szkolenia dla przyszłych użytkowników ICSE.

7.3 Współpraca z państwami trzecimi

Do celów współpracy z państwami trzecimi w obszarze zwalczania seksualnego wykorzystywania dzieci i materiałów prezentujących takie wykorzystywanie korzysta się głównie z kanału jakim jest Interpolu. Policja korzysta jednak również z pomocy Europolu do współpracy z państwami trzecimi, które podpisały porozumienie operacyjne o współpracy z Europolem (m.in. Australią, Kanadą, USA lub Kolumbią). Niemniej do celów komunikacji i współpracy z wyżej wymienionymi państwami trzecimi częściej korzysta się z pośrednictwa Interpolu. Czasami Policja wykorzystuje również polskich oficerów łącznikowych, w szczególności w kontaktach z Białorusią, Rosją i Ukrainą.

Według władz polskich współpraca z państwami trzecimi za pośrednictwem Europolu jest przydatna. Pełną ocenę można jednak przeprowadzić indywidualnie na podstawie okoliczności konkretnej operacji lub postępowania przygotowawczego. Jako przykład istotnej roli Europolu podaje się współpracę przy operacjach prowadzonych z USA lub dowodzenie takimi operacjami.

W państwach trzecich składano wnioski o pomoc prawną (Indie, Tajlandia i USA). Wszystkie sprawy dotyczyły przestępstw, w których użyto komputera lub systemu IT jako narzędzia lub celu, w szczególności w oszustwach internetowych z wykorzystaniem kart. Wnioski przesyłano za pośrednictwem Prokuratury Generalnej, z pomocą Europolu lub Eurojustu.

Polscy prokuratorzy składali wnioski o wzajemną pomoc prawną – w sprawach dotyczących cyberprzestępstw – w Singapurze i Indonezji. Realizacja tych wniosków trwała odpowiednio 11 i 18 miesięcy.

7.4 Współpraca z sektorem prywatnym

Policja współpracuje z podmiotami prywatnymi, w większości w USA, w przypadkach dotyczących działalności przestępczej: seksualnego wykorzystywania dzieci za pośrednictwem internetu, rozpowszechnianie w internecie materiałów prezentujących seksualne wykorzystywanie dzieci, itp. W takich przypadkach Policja współpracowała lub próbowała współpracować bezpośrednio z tymi firmami, z uwagi na fakt, że w Polsce takie spółki jak Facebook, Yahoo i Google nie mają swoich oddziałów. Zazwyczaj policja współpracowała na szczeblu operacyjnym/wywiadowczym wysyłając konkretne wnioski i bardzo często otrzymywała odpowiedź, że bez wniosku o pomoc prawną lub nakazu sądowego dany podmiot nie może przekazać tych informacji. Sytuacje te miały duży wpływ na toczące się postępowania, a czasami skutkowały nawet zamknięciem danej sprawy.

7.5 Narzędzia współpracy międzynarodowej

7.5.1 Wzajemna pomoc prawna

Zasady wzajemnej pomocy prawnej ogółem (wzajemna pomoc prawna, przekazywanie ścigania, przekazywanie wykonywania wyroków oraz ekstradycja) reguluje Kodeks postępowania karnego, a jego przepisy są stosowane zgodnie z zasadą pomocniczości –wyłącznie jeśli brak jest międzynarodowego instrumentu prawnego lub jeśli przepisy takiego instrumentu nie regulują konkretnych kwestii. Wynika to z podstawowej konstytucyjnej zasady pierwszeństwa ratyfikowanych konwencji w stosunku do prawa krajowego, która to zasada stosuje się również do wzajemnej pomocy prawnej w sprawach karnych. W ustawodawstwie polskim nie ma konkretnych przepisów dotyczących wzajemnej pomocy prawnej w sprawach dotyczących cyberprzestępczości, ponieważ zastosowanie mają ogólne przepisy dotyczące wzajemnej pomocy prawnej.

Współpraca z państwami członkowskimi Unii Europejskiej

Współpraca sądowa z właściwymi organami w UE regulowana jest rozdziałami 62a–67 kpk, które uwzględniają wszystkie przyjęte instrumenty wzajemnego uznawania w sprawach karnych i stosowne przepisy proceduralne dotyczące wzajemnej pomocy prawnej oraz przekazywania ścigania. Głównym celem jego przepisów jest umożliwienie płynniejszej i szybszej współpracy oraz uproszczenie i przyspieszenie procedur. A zatem, w powiązaniu ze stosownymi instrumentami wielostronnymi (takimi jak Europejska konwencja o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi UE, ustanowiona przez Radę zgodnie z art. 34 Traktatu o Unii Europejskiej, oraz konwencja z Schengen), umożliwia on bezpośrednią komunikację pomiędzy władzami sądowymi państw członkowskich UE.

W 2014 r. władze polskie otrzymały z państw członkowskich 781 wniosków w sprawie wzajemnej pomocy prawnej i same złożyły 564 wnioski. Większość wniosków z zakresu cyberprzestępczości, zarówno złożonych, jak i otrzymanych, dotyczyła przestępstw internetowych (oszustwa komputerowe, oszukańcze maile) i ataków na systemy komputerowe (przede wszystkim korzystanie ze złośliwego oprogramowania w celu uzyskania dostępu do systemów bankowych). Kilka wniosków dotyczyło materiałów prezentujących niegodziwe traktowanie dzieci, naruszania praw autorskich i przestępstw z nienawiści (nawoływanie do nienawiści na tle rasowym i ksenofobicznym).

Wszystkie wnioski rozpatrzono w terminie od jednego do trzech miesięcy, przy czym średni czas rozpatrywania wynosił mniej niż 30 dni w przypadku pilnych wniosków. Realizacja wniosków przesłanych przez władze polskie trwała średnio od trzech do dwunastu miesięcy, a do osiemnastu miesięcy w szczególnie złożonych sprawach.

Współpraca z państwami trzecimi

Ogólne zasady dotyczące wzajemnej pomocy prawnej z państwami trzecimi są określone w kpk i przepisach regulaminowych prokuratur i sądów. Zgodnie z tymi aktami, w zależności od przepisów umów dwu- i wielostronnych, wnioski o wzajemną pomoc prawną są przekazywane bezpośrednio (pomiędzy właściwymi krajowymi lub centralnymi organami sądowymi) lub kanałem dyplomatycznym (przez Ministerstwo Spraw Zagranicznych).

Do wysyłania wniosków o wzajemną pomoc prawną w sprawach związanych z cyberprzestępczością często wykorzystywano ustalenia dwustronne lub wielostronne. Największą trudnością jest to, że właściwe organy państw trzecich wykonują wniosek polskich organów dwa do trzy razy dłużej niż trwa to w ramach UE.

Wnioski o międzynarodową pomoc prawną najczęściej dotyczą: odnalezienia (ustalenia tożsamości) i przesłuchania użytkowników komputerów o określonym adresie IP, zachowania i wyświetlenia dokumentów lub innych nośników danych i ich kopii, ustalenia tożsamości i przesłuchania posiadaczy kont bankowych (zwłaszcza tych, na które wpływają kwoty wyłudzone wskutek phishingu), przesłuchania świadka lub podejrzanego oraz uzyskania informacji z rejestrów karnych.

Pomoc możliwa jest na wszystkich etapach postępowania i w odniesieniu do wszystkich czynności dochodzeniowo-śledczych lub proceduralnych (przesłuchanie, udostępnianie dokumentów, uzyskiwanie informacji bankowych, ocena przez ekspertów, śledzenie przekazów telekomunikacyjnych, identyfikacja użytkowników takich przekazów, przechwytywanie i zapisywanie przekazów telekomunikacyjnych i innych form komunikacji, przechwytywanie wiadomości e-mail, przeszukanie i zajęcie, konfiskata itp.). Wnioski o wzajemną pomoc prawną w zakresie cyberprzestępczości dotyczą najczęściej śledzenia przekazów telekomunikacyjnych i identyfikacji użytkowników takich przekazów.
Muszą one być wysyłane dość często, gdyż wiele cyberprzestępstw (nie tylko ataków cybernetycznych) popełnianych jest przez obywateli innych państw lub z użyciem zagranicznej infrastruktury informatycznej.

Co roku prokuratura wysyła ponad 300 wniosków, a sama otrzymuje około 100. Większość z nich dotyczy różnych rodzajów oszustw w internecie (głównie fałszywych aukcji internetowych), złośliwego oprogramowania i phishingu. Rozpatrywanie otrzymanych wniosków trwa średnio od 1 do 3 miesięcy. Uzyskanie odpowiedzi od innych państw trwa zwykle od 4 do 12 miesięcy, przy czym okres ten jest znacznie dłuższy w przypadku państw spoza UE.

Osoby, z którymi rozmawiano, poruszyły problem współpracy z niektórymi państwami członkowskimi, np. z tymi, które regularnie odmawiają współpracy w przypadkach, gdy wartość szkody jest niższa niż określona kwota.

7.5.2 Instrumenty dotyczące wzajemnego uznawania

Nie można przedstawić wymaganych danych na temat instrumentów dotyczących wzajemnego uznawania, gdyż ten rodzaj przestępczości nie jest wyszczególniony w odnośnych statystykach.

7.5.3 Wydawanie osób / ekstradycja

ENA

Na mocy art. 607b § 1 kpk zwrócenie się o wydanie osoby na podstawie ENA w związku z przestępstwem zagrożonym w prawie polskim karą pozbawienia wolności w wymiarze co najmniej roku. Ma to zastosowanie do cyberprzestępstw, gdyż kary przewidziane w odnośnych przepisach kpk przekraczają to minimum.

Przy wydawaniu osoby nie jest wymagany minimalny okres zagrożenia karą, a zasada podwójnej odpowiedzialności karnej nie jest sprawdzana, jeśli nakaz wydano w odniesieniu do przestępstwa zagrożonego w prawie państwa członkowskiego, które go wydało, maksymalną karą pozbawienia wolności w wymiarze co najmniej trzech lat oraz jeśli przestępstwo takie jest w tym prawie zakwalifikowane m.in. jako przestępstwo komputerowe.

Maksymalne kary za wszystkie przestępstwa komputerowe wynoszą ponad rok pozbawienia wolności, a zatem według polskiego prawa wszystkie przestępstwa komputerowe wchodzą w zakres listy przestępstw podlegających ENA i stanowią podstawę do ekstradycji.

Co roku wysyłanych jest średnio 10 ENA w sprawach dotyczących cyberprzestępczości, a otrzymuje się ich ok. 4. Wykonanie nakazu trwa od 12 dni do 3 miesięcy.

Nakazy te wydawane są (na wniosek prokuratury lub z urzędu) przez sądy okręgowe i przekazywane bezpośrednio między organami sądowymi lub – jeśli nie jest znane miejsce pobytu poszukiwanej osoby – centralnej jednostce policji.

Ekstradycja

Jeśli chodzi o minimalny okres zagrożenia karą, to w polskim prawie (art. 604 § 2 kpk) istnieje wymóg, by w przypadku ekstradycji popełnione przestępstwo było w państwie, który złożyło wniosek, zagrożone karą pozbawienia wolności o wymiarze co najmniej roku (chodzi o maksymalny wymiar kary za popełnienie tych przestępstw).

Wnioski o ekstradycję wydawane są przez prokuratorów lub sądy i przekazywane właściwym organom w państwie trzecim za pośrednictwem Ministerstwa Sprawiedliwości lub kanałami dyplomatycznymi.

Zarówno europejskie nakazy aresztowania, jak i wnioski o ekstradycję, są realizowane przez prokuraturę, a ostateczną decyzję o wydaniu osoby podejmuje sąd okręgowy (w przypadku ekstradycji o wydaniu rozstrzyga następnie minister sprawiedliwości).

7.6 Wnioski

- Polska prowadzi współpracę z szeregiem agencji UE, takich jak Europol/EC3, Eurojust i ENISA. Prokuratorzy zajmujący się cyberprzestępczością w pełni zdają sobie sprawę zarówno z roli Eurojustu, jak i z atutów współpracy z nim, i zwracają się do niego o pomoc, gdy jest taka potrzeba. Ponadto CERT POLSKA skutecznie współpracuje z ENISĄ w zwalczaniu cyberataków.

- Policja ściśle współpracuje z Europolem/EC3. Bierze udział w działaniach strategicznych poprzez uczestnictwo w platformach EMPACT w dziedzinach: seksualnego wykorzystywania dzieci, cyberataków i oszustw związanych z kartami. Polska jest członkiem trzech punktów kontaktowych EC3/Europolu: punkt kontaktowy Twins (udział w organizowanych przez niego operacjach, spotkaniach ekspertów i szkoleniach); punkt kontaktowy Terminal (aktywne uczestnictwo w Dniu Przeciwdziałania Oszustwom przy Zakupie Biletów Lotniczych, prowadzące do szeregu zatrzymań na lotnisku w Warszawie) oraz punkt kontaktowy Cyborg (udział w operacji Onynimous).

- W 2015 r. Polska i Szwecja utworzyły wspólny zespól dochodzeniowo-śledczy w celu zwalczania zorganizowanej grupy przestępczej zajmującej się oszustwami komputerowymi na świecie. Prowadzony przez Polskę projekt „Partnerstwo Wschodnie" wszedł w skład planu działań operacyjnych na rok 2016. Polska prowadzi aktywną współpracę z EC3 (punkt kontaktowy Terminal), aby zaangażować państwa Partnerstwa Wschodniego we wspólną walkę z oszustwami związanymi z kartami płatniczymi. Polska dołączyła do platformy EMPACT w dziedzinie tych oszustw w 2016 r.

- Od 2013 r. Polska jest członkiem zarządu Grupy Zadaniowej Unii Europejskiej ds. Zwalczania Cyberprzestępczości, w której skład wchodzą szefowie wyznaczonych w każdym z państw członkowskich zespołów ds. zwalczania cyberprzestępczości oraz Europol. Ta grupa o charakterze międzyagencyjnym powstała, by umożliwić szefom zespołów ds. zwalczania cyberprzestępczości, Europolowi, Komisji Europejskiej, CEPOL-owi i Eurojustowi, przy udziale obserwatorów: Interpolu, Norwegii, Szwajcarii i Islandii, omawianie kwestii strategicznych i operacyjnych związanych ze ściganiem cyberprzestępczości w UE i poza nią. Polska wniosła częściowy wkład w publikowaną co roku ocenę zagrożenia wykorzystania internetu przez zorganizowane grupy przestępcze (iOCTA) w latach 2014 i 2015. W 2016 r. i w kolejnych latach wkład ten ma być pełniejszy.

- Organy w Polsce zdobyły już pewne doświadczenie we współpracy z podmiotami prywatnymi z państw trzecich, w większości pochodzącymi z USA zajmującymi się zwalczaniem przestępczości w dziedzinach takich jak: niegodziwe traktowanie dzieci w internecie, rozpowszechnianie związanych z tym materiałów w internecie itp. W tych przypadkach policja starała się uzyskać dane bezpośrednio od firm prywatnych, takich jak Facebook, Yahoo i Google). Te twierdziły jednak, że bez wniosku o (wzajemną) pomoc prawną lub nakazu sądowego nie mogą przekazać tych informacji. Oceniający stwierdzili, że ze względu na te doświadczenia UE powinna rozważyć możliwość zawarcia umowy z usługodawcami takimi jak Facebook, Yahoo i Google w zakresie dostarczania danych potrzebnych do zwalczania cyberprzestępczości.

- Procedura wnioskowania o wzajemną pomoc prawną jest stosowana do uzyskania dowodów elektronicznych od innych państw członkowskich i państw trzecich. Średni czas rozpatrywania wniosków wynosi od 1 do 3 miesięcy. Zdaniem oceniających procedura wzajemnej pomocy prawnej wydaje się najskuteczniejszym sposobem uzyskiwania dowodów elektronicznych do celów ścigania, choć czasami zabiera zbyt dużo czasu, a to niekorzystnie wpływa na postępowanie przygotowawcze.

8 SZKOLENIE, PODNOSZENIE ŚWIADOMOŚCI I PREWENCJA

8.1 Szkolenia specjalistyczne

Szkolenie pracowników wymiaru sprawiedliwości

Krajowa Szkoła Sądownictwa i Prokuratury regularnie organizuje szkolenia z zakresu cyberprzestępczości dla kadr wymiaru sprawiedliwości i prokuratury. Od 2009 r. zorganizowała ona następujące kursy:

- „Metodologia prowadzenia postępowania karnego w sprawach związanych z wykorzystaniem systemów informatycznych" (2009 i 2010 r.),
- „Postępowanie przygotowawcze a systemy informatyczne – dowody elektroniczne w postępowaniu karnym" (2010 r.),
- „Praktyczne aspekty postępowania karnego opartego o prawo autorskie i prawa pokrewne" (2011 r.; wśród omawianych tematów znajdowała się współpraca z administratorami internetowych serwisów aukcyjnych i rola biegłych informatyków w postępowaniu),
- „Kryminologiczna rekonstrukcja przestępstwa. Najnowsze osiągnięcia kryminalistyki w wykrywaniu i zabezpieczaniu śladów na miejscu zdarzenia" (2011 r.; dyskusje dotyczyły zwłaszcza zabezpieczania elektronicznych nośników danych i sprzętu komputerowego),
- „Odpowiedzialność karna a świadczenie usług medycznych. Przestępstwa popełniane za pośrednictwem sieci informatycznych" (2013 r.).

Ponadto w ramach projektu „Szkolenie kadr wymiaru sprawiedliwości i prokuratury w zakresie zwalczania i zapobiegania przestępczości transgranicznej i zorganizowanej" w 2015 r. zorganizowano dziewięć szkoleń na temat transgranicznej przestępczości zorganizowanej. Szkolenie to jest także kontynuowane w 2016 r.

Ponadto, co roku wszyscy nowo powołani sędziowie i asesorzy uczestniczą w specjalnym szkoleniu na temat przestępstw popełnianych z wykorzystaniem komputerów i systemów informatycznych. Na 2016 r. zaplanowany jest moduł szkoleniowy na temat przestępczości komputerowej dla 140 sędziów, prokuratorów, asesorów i asystentów. Omówione zostaną następujące tematy:

- cyberprzestępczość,
- zabezpieczanie istotnych informacji dowodowych, zwłaszcza danych informatycznych, w zakresie przestępstw bankowych, internetowych przestępstw seksualnych i cyberataków;
- wykorzystywanie dowodów elektronicznych w postępowaniach karnych;
- dopuszczalność dowodów elektronicznych;
- funkcjonowanie sieci anonimizujacej „TOR" i możliwości identyfikacji przestępców korzystających z niej,
- metodologia prowadzenia postępowań karnych w sprawach dotyczących oszustw internetowych i komputerowych, w tym przestępstw popełnionych poprzez rozpowszechnianie wirusów komputerowych.

Ponadto Biuro Kryminalne Komendy Głównej Policji w porozumieniu z siecią NASK oferowało kursy w zakresie dowodów elektronicznych i technik walki z cyberprzestępczością przeznaczone dla sędziów, prokuratorów i funkcjonariuszy policji.

Szkolenie Policji

Policja prowadzi szkolenie z dziedziny cyberprzestępczości zatytułowane: „Przestępczość komputerowa – uzyskiwanie informacji z internetu". Szkolenie to jest regularnie prowadzone w Wyższej Szkole Policji w Szczytnie od 2005 r. Jest ono przeznaczone dla policjantów zajmujących się przestępczością komputerową i cybernetyczną. Ma ono poszerzyć wiedzę policjantów z wydziałów kryminalnych na temat przestępczości komputerowej i uzyskiwania informacji z internetu, aby usprawnić prowadzenie postępowań przygotowawczych w sprawach z tej dziedziny. Tematyka szkolenia obejmuje: charakterystykę przestępczości komputerowej, środowisko komputerowe, usługi w sieciach komputerowych lub procedury, jakich należy przestrzegać w sprawach o przestępstwa komputerowe. To trwające 45 godzin (5 dni) szkolenie jest powtarzane kilka razy w roku.

W ramach centralnego systemu szkolenia policji organizowane są specjalistyczne kursy z zakresu gromadzenia danych internetowych dla funkcjonariuszy zajmujących się zwalczaniem cyberprzestępczości. Uczestnictwo w kursie podlega następującym kryteriom:

- funkcjonariusz powinien zajmować się cyberprzestępczością i zbieraniem danych internetowych,
- funkcjonariusz powinien być bezpośrednio zaangażowany w zwalczanie cyberprzestępczości w wydziałach/jednostkach kryminalnych i gospodarczych,
- funkcjonariusz powinien posiadać podstawowe umiejętności komputerowe (obsługa komputera osobistego z oprogramowaniem MS Windows)
- znajomość polskiego prawa karnego w dziedzinie cyberprzestępczości.

Kurs trwa pięć dni. W 2014 r. zorganizowano 25 takich kursów, podczas których przeszkolono 304 funkcjonariuszy. Na 2015 r. zaplanowano organizację 25 takich kursów, podczas których miało zostać przeszkolonych 299 funkcjonariuszy. Decyzją Komendy Głównej Policji w 2015 r. utworzono zespół, którego zadaniem jest opracowanie programu kursu dla policjantów specjalizujących się w zadaniach związanych ze zwalczaniem cyberprzestępczości.

W dziedzinie walki z wykorzystywaniem seksualnym dzieci i materiałami prezentującymi niegodziwe traktowanie dzieci policja planuje organizację 3-4 kursów rocznie dla policjantów w całym kraju, w tym funkcjonariuszy zaangażowanych w międzynarodową współpracę policyjną. Brak jest jednak kursów skierowanych specjalnie do funkcjonariuszy zajmujących się międzynarodową współpracą policyjną w tych obszarach przestępczości. Ponadto policyjni eksperci specjalizujący się w tych obszarach spotykają się co najmniej raz lub dwa razy w roku, by zebrać nowe doświadczenia, uzyskać informacje o bieżących tendencjach i zagrożeniach, a także wymienić się optymalnymi rozwiązaniami i przeanalizować konkretne przykłady.

Działania zespołu CERT.GOV.PL obejmują organizację szkoleń i kampanie informacyjne. Agencja Bezpieczeństwa Wewnętrznego zorganizowała we współpracy z Microsoftem szkolenie dla administratorów systemów teleinformatycznych administracji publicznej w ramach modułu bezpieczeństwa informatycznego programu SCP (Security Cooperation Program). W szkoleniu tym wzięło udział 176 uczestników.

Ministerstwo Spraw Wewnętrznych i Administracji oraz Komenda Główna Policji we współpracy z NASK rozpoczęły w 2015 r. projekt „CyberPol". Głównym jego celem jest poprawa kompetencji krajowych organów ścigania w dziedzinie cyberprzestępczości. W szkoleniu, podzielonym na trzy stopnie zaawansowania, bierze udział 210 funkcjonariuszy (30 policjantów z wydziałów/jednostek zajmujących się cyberprzestępczością uczestniczyło w dwudniowym kursie zorganizowanym przez zespół CERT POLSKA). Projekt „Safer Internet" (prowadzony przez NASK i Fundację Dzieci Niczyje) zapewnia szkolenia i konferencje dla organów ścigania oraz oferuje elektroniczne materiały na temat bezpieczeństwa dzieci w internecie i nowych technologii.

W ramach szkoleń zawodowych dla techników kryminalistyki prowadzone są kursy wybranych zagadnień teleinformatycznych (obejmujące część dla informatyków śledczych). W trakcie swojego szkolenia funkcjonariusze zajmujący się zwalczaniem przestępczości gospodarczej biorą udział w zajęciach dotyczących przestępczości komputerowej.

Wyższa Szkoła Policji w Szczytnie prowadzi następujące wykłady na tematy znajdujące się w programie zajęć (na poziomie podstawowym): Metodyka prowadzenia śledztwa w sprawach związanych z nielegalnym kontentem (zawartością) oraz Pozyskiwanie i badanie dowodów elektronicznych z nośników komputerowych. Za prowadzenie szkoleń z informatyki śledczej odpowiadają Wyższa Szkoła Policji w Szczytnie i Centrum Szkolenia Policji w Legionowie.

Centrum Badań nad Cyberprzestępczością – Wydział Prawa i Administracji Uniwersytetu Mikołaja Kopernika

W dniu 1 października 2013 r. na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika utworzone zostało i rozpoczęło swą działalność Centrum Badań nad Cyberprzestępczością. Powadzi ono badania i działalność szkoleniowo-edukacyjną w dziedzinie zapobiegania cyberprzestępczości i zwalczania jej. Organizuje doroczne konferencje (nt. ataków sieciowych) oraz ułatwia współpracę i wymianę poglądów i doświadczeń pomiędzy różnymi podmiotami (dostawcami usług internetowych lub elektronicznych, organami ścigania, sędziami, naukowcami).

Centrum Analityczno-Wywiadowcze i Doskonalenia Zwalczania Cyberprzestępczości

W 2015 r. w Wyższej Szkole Policji w Szczytnie utworzono Centrum Analityczno-Wywiadowcze i Doskonalenia Zwalczania Cyberprzestępczości. Podpisano umowy o współpracy z szeregiem podmiotów prywatnych i publicznych. Działalność Centrum obejmuje:

- szkolenie i doskonalenie zawodowe służb mundurowych;
- metodykę szkolenia i doskonalenia zawodowego służb mundurowych;
- badania naukowe i prace rozwojowe nad problematyką szeroko rozumianej cyberprzestępczości;
- opracowywanie raportów, publikacji i materiałów dydaktycznych związanych z problematyką cyberprzestępczości;
- organizowanie wykładów, spotkań okolicznościowych i konferencji oraz seminariów naukowych i przedsięwzięć specjalistycznych;
- wzajemne spotkania robocze mające na celu określenie obszarów współpracy możliwych do wykorzystania w procesie naukowo-dydaktycznym;
- konsultacje w zakresie rozwiązywania problemów związanych ze zwalczaniem cyberprzestępczości.

Narodowe Centrum Kryptologii

Działające w ramach struktur Ministerstwa Obrony Narodowej Narodowe Centrum Kryptologii podpisało umowy z trzema wiodącymi uczelniami państwowymi (Politechnika Wrocławska, Uniwersytet Warszawski, Politechnika Warszawska). Zgodnie z tymi umowami uczelnie te utworzyły kierunki studiów w zakresie bezpieczeństwa systemów informatycznych. Ponadto uczelnie te podejmą współpracę naukową w zakresie cyberbezpieczeństwa (wspólne projekty i laboratoria badawcze). Politechnika Warszawska utworzyła Zakład Cyberbezpieczeństwa (http://cybsec.pl/

Ze względu na swoją rolę dydaktyczną środowisko naukowe zajmuje ważne miejsce w procesie edukacji, zwłaszcza względem studentów i w niektórych dziedzinach kształcenia specjalistycznego (np. studia podyplomowe). Niezależność zarówno uczelni prywatnych, jak i publicznych, pozwala im samodzielnie kształtować programy studiów. Ministerstwo Nauki i Szkolnictwa Wyższego nie może zatem narzucić im obowiązku prowadzenia zajęć związanych z cyberprzestępczością. Zauważa się jednak większą częstotliwość organizowania takich zajęć. Poza trzema uczelniami wymienionymi powyżej studia ze specjalizacją w dziedzinie cyberprzestępczości prowadzą na przykład: WAT – Wojskowa Akademia Techniczna w Warszawie, Akademia Ekonomiczna w Radomiu, WSB – Wyższa Szkoła Biznesu w Dąbrowie Górniczej, WSPiA – Wyższa Szkoła Prawa i Administracji w Rzeszowie. Inne uczelnie oferują studia podyplomowe w zakresie cyberprzestępczości. Są to między innymi: Politechnika Warszawska, AGH Uniwersytet Nauki i Technologii, Zachodniopomorska Szkoła Biznesu, Wyższa Szkoła Bezpieczeństwa w Poznaniu, Wyższa Szkoła Ekonomii i Informatyki w Krakowie, Uniwersytet Ekonomiczny we Wrocławiu, Politechnika Rzeszowska, AMW – Akademia Marynarki Wojennej w Gdyni. Stosunkowo szeroka oferta studiów podyplomowych w zakresie cyberprzestępczości wskazuje na rosnący w Polsce popyt na specjalistów w zakresie bezpieczeństwa sieci teleinformatycznych.

Ponadto w ramach studiów podyplomowych w Wyższej Szkole Policji w Szczytnie prowadzone są zajęcia z przedmiotów „Podstawy pozyskiwania i badania dowodów elektronicznych z nośników komputerowych” i „Cyberprzestępczość”. W ramach studiów pierwszego i drugiego stopnia w Wyższej Szkole Policji w Szczytnie prowadzone są zajęcia z następujących przedmiotów: „Metodyka prowadzenia śledztwa w sprawach związanych z nielegalnym kontentem (zawartością)”, „Pozyskiwanie i badanie dowodów elektronicznych z nośników komputerowych”, „Przestępczość w cyberprzestrzeni”, „Zwalczanie przestępczości w cyberprzestrzeni”.

Szkoła ta organizuje także co roku następujące międzynarodowe konferencje naukowo-praktyczne:

– Techniczne Aspekty Przestępczości Teleinformatycznej – od 1998 r. (250–300 uczestników); po każdej konferencji wydawany jest zbiór materiałów „Przestępczość teleinformatyczna”,
– Przestępczość z Wykorzystaniem Elektronicznych Instrumentów Płatniczych – w latach 2000–2013 (200–300 uczestników),

Sympozjum Analityków Kryminalnych z warsztatami; Dzień GIS-u – od 2002 r. (150–200 uczestników),

– Międzynarodowa Konferencja „Internetowe Naruszenia Własności Intelektualnej” – od 2014 r. (150–200 uczestników); po każdej konferencji wydawany jest zbiór materiałów „Internetowe Naruszenia Własności Intelektualnej”,
– Przeciwdziałanie i Zwalczanie Cyberprzestępczości – od 2015 r. (100 uczestników) we współpracy z Akademią Obrony Narodowej w Warszawie, Wojskową Akademią Techniczną w Warszawie i Akademią Marynarki Wojennej w Gdyni.

Oprócz regularnych kursów CEPOL organizuje także jednorazowe szkolenia. Funkcjonariusze zajmujący się zwalczaniem cyberprzestępczości, w tym wykładowcy w tych dziedzinach, często uczestniczą w szkoleniach organizowanych przez CEPOL, ECTEG i Europol / EC3. Pracownicy tych organów zapraszani są do udziału w różnych programach szkoleniowych lub seminariach i konferencjach na temat zwalczania cyberprzestępczości.

CEPOL

1. Działania stacjonarne (kursy, seminaria, konferencje) organizowane przez państwa członkowskie UE; w 2014 r. kilku funkcjonariuszy policji uczestniczyło w czterech działaniach dotyczących cyberprzestępczości, a w 2015 r. – w szeregu takich działań. Na 2016 r. zaplanowano przeprowadzenie pięciu takich działań. Polska złożyła wniosek i otrzymała dotację do kursu na temat służb pierwszego kontaktu i informatyki śledczej.

2. Kursy internetowe (seminaria internetowe)

W 2014 r. zorganizowano trzy seminaria internetowe, w których wzięło udział 31 uczestników z Polski. W 2015 r. zorganizowano siedem działań w tym zakresie. Ze względu na ograniczenia systemów informatycznych nie jest znana dokładna liczba uczestników z Polski, lecz zaangażowanie Polski nadal było duże. Na 2016 r. zaplanowano kolejne trzy seminaria internetowe. Ponadto w razie potrzeby można się zwrócić o zorganizowanie takiego działania ad hoc.

3. Program wymiany

W 2014 r. dwóch funkcjonariuszy z Polski wzięło udział w programie wymiany w dziedzinie cyberprzestępczości (między Komendą Wojewódzką Policji w Łodzi a Gruzją oraz Komendą Wojewódzką Policji w Poznaniu a Kosowem). W 2015 r. było pięć takich programów wymiany (Centralne Biuro Śledcze Policji – wymiana z Hiszpanią, Służba Celna – wymiana z Gruzją, Komenda Wojewódzka Policji w Krakowie – wymiana z Bułgarią oraz Biuro Kryminalne KGP – dwie osoby uczestniczyły w wymianie ze Słowacją). Program wymiany w 2016 r. także obejmie problematykę cyberprzestępczości.

4. Kursy internetowe

CEPOL opracował ponadto internetowy kurs na temat zwalczania cyberprzestępczości.

EUROPOL

W 2015 r. można było korzystać ze szkoleń organizowanych przez EC3/Europol/EUCTF/ECTEG w formie kursów, seminariów i konferencji, takich jak:

- posiedzenie Grupy Zadaniowej Unii Europejskiej ds. Zwalczania Cyberprzestępczości (EUCTF), 26–27 marca 2015 r. w Hadze – jeden uczestnik z Polski;
- konferencja poświęcona oszustwom internetowym związanym z użyciem kart płatniczych, 8–9 kwietnia 2015 r. w Hadze – jeden uczestnik z Polski;
- Pierwsze szkolenie Europolu w zakresie kryminalistyki w oszustwach związanych z użyciem kart płatniczych, 13–17 lipca 2015 r. w Avila (Hiszpania) – jeden uczestnik z Polski;

- seminarium eksperckie na temat wykorzystywania seksualnego dzieci, 1–3 czerwca 2015 r. w Hadze – jeden uczestnik z Polski;
- posiedzenie Eksperckiego Forum Kryminalistycznego, 8–9 czerwca 2015 r. w Hadze – jeden uczestnik z Polski;
- Posiedzenie platformy EMPACT w dziedzinie seksualnego wykorzystywania dzieci, 21 września 2015 r. w Hadze – jeden uczestnik z Polski;
- Konferencja „Analytical Vienna 2015", 21–23 września 2015 r. w Wiedniu – trzech uczestników z Polski;
- Konferencja poświęcona przemocy elektronicznej i cyberprzestępczości, 15–16 października 2015 r. w Igławie (Czechy) – dwóch uczestników z Polski;
- Posiedzenie Europejskiej Grupy ds. Szkolenia i Kształcenia w dziedzinie Cyberprzestępczości, 10–11 listopada 2015 r. w Hadze – jeden uczestnik z Polski.

Czterech policjantów wzięło udział w pilotażowych kursach organizowanych przez ECTEG: Programowanie w języku Python dla śledczych, (5–9 października 2015 r. w Dublinie); Złośliwe oprogramowanie – kurs dla śledczych (30 listopada – 4 grudnia 2015 r. w Dublinie); Analiza kryminalistyczna danych bieżących (19–23 października 2015 r. w Apeldoorn i 7–11grudnia 2015 r. w Wiesbaden).

Rozwój technologii informatycznych ma wpływ na codzienne życie obywateli i zwiększa działalność przestępców. W związku z tym w drugiej połowie 2014 r. w komendach wojewódzkich policji utworzono wydziały do walki z cyberprzestępczością. To z kolei doprowadziło do wzrostu zapotrzebowania na szkolenia dla policjantów.

Oprócz szkoleń organizowanych centralnie, Policja organizuje także szkolenia lokalne, za które odpowiedzialni są komendanci wojewódzcy policji (Komenda Stołeczna Policji w Warszawie) i które finansowane są przez wydziały finansowe komend wojewódzkich.

Kursy przeciwdziałania i zwalczania cyberprzestępczości prowadzone są przez komendy wojewódzkie, Komendę Główną Policji oraz Centrum Szkolenia Policji w Legionowie.

Dla policjantów zajmujących się cyberprzestępczością centrum to prowadzi także zajęcia w ramach specjalistycznego kursu w dziedzinie pozyskiwania informacji z internetu. Podczas tego kursu policjanci zdobywają wiedzę i umiejętności w zakresie walki z cyberprzestępczością. Roczny koszt kursu w 2014 r. wynosił 34 000 PLN (7824 EUR), a w 2015 r. – 25 000 PLN (5753 EUR).

Przykłady finansowania szkoleń/kształcenia przez fundusze UE oraz Norweski Mechanizm Finansowy

1. Komenda Wojewódzka Policji w Lublinie

Rok 2015 – szczegółowy program Komisji Europejskiej „Zapobieganie i walka z przestępczością" (ISEC): projekt „Międzynarodowa współpraca organów ścigania UE w walce z cyberprzestępczością" – 1 168 232 PLN (268 825 EUR)

2. Komenda Wojewódzka Policji w Łodzi

Rok 2014 – Regionalny Program Operacyjny Województwa Łódzkiego na lata 2007–2013: „Nowoczesne technologie w walce z przestępczością – doposażenie służb operacyjnych Policji województwa łódzkiego" Koszty szkolenia w ramach tego programu: 130 000 PLN (29 915 EUR), w tym 19 500 PLN (4 487 EUR) z budżetu państwowego i 110 500 PLN (25 427 EUR) z budżetu UE.

Rok 2015 – Norweski Mechanizm Finansowy na lata 2009–2014: projekt: „Bezpieczna Europa bez granic" (szkolenie obejmuje wykorzystanie technologii informatycznych w postępowaniu przygotowawczym, odzyskiwanie danych, hakowanie itp.) – 1 165 000 PLN

(268 081 EUR), w tym: 175 000 PLN (40 269 EUR z budżetu państwowego i 990 000 PLN (227 811 EUR) z budżetu UE.

3. Komenda Stołeczna Policji w Warszawie

Rok 2014 – Norweski Mechanizm Finansowy 2009–2014 – Zwiększenie zdolności policji w zapobieganiu i zwalczaniu przestępczości transgranicznej i zorganizowanej, w tym handlu ludźmi i migracji grup przestępczych poprzez utworzenie platformy edukacyjnej z wykorzystaniem e-learningu i nauki zdalnej – 55 975 PLN (12 881 EUR), w tym 8 396 PLN (1932 EUR) z budżetu państwowego i 47 579 PLN (10 948 EUR) z budżetu UE.

Rok 2015 – Norweski Mechanizm Finansowy 2009–2014 – Zwiększanie zdolności policji w zapobieganiu i zwalczaniu przestępczości transgranicznej i zorganizowanej, w tym handlu ludźmi i migracji grup przestępczych poprzez utworzenie platformy edukacyjnej z wykorzystaniem e-learningu i nauki zdalnej – 731 000 PLN (168 212 EUR), w tym 110 000 PLN (25 312 EUR) z budżetu państwowego i 621 000 PLN (142 900 EUR) z budżetu UE.

8.2 Podnoszenie świadomości

Ministerstwo Cyfryzacji

W ramach swoich działań koordynacyjnych Ministerstwo Cyfryzacji rozwija i rozszerza sieć pełnomocników do spraw bezpieczeństwa cyberprzestrzeni, przewidzianą w dokumencie strategicznym – Polityka ochrony cyberprzestrzeni. Obecnie sieć ta ma ok. 150 przedstawicieli w różnych urzędach administracji publicznej. Do tej pory Ministerstwo zorganizowało dla przedstawicieli sześć specjalistycznych szkoleń i zamierza zorganizować kolejne. Stworzyło ono specjalny portal dla pełnomocników, na którym znajdują się aktualne informacje na temat bezpieczeństwa cyberprzestrzeni. Ponadto Ministerstwo Cyfryzacji było współorganizatorem konferencji CYBERGOV 2015 poświęconej bezpieczeństwu informatycznemu w sektorze publicznym, która odbyła się 18 czerwca 2015 r.

Polityka ochrony cyberprzestrzeni przewiduje przeprowadzenie kampanii społecznej o charakterze edukacyjno-prewencyjnym, która skupi się na podnoszeniu świadomości w zakresie bezpiecznych metod korzystania z Internetu wśród dzieci, nastolatków, rodziców i nauczycieli. W dziedzinie tej ministerstwo organizowało konkursy na wykonanie zadania publicznego zgodnie z ustawą o działalności pożytku publicznego i o wolontariacie, które zaowocowały wieloma materiałami edukacyjnymi, np. na temat bezpiecznego korzystania z usług elektronicznych.

W ramach rozpowszechniania ważnych informacji na temat bezpieczeństwa sieci i informacji Ministerstwo Cyfryzacji zainicjowało także sporządzanie dokumentu zatytułowanego „Rekomendacje dla pełnomocników do spraw bezpieczeństwa cyberprzestrzeni" Rzeczypospolitej Polskiej, który został przyjęty przez rządową Radę ds. Cyfryzacji. Ministerstwo Cyfryzacji współpracuje z polskim członkiem Zarządu agencji ENISA, a uzyskane materiały i wskazówki agencji są rozpowszechniane wśród pełnomocników.

Działania mające podnieść świadomość, oraz działania edukacyjne w zakresie bezpiecznego korzystania z usług elektronicznych podejmowane są również przez inne organy krajowe, organy administracji publicznej, izby handlowe i instytuty badawcze, a także przez podmioty prywatne, w tym spółki telekomunikacyjne i banki. Program Operacyjny Polska Cyfrowa na lata 2014–2020 stwarza możliwość podniesienia świadomości obywateli, jeśli chodzi o bezpieczne korzystanie z internetu i usług elektronicznych, a także zwiększenia ich wiedzy o dostępnych narzędziach.

Policja

Policyjne środki prewencyjne mające na celu nauczenie społeczeństwa świadomego i odpowiedzialnego korzystania z internetu przyczyniają się do zmniejszenia zagrożeń. Nasilenie działalności Policji w tej dziedzinie pomaga zapobiegać zagrożeniom społecznym, ze szczególnym naciskiem na przyjęte priorytety.

Świadomość społeczeństwa podnosi się także za pośrednictwem mediów, z wykorzystaniem publikacji internetowych zamieszczonych na stronie policja.gov.pl. Znajdują się tam informacje na temat ochrony przed cyberatakami i zapobiegania im. Obok kampanii informacyjnych, takich jak „Stop dopalaczom” i „Stop cyberprzemocy”, organizowane są także na ten temat pogadanki w szkołach itp.

Ponadto funkcjonariusze z Wydziału do walki z cyberprzestępczością Komendy Stołecznej Policji w Warszawie w ramach współpracy z placówkami edukacyjnymi w Warszawie przeprowadzili 10 spotkań z nauczycielami, rodzicami, uczniami gimnazjów i szkół średnich. Tematem szkoleń było zapobieganie, identyfikacja i zwalczanie cyberprzestępczości. Ze względu na zapotrzebowanie na takie szkolenia w placówkach edukacyjnych Wydział do walki z cyberprzestępczością Komendy Stołecznej Policji w Warszawie planuje zorganizowanie kolejnych siedmiu warsztatów w 2016 r.

Badania naukowe i Naukowa Akademicka Sieć Komputerowa

Policja wraz z siecią NASK przeprowadziły kampanię informacyjną „CyberPol” poświęconą bezpieczeństwu dzieci w internecie, aby zwiększyć świadomość zagrożeń, jakie niesie ze sobą korzystanie z internetu. Szkolenia w tym zakresie odbyli policjanci z wydziałów prewencji, wydziałów kryminalnych i walki z cyberprzestępczością.

NASK organizuje wiele konferencji na temat bezpieczeństwa, w tym konferencję „SECURE", która jest najważniejszą konferencją w Polsce na temat cyberbezpieczeństwa. W przeszłości zorganizowano wiele innych działań, w tym także w ramach projektów unijnych. Ponadto NASK (CERT POLSKA) jest partnerem projektu CyberROAD prowadzonego w ramach siódmego programu ramowego. Projekt ten ma na celu ustalenie harmonogramu działań w zakresie cyberprzestępczości i cyberterroryzmu. NASK uczestniczy także w obchodach Europejskiego Miesiąca Bezpieczeństwa Cyberprzestrzeni (październik) organizowanych przez agencję ENISA. Obejmuje to publikowanie w sieci quizów wiedzy o cyberbezpieczeństwie oraz konkursów HackMe.

Szkoły

Aby zwiększyć wiedzę uczniów na temat cyberbezpieczeństwa, funkcjonariusze uczestniczą w prowadzeniu pogadanek w szkołach podstawowych i średnich. We współpracy z sektorem prywatnym i publicznym, w tym siecią NASK i Fundacją Dzieci Niczyje, co roku organizowany jest Dzień Bezpiecznego Internetu. W dniu tym organizowane są seminaria na ten temat dla nauczycieli i młodzieży. Rozpowszechniane są także audiowizualne materiały edukacyjne, które można wykorzystywać podczas zajęć szkolnych i do edukowania dzieci w przyszłości.

Podstawa programowa kształcenia ogólnego w poszczególnych rodzajach szkół obejmuje zajęcia informatyczne. Uczniowie dowiadują się o zagrożeniach wynikających z rozwoju technologii informacyjnej i powszechnego dostępu do informacji; zagrożeniach wynikających z uzależnienia od komputera; kwestiach etycznych i prawnych związanych z ochroną praw własności intelektualnej i ochroną danych oraz o zagrożeniach, jakie niesie ze sobą przestępczość komputerowa, a także o ochronie poufności i bezpieczeństwa oraz danych i informacji w komputerach i sieciach komputerowych. Ważnym zadaniem polskich szkół jest przygotowanie uczniów do życia w społeczeństwie informacyjnym. Nauczyciele różnych przedmiotów, także innych niż obowiązkowe zajęcia informatyczne, przygotowują uczniów do poszukiwania, organizowania i wykorzystywania informacji z różnych źródeł za pomocą technologii informacyjnych.

Fundacja Dzieci Niczyje

NASK wraz z innymi partnerami, np. Fundacją Dzieci Niczyje, poprowadził szereg projektów w zakresie podnoszenia świadomości, skierowanych zwłaszcza do młodej generacji. Fundacja Dzieci Niczyje przeprowadziła następujące projekty:

- Projekt edukacyjny Necio.pl, skierowany do dzieci w wieku 4–5 lat i ich rodziców. Głównym elementem projektu jest strona internetowa www.necio.pl z animacjami, grami i piosenkami dla dzieci, wyjaśniającymi zasady bezpieczeństwa w sieci i podstawy korzystania z komputera;
- Aplikacja BeSt – połączenie funkcji przeglądarki internetowej, wyszukiwarki i programu do kontroli rodzicielskiej. Przeznaczona dla dzieci w wieku 3–12 lat. Aplikacja ta bazuje na katalogu stron przyjaznych dzieciom, zebranych na portalu www.sieciaki.pl i obecnie zawiera setki stron sklasyfikowanych według wieku i tematyki. Będzie umożliwiać dzieciom wyszukiwanie i odwiedzanie tylko stron odpowiednich dla ich grupy wiekowej. Przeglądarkę BeSt można pobrać na stronach: www.best.fdn.pl;
- Projekt Dziecko w Sieci (http://dzieckowsieci.fdn.pl/) – podnoszenie świadomości dzieci, młodzieży i ich rodziców. Obejmuje np. kampanie informacyjne, organizację imprez i materiały informacyjne dla rodziców.

Kolejnym ważnym projektem jest Saferinternet.pl (http://saferinternet.pl/pl/) realizowany przez NASK i Fundację Dzieci Niczyje. Realizacja tego projektu rozpoczęła się w 1999 r. i ma na celu promowanie bezpieczniejszego korzystania z internetu i nowych technologii sieciowych, zwłaszcza przez dzieci.

Główne cele projektu to walka z treściami nielegalnymi, niechcianymi i szkodliwymi oraz podnoszenie świadomości. Projekt obejmuje szeroko zakrojone działania promujące bezpieczne i odpowiedzialne korzystanie z nowych mediów przez dzieci i młodzież. Wśród przykładów można wymienić:

Znajomi / nieznajomi? – kurs e-uczenia się dla szkół, „Dbaj o fejs" – kampania dla nastolatków na Facebooku, „Zostań znajomym swojego dziecka" – materiały edukacyjne dla rodziców.

8.3 Prewencja

8.3.1 Przepisy/strategie krajowe i inne środki

W rozporządzeniu w sprawie Krajowych Ram Interoperacyjności określone są minimalne wymagania dla systemów teleinformatycznych, w tym sposoby zapewnienia bezpieczeństwa przy wymianie informacji. Rozporządzenie to stanowi mianowicie, że podmioty realizujące zadania publiczne zobowiązane są do opracowania i wdrożenia (a także eksploatowania, monitorowania i doskonalenia) systemu zarządzania bezpieczeństwem informacji. Szczegółowo rozwinięty jest aspekt zarządzania bezpieczeństwem informacji oraz m.in. plany w zakresie działań takich, jak przeprowadzanie okresowych analiz ryzyka i podejmowanie działań minimalizujących to ryzyko.

Ten wymiar prewencyjny odzwierciedlony jest w Polityce ochrony cyberprzestrzeni. Celem strategicznym tej polityki jest uzyskanie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa. Cel ten jest realizowany poprzez stworzenie ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy użytkownikami polskiej cyberprzestrzeni Rzeczypospolitej Polskiej.

Ustawa o policji stanowi podstawę prawną dla inicjowania i organizowania działań, których celem jest zapobieganie przestępstwom, i powadzenia współpracy w tej dziedzinie z innymi organami państwa, samorządami i organizacjami społecznymi. Istnieje także szereg innych aktów prawnych regulujących konkretne czynności prawne, w tym dotyczące walki z cyberprzestępczością, takie jak Kodeks karny, ustawa z 2001 r. o ochronie baz danych, Prawo telekomunikacyjne z 2002 r., ustawa o zarządzaniu kryzysowym z 2007 r. i inne.

Przykłady działań prewencyjnych prowadzonych przez Policję we współpracy z innymi instytucjami to:

– „Bądź bezpieczny w sieci” - materiały edukacyjne „W Sieci” (Komenda Stołeczna Policji w Warszawie, Fundacja Dzieci Niczyje, Microsoft),
– „Cybernetyczna dżungla” (Wydział Kadr i Szkolenia Komendy Wojewódzkiej Policji w Szczecinie),
– „Służę, Szanuję” (Komenda Wojewódzka Policji w Gorzowie Wielkopolskim, Wojewódzki Ośrodek Metodyczny),
– „Bezpieczeństwo w sieci” – konkurs (Komenda Wojewódzka Policji w Białymstoku),
– „Stop cyberprzemocy” – Konkurs Małych Form Teatralnych i Krótkich Form Filmowych (Komenda Wojewódzka Policji w Gdańsku),
– „Odpowiedzialni rodzice - szczęśliwe dzieci”, program „Ucieczka w cyberprzestrzeń – przyczyny i konsekwencje uzależnienia” (Komenda Wojewódzka Policji w Olsztynie, Radio ZET Gold),
– „Uniwersytet Trzeciego Wieku”, Komenda Policji w Krakowie i Centrum Pedagogiki i Psychologii Politechniki Krakowskiej,
– „Uczyć, informować, zapobiegać. Otwarte szkoły – otwarte jednostki policji” (Komenda Wojewódzka Policji w Olsztynie, Sąd Okręgowy w Olsztynie, Kuratorium Oświaty, Kuratorska Służba Sądowa),
– „W sieci elektronicznej przemocy” – seminarium dla nauczycieli (Komenda Wojewódzka Policji w Katowicach),
– „Szybuj bezpiecznie w internetowej chmurze” – konkurs na przedstawienie infografiki dla rodziców i członków rodziny na temat skutecznego i bezpiecznego korzystania z internetu (Komenda Wojewódzka Policji w Kielcach i Świętokrzyskie Centrum Doskonalenia Nauczycieli, Urząd Marszałkowski Województwa Świętokrzyskiego),
– Konferencja „Prawne i psychologiczne aspekty cyberprzestępczości i uzależnień wśród dzieci i młodzieży” (Komenda Wojewódzka Policji w Rzeszowie, Samorząd Województwa Podkarpackiego).

W styczniu 2015 r. Prezes Urzędu Komunikacji Elektronicznej opublikował „Poradnik bezpiecznego korzystania ze środków komunikacji elektronicznej w cyberprzestrzeni”[29], aby propagować bezpieczne korzystanie z elektronicznych środków komunikacji w cyberprzestrzeni. Poradnik ma na celu przedstawienie zagrożeń, jakie czekają na każdego użytkownika cyberprzestrzeni, zalecanych środków bezpieczeństwa oraz najpopularniejszych sposobów ochrony danych i sprzętu. Zawiera on ważne informacje o mechanizmach zagrożeń, konsekwencjach skutecznych cyberataków oraz sposobach zabezpieczenia obiektów i systemów komputerowych. Można w nim znaleźć także zestaw informacji o najważniejszych technikach zabezpieczania komputerów wraz z praktycznymi wskazówkami ich stosowania.

W marcu 2015 r. wydano kolejny poradnik „Ochrona najmłodszych przed pornografią dostępną za pośrednictwem usług Premium Rate”[30]. Usługi Premium Rate, takie jak SMS Premium Rate, MMS Premium Rate i głosowe usługi specjalne, dostępne są za pośrednictwem tzw. numerów specjalnych, zwykle cztero- lub pięciocyfrowych wiadomości SMS/MMS rozpoczynających się od cyfry 7 lub 9. Za pośrednictwem usług Premium Rate najmłodsi użytkownicy mogą uzyskać dostęp do różnego rodzaju treści, w tym do treści erotycznych i pornograficznych. Ponadto niekontrolowane korzystanie z takich usług może prowadzić do wysokich opłat za usługi telefoniczne. Poradnik jest pomyślany tak, by uświadomić młodzieży, jakie zagrożenia niosą ze sobą usługi Premium Rate.

8.3.2 Partnerstwa publiczno-prywatne

Policja prowadzi projekty naukowe we współpracy z sektorem prywatnym (badacze z dziedziny wdrażania oprogramowania i narzędzi w celu zwalczania cyberprzestępczości z Akademii Górniczo-Hutniczej i Politechniki Warszawskiej) w ramach Polskiej Platformy Bezpieczeństwa Wewnętrznego. Projekty te dotyczą testowania w trybie offline danych testowych w miejscu wykonywania procedur i programu do analizy powiązań przestępczych.
Przykłady współpracy policyjnej z sektorem prywatnym obejmują:

[29] https://www.uke.gov.pl/files/?id_plik=18438
[30] https://www.uke.gov.pl/files/?id_plik=19323

- Wyższa Szkoła Policji w Szczytnie jest członkiem konsorcjum w siódmym programie ramowym: Comprehensive Approach to cyber roadMap coordINation and develOpment (CAMINO) – 2014-2016 O ROB 0003 03 001.
- Funkcjonariusze Policji byli członkami konsorcjum w projekcie CIPS/ISEC: Creation of a Polish Centre of Excellence for Research on Cybercrime - 2013-2014 HOME / 2012 / ISEC / INT / 4000003858.

W ramach współpracy z sektorem prywatnym planuje się zapewnienie bezpieczeństwa w niedawno stworzonych urządzeniach do programowania oraz uczestnictwo policji w tworzeniu nowych technologii dla sektora finansów. Wspólnie ze Związkiem Banków Polskich zostaną przeprowadzone testy, by zapewnić, że rozwiązania IT będą odporne na przestępstwa.

Utworzone w Wyższej Szkole Policji w Szczytnie Centrum Analityczno-Wywiadowcze i Doskonalenia Zwalczania Cyberprzestępczości ściśle współpracuje z ważnymi spółkami prywatnymi działającymi w cyberprzestrzeni, w tym z takimi jak: Allegro.pl, WPW, Fundacja Bezpieczna Cyberprzestrzeń, Matic, Scott Tiger S.A., Stow. Sygnał, ZPAV Warszawa, PwC, VSData i EY.

8.4 Wnioski

- Pracownicy sądownictwa i prokuratury oraz policjanci mają wiele możliwości szkoleń w dziedzinie cyberprzestępczości. Krajowa Szkoła Sądownictwa i Prokuratury oraz Wyższa Szkoła Policji w Szczytnie oferują im szeroką gamę specjalistycznych zajęć. Ponadto szkolenia w tej dziedzinie organizuje także CERT POLSKA.

- Krajowa Szkoła Sądownictwa i Prokuratury od 2009 r. organizuje szkolenia w zakresie zapobiegania i zwalczania cyberprzestępczości. Pomimo dobrej jakości prac prowadzonych w tej dziedzinie przez Krajową Szkołę Sądownictwa i Prokuratury, szkolenia te nie są obowiązkowe. Zespół oceniający poinformowano, że z powodu dużego obciążenia pracą sędziom i prokuratorom trudno jest uczestniczyć w nieobowiązkowych działaniach szkoleniowych.

- Brak jest ponadto sieci prokuratorów i sędziów zajmujących się sprawami z dziedziny cyberprzestępczości. Ponieważ tematyka cyberprzestępczości i zabezpieczania dowodów w środowisku IT stale się zmienia, dużą wartość mogłaby mieć wymiana najlepszych wzorców pomiędzy praktykami.

- Wyższa Szkoła Policji w Szczytnie prowadzi studia pierwszego i drugiego stopnia oraz studia podyplomowe w dziedzinie cyberbezpieczeństwa i zwalczania cyberprzestępczości. Oferuje także specjalistyczne szkolenia dla funkcjonariuszy wydziałów ds. walki z cyberprzestępczością oraz szkolenia z cyberprzestępczości dla kadetów Policji. Policja korzysta także z zewnętrznych możliwości szkoleń, np. oferowanych przez Europol czy CEPOL.

- Większość zajęć oferowanych przez Wyższą Szkołę Policji w Szczytnie jest obowiązkowych dla funkcjonariuszy Policji. Z drugiej strony jednak szkolenia przeznaczone dla sędziów i prokuratorów nie są obowiązkowe. Zespół oceniający uważa zatem, że przydatne byłoby wprowadzenie większej liczby szkoleń obowiązkowych, by zwiększyć wiedzę przedstawicieli organów zajmujących się cyberprzestępczością.

- Zapobieganiem cyberprzestępczości i podnoszeniem świadomości tego problemu zajmują się różne ministerstwa, które współpracują z organizacjami pozarządowymi, w większości w oparciu o granty unijne. Przed złożeniem ostatecznego wniosku wszystkie propozycje dotyczące kampanii informacyjnych są oceniane przez Ministerstwo Cyfryzacji, gdyż to ono decyduje, które z wniosków zostaną dopuszczone do ubiegania się o grant. Wydaje się jednak, że istnieje potrzeba koordynacji kampanii informacyjnych/prewencyjnych, nie tylko jeśli chodzi o ich adresatów (aby uniknąć sytuacji, w których niektóre dzieci będą uczestniczyły w kilku zajęciach, a inne w żadnych), lecz także jeśli chodzi o treść (aby nie przekazywać różnych ani sprzecznych informacji). Ponadto oceniający uważają, że dobrze byłoby włączyć w te kampanie przedstawicieli organów sądowych.

- Policja posiada wydział zajmujący się koordynacją wszystkich jej działań prewencyjnych. Brak jest jednak odrębnego budżetu przeznaczonego na działania prewencyjne i podnoszące świadomość.

9 UWAGI KOŃCOWE I ZALECENIA

9.1 Propozycje z Polski

Władze polskie uważają, że dla zapewnienia skutecznej walki z cyberprzestępczością zasadnicze znaczenie ma zapewnienie wystarczających zasobów finansowych, kadrowych i rzeczowych, a także odpowiednich kompetencji wszystkich organów ścigania i sądów (sędziów).

Przepisy i procedury w tej dziedzinie muszą iść w parze z szybkim rozwojem technologii teleinformatycznych, aby umożliwić monitorowanie zjawisk w dziedzinie cyberprzestępczości oraz zacieśnienie współpracy pomiędzy wszystkimi uczestnikami walki z cyberprzestępczością.
Ponadto ważne jest ujednolicenie międzynarodowych zasad walki z cyberprzestępczością oraz aspektów prawnych dotyczących dowodów elektronicznych i ich przekazywania.

Z perspektywy Policji ważne jest także rozszerzenie struktur zajmujących się walką z cyberprzestępczością oraz wyposażenie ich w nowe systemy teleinformatyczne, aby rozwijać przetwarzanie w oparciu o algorytmy w sprawach związanych z cyberprzestępczością, współpracować z sektorem publicznym i prywatnym na rzecz zwiększania bezpieczeństwa obywateli oraz zwiększać ich wiedzę i umiejętności w tej dziedzinie. Policja proponuje następujące działania, które można uznać za dobre praktyki:

– informowanie społeczeństwa o najnowszych aktualizacjach oprogramowania, w tym o aspektach inżynierii społecznej, np. kampanie informacyjne na stronie policji na temat złośliwego oprogramowania i praktyczne wskazówki dotyczące usuwania wirusów[31];
– wymiana informacji związanych ze ściganiem poprzez krajowych koordynatorów plików analitycznych; punkty kontaktowe: Terminal, Cyborg, Twins;

[31] http://www.policja.pl/pol/kgp/bsk/dokumenty/cyberprzestepczosc/79328,Uwaga-hakerzy-podszywaja-sie-pod-Policje.html. Ponadto informacje i kwestie związane cyberprzestępczością, a także instrukcje bezpiecznego korzystania z internetu zamieszczone są na stronie: http://www.policja.pl/pol/kgp/bsk/dokumenty/cyberprzestepczosc.

– bezpośrednia współpraca między punktami kontaktowymi Europolu, umożliwiająca dostęp do informacji o obecnych praktykach i identyfikację pojawiających się problemów;
– w ramach działań podnoszących świadomość prowadzonych przez Koalicję Antypiracką trzy organizacje:
– Związek Producentów Audio Video, Stowarzyszenie Sygnał i The Software Alliance (BSA) wspierają działania Policji w walce z naruszeniami praw własności intelektualnej. Policji przyznano „Złote Blachy" w uznaniu jej wkładu w zwalczanie przestępczości związanej z prawem autorskim.
– współpraca i wymiana informacji z sektorem prywatnym, by umożliwić organom ścigania uzyskiwanie informacji o obecnych tendencjach i zagrożeniach związanych z korzystaniem z nowych technologii przez przestępców w cyberprzestrzeni oraz o sposobach naruszania bezpieczeństwa;
– organizacja szkoleń i konferencji z udziałem funkcjonariuszy z wydziałów ds. walki z cyberprzestępczością komend wojewódzkich Policji oraz regionalnych zarządów Centralnego Biura Śledczego Policji, a także przedstawicieli sektora prywatnego i bankowego, co stanowi dobrą okazję do zapoznania się z istniejącymi procedurami uzyskiwania i dostarczania informacji, przedstawienia narzędzi i rozwiązań oraz wymiany metod i technik sprawnej walki z cyberprzestępczością;
– uczestnictwo w wielu specjalistycznych kursach z zakresu informatyki śledczej i odzyskiwania danych;

Warto rozważyć utworzenie – oprócz zespołów reagowania na incydenty komputerowe (CSIRT), które gromadzą dane na temat zagrożeń i luk oraz wydają wskazówki w zakresie bezpieczeństwa informatycznego – jednostek ds. bezpieczeństwa sieci i informacji dla sektora cywilnego, a także wyspecjalizowanych jednostek do zwalczania cyberprzestępczości i do cyberobrony.

Głównymi problemami wymienionymi przez Policję były:

- kryptowaluta Bitcoin;
- sieć TOR – ukryta tożsamość;
- inne środki anonimizujące – serwery proxy itp.;
- przepisy międzynarodowe – brak jednolitych systemów prawnych w państwach członkowskich;
- bezpieczeństwo danych w chmurze – dane użytkownika mogą być oferowane dobrowolnie, gdyż zlokalizowane są poza Polską;
- brak wykwalifikowanej kadry;
- wysokie koszty szkoleń;
- standaryzacja programu prewencji.

9.2 Zalecenia

Jeśli chodzi o praktyczne wykonanie i funkcjonowanie decyzji ramowych i dyrektyw, zespół ekspertów biorący udział w ocenie Polski mógł wydać zadowalającą opinię systemu funkcjonującego w Polsce.

Polska powinna powrócić do zaleceń zawartych w niniejszym sprawozdaniu w terminie 18 miesięcy od oceny i poinformować o poczynionych postępach Grupę Roboczą do Spraw Ogólnych, w tym Oceny (GENVAL).

Zespół oceniający uznał za stosowne przedstawić polskim władzom szereg propozycji. Ponadto w związku z różnymi dobrymi praktykami poczyniono zalecenia skierowane do UE oraz jej instytucji i agencji, w szczególności Europolu.

9.2.1 Zalecenia dla Polski

1. Polska powinna rozważyć utworzenie mechanizmu generującego ustandaryzowane statystyki dotyczące postępowań przygotowawczych, postępowań sądowych, wyroków skazujących i odnotowanych incydentów związanych z cyberprzestępczością; (por. pkt 3.3.2 i 3.5)
2. Polska powinna zacieśnić współpracę pomiędzy różnymi organami zajmującymi się cyberprzestępczością i wyznaczyć jeden organ, który będzie miał uprawnienia niezbędne do wydawania wskazówek organom zajmującym się cyberbezpieczeństwem i ich realizacji. (por. pkt 4.3, 4.4.1 i 4.5)
3. (por. pkt 4.3, 4.4.1 i 4.5) Polskę zachęca się do wyznaczenia krajowego zespołu CERT na szczeblu centralnym, który mógłby podjąć się koordynacji działań innych takich zespołów (CERT.GOV.PL, CERT.PL itp.). (por. pkt 4.3 i 4.5)
4. Polska powinna rozważyć utworzenie krajowej bazy danych dotyczącej pornografii dziecięcej wykorzystującej funkcje haszujące i inne techniki pozwalające uniknąć konieczności ręcznej oceny każdego pliku i ułatwić identyfikację ofiar. (por. pkt 6.2.1 i 6.4)
5. Polska powinna rozważyć utworzenie sieci umożliwiającej prokuratorom wymianę poglądów i optymalnych rozwiązań w dziedzinie cyberprzestępczości. (por. pkt 8.1 i 8.4)
6. Polska powinna rozważyć możliwość wprowadzenia większej liczby obowiązkowych szkoleń dla prokuratorów i sędziów zajmujących się cyberprzestępczością. (por. pkt 8.1 i 8.4)
7. Polskę zachęca się do skoordynowania różnych kampanii informacyjnych i kampanii prewencyjnych, które obecnie prowadzone są odrębnie przez Ministerstwo Cyfryzacji, Ministerstwo Edukacji, policję i inne podmioty. (por. pkt 8.2 i 8.4)

9.2.2 Zalecenia dla Unii Europejskiej, jej instytucji i dla innych państw członkowskich

1. Państwa członkowskie powinny rozważyć utworzenie krajowych zespołów CERT (lub nadanie już istniejącym takim zespołom odpowiednich uprawnień) uprawnionych do gromadzenia i analizowania danych na temat incydentów cybernetycznych wymierzonych w domeny publiczne lub prywatne oraz zdolnych do reagowania na zagrożenia, opracowywania oprogramowania do wczesnego ostrzegania i prowadzenia specjalistycznych szkoleń na temat cyberprzestępczości i cyberbezpieczeństwa, takich jak działania prowadzone przez NASK (CERT POLSKA). (por. pkt 4.3, 4.4.1 i 4.5)
2. Państwom członkowskim zaleca się, by co roku sporządzały sprawozdania na temat panującej w ich kraju sytuacji w zakresie cyberbezpieczeństwa, tak jak czynią to Agencja Bezpieczeństwa Wewnętrznego i NASK w Polsce. (por. pkt 4.3 i 4.5)
3. Państwa członkowskie powinny rozważyć utworzenie w swoich organach ścigania wyspecjalizowanych jednostek do skuteczniejszego zwalczania cyberprzestępczości zarówno na szczeblu krajowym, jak i regionalnym/lokalnym, tak jak uczyniła to Policja w Polsce; (por. pkt 4.2 i 4.5)
4. Państwom członkowskim zaleca się, by opracowały narzędzia i środki mające chronić dzieci i młodzież przed ponowną wiktymizacją, tak jak czyni to Fundacja Dzieci Niczyje. (por. pkt 6.2.1 i 6.4). (por. pkt 6.2.1 i 6.4)
5. Państwom członkowskim zaleca się, by wykorzystywały partnerstwa publiczno-prywatne do nawiązania lub wzmocnienia współpracy z sektorem finansowym w zwalczaniu cyberprzestępczości, tak jak w Polsce ma to miejsce w przypadku Związku Banków Polskich. (por. pkt 6.3.2 i 6.4)
6. Państwom członkowskim zaleca się, by zacieśniły współpracę z państwami sąsiadującymi, by wzmocnić swoją politykę w zakresie walki z cyberprzestępczością, tak jak uczyniła to Polska w stosunkach z państwami Partnerstwa Wschodniego. (por. pkt 7.1.1 i 7.6)
7. Państwa członkowskie powinny zbadać, czy wykonalne jest przeprowadzenie wspólnego szkolenia w zakresie cyberprzestępczości dla funkcjonariuszy Policji, prokuratorów i sędziów, tak jak w Polsce robi to Wyższa Szkoła Policji w Szczytnie we współpracy z Krajową Szkołą Sądownictwa i Prokuratury. (por. pkt 8.1 i 8.4)
8. UE powinna pracować nad rozwiązaniami pozwalającymi poprawić i przyspieszyć komunikację między państwami członkowskimi a państwami trzecimi, zwłaszcza jeśli chodzi o wymianę informacji operacyjnych oraz wnioski o wzajemną pomoc prawną. (por. pkt 7.3 i 7.6)
9. UE powinna rozważyć możliwość zawarcia umów z dużymi spółkami prywatnymi (np. Facebook, Google), aby ułatwić współpracę w sprawach karnych. (por. pkt 7.4 i 7.6)

Annex A: Programme for the on-site visit and persons interviewed/met

AGENDA		
DAY I	***01 FEB 2016***	
PM	Arrival of GENVAL experts in Warsaw	
17.30-18.30	Briefing with representatives of the Ministry of Interior and Administration	**Hotel bar**
DAY II	***02 FEB 2016***	
09.00 - 09.30	Transfer from the hotel to the Ministry of Digital Affairs	
09.30-11.00	National cyber security strategic and legislative framework – civilian sphere - Introduction by the Ministry of Digital Affairs - The Cyberspace Protection Policy of the Republic of Poland, actions planned in the future - Governmental Committee for Digitization, A Task Force for the security of cyberspace of the Republic of Poland – Ministry of Digital Affairs - National Critical Infrastructure Protection Programme – the Government Centre for Security - National Security Strategy of the Republic of Poland, the Doctrine of Cyber Security of the Republic of Poland – Ministry of Defense, the National Security Bureau - Questions and comments	**Ministry of Digital Affairs** 27 Królewska street Warsaw with representatives of: - the Government Centre for Security, - the National Security Bureau, - Ministry of Defense
11.00-11.15	***COFFEE BREAK***	
11.15-12.45	National cyber security strategic and legislative framework – civilian sphere - Act of February 17, 2005 on the computerization of the activities of entities performing public tasks, Regulation of the Council of Ministers of April 12, 2012 on the national interoperability frameworks – Ministry of Digital Affairs - Act of 16th July 2004 Telecommunications Law with corresponding regulations on security and integrity of telecommunications networks and services - the Polish Office of Electronic Communications - Act of August 29, 1997 on the protection of personal data - General Inspector for Personal Data Protection - Act of July 18, 2002 on the electronic provision of services – Ministry of Digital Affairs - Questions and comments	**Ministry of Digital Affairs** with representatives of: - the Polish Office of Electronic Communications - General Inspector for Personal Data Protection

12.45-13.15	***LUNCH***	
13.15-14.45	Operational aspects of cybersecurity, education, prevention, raising awareness - Main cyber incidents in domain .pl - Research and Academic Computer Network (NASK) - Cyber incidents identified by governmental CERT.GOV.PL – the Internal Security Agency (CERT.GOV.PL) - Prevention measures performed by the plenipotentiaries for cyberspace security – Ministry of Digital Affairs - Educational projects on information security financed by Ministry of Digital Affairs - Questions and comments	**Ministry of Digital Affairs** with representatives of: - Research and Academic Computer Network (NASK), - the Internal Security Agency (CERT.GOV.PL)
DAY III	***03 FEB 2016***	
08.30–09.00	Transfer from hotel to the National Police Headquarters (NPH)	
09.00-09.15	Official welcome by the Commanders of the Polish Police	**The National Police Headquarters**
09.15- 9.45	Introduction to the issue of combating cybercrime, including Police structure, international cooperation and cooperation with private sector and NGOs - Department for Fighting against Cybercrime, Criminal Service Bureau	148/150 Puławska street Warsaw
9.45-10.15	Combating child abuse on-line and off-line: Polish Police perspective and experience including international cooperation – Department for Fighting against Human Trafficking, Criminal Service Bureau	
10.15–10.45	The new modus operandi in the field of card fraud – Department for Fighting against Economic Crime, Criminal Service Bureau	
10.45-11.15	The Polish Banks Association (PBA) cooperation with Polish Police – vice president of the PBA	
11.15-11.30	***COFFEE BREAK***	
11.30-12.00	International information exchange with Europol and Interpol in the field of cybercrime - International Police Cooperation Bureau of the NPH	

12.00-12.30	The role of the Computer Emergency Response Team POL - CERT in the system of cybersecurity of Poland - Bureau of Communication and Information of the NPH	
12.30-13:00	The Police activities in preventing cyber threats – Prevention and Road Traffic Bureau of NPH	
13.00–13.30	The Police Academy in Szczytno input in combating cybercrime	
13.30-14.30	***LUNCH***	
14.30-15.00	Current challenges in the field of cybercrime combating and prevention – Prevention and Road Traffic Bureau of the NPH, Department for Fighting against Cybercrime, Criminal Service Bureau Discussion/Questions	
15.00-15.30	Transfer to the premises of the Department for Combating Cybercrime Central Bureau of Investigation of the Police	
15.30-16.00	*TASKS AND EQUIPMENT OF THE DEPARTMENT FOR COMBATING CYBERCRIME CENTRAL BUREAU OF INVESTIGATION OF THE POLICE* Presentation of the equipment and their tasks	**Central Investigation Bureau of the Police** Taborowa street Warsaw
16.00-16.30	*THE COOPERATION BETWEEN POLICE AND NGOS* Transfer to the Nobody's Children Foundation	
16.30-17.00	Presentation of „friendly rooms" and information about cooperation between the Nobody's Children Foundation and law enforcement in the scope of protecting children from abuse and providing help for abused children	**Nobody's Children Foundation** 12 Mazowiecka street Warsaw
17.00 – 17.30	Transfer to hotel	

DAY IV	***04 FEB 2016***	
9.15 – 10.45	Judicial and legislative framework for prevention and combating cybercrime	**Ministry of Justice** 11 Aleje Ujazdowskie street Warsaw
10.45 – 11.00	***COFFEE BREAK***	
11.00 – 11.30	Overview of courts statistics on cybercrime	
11.30 – 12.30	International judicial cooperation in the field of cybercrime	
12.30 – 13.30	***LUNCH***	
13.30 – 14.00	Overview of prosecution statistics on cybercrime	**Ministry of Justice**
14.00 – 15.30	Role of the Prosecution Service in combating cybercrime – presentation of case studies	with the representatives of **the Prosecution General**
15.30-15.45	***COFFEE BREAK***	
15.45 – 16.15	Judicial training on prevention and combating cybercrime	
19.30-22.00	***DINNER***	
DAY V	***05 FEB 2016***	
9.30-10.00	Start up with coffee	**Ministry of Interior and Administration** 5 Batorego street Warsaw
10.00-11.30	Closed session for Genval experts and/or possibility for extra exchange of views, interviews, etc.	
11.30	Transfer to the airport	

Annex B: Persons interviewed/met

Meeting 2 February 2016

Venue: Ministry of Digital Affairs, Warsaw

Person	Function/Organisation represented
Paweł Wiszniewski	Expert, National Security Bureau
Maciej Pyznar	Head of Unit, Government Centre for Security
Jarosław Łuba	Counsellor of the Minister, Ministry of Digital Affairs
Magdalena Wrzosek	Expert, Ministry of Digital Affairs
Maciej Groń	Director, Ministry of Digital Affairs
Marek Jurkiewicz	Head of Unit, Office of Electronic Communications
Paweł Makowski	Deputy Director, Inspector General for Personal Data Protection
Piotr Kijewski	Head of CERT POLSKA, NASK
Monika Pieniek	Chief expert, Ministry of Digital Affairs
Łukasz Olszewski	Senior expert, Ministry of Interior and Administration

Meetings 3 February 2016

Venue: National Police Headquarters, Warsaw

Person	Function/Organisation represented
Lt Col. Andrzej Szymczyk	Deputy Chief Commander of the Police
Col. Natalia Rost	Director of the Criminal Service Bureau of the NPH
Col. Renata Skawińska	Commander of the Central Investigation Bureau of Police
Maj. Irmina Gołebiewska	Deputy Director of the International Police Cooperation Bureau of the NPH
Lt Col. Marcin Golizda – Bliziński	Head of the Department for Fighting Against Cybercrime, Criminal Service Bureau of the NPH
Lt. Ph.D. Aneta Trojanowska	Deputy Head of the Department for Fighting Against Cybercrime, Criminal Service Bureau of the NPH
Lt Col. Jerzy Kosiński	Police Academy in Szczytno

Person	Function/Organisation represented
Cpt. Jarosław Kończyk	Department for Fighting Against Human Trafficking, Criminal Service Bureau of the NPH
2d WO Marta Krakowian	Department for Fighting Against Economic Crime, Criminal Service Bureau of the NPH
Maj. Marzena Kordaczuk- Wąs	Prevention and Road Traffic Bureau of the NPH
Lt. Marcin Kuskowski	IT and Communication Bureau of the NPH
Lt. Marcin Szlechta	Department for Combating Cybercrime, Central Investigation Bureau of Police
Gabriela Kuhn	Nobody's Children Foundation
Executive Vice President Polish Bank Association Ph.D. Mieczysław Groszek	The Polish Banks Association (PBA) cooperation with Polish Police
Martyna Różycka	Team Leader, Dyżurnet.pl
Łukasz Olszewski	Senior expert, Ministry of Interior and Administration
Izabela Iglewska	Senior expert, Ministry of Interior and Administration
Rafał Kierzynka	Judge, Department of Legislation, Ministry of Justice
Kuba Sękowski	Legal Counsel, Chief Expert, Department of Legislation, Ministry of Justice

Meeting 4 February 2016

Venue: Ministry of Justice, Warsaw

Person	Function/Organisation represented
Rafał Kierzynka	Judge, Department of Legislation, Ministry of Justice
Kuba Sękowski	Legal Counsel, Chief Expert, Department of Legislation, Ministry of Justice
Kazimierz Ujazdowski	Senior Expert, Department of Legislation, Ministry of Justice
Małgorzata Pawelec	Head of Coordination Unit, Department

Person	Function/Organisation represented
	of Legislation, Ministry of Justice
Magdalena Wójcikowska-Izdebska	Senior Expert, Department of Legislation, Ministry of Justice
Sławomir Piwowarczyk	Prosecutor, Prosecution General Office
Jacek Łazarowicz	Prosecutor, Prosecution General Office
Jacek Bilewicz	Prosecutor, Prosecution General Office
Konrad Gołębiowski	Prosecutor, Appellate Prosecutor's Office in Warsaw
Beata Klimczyk	Prosecutor, National School of Judiciary and Public Prosecution
Janusz Konecki	Judge, National School of Judiciary and Public Prosecution
Izabela Iglewska	Senior expert, Ministry of Interior and Administration
Łukasz Olszewski	Senior expert, Ministry of Interior and Administration
Lt Col. Marcin Golizda – Bliziński	Head of the Department for Fighting Against Cybercrime, Criminal Service Bureau of the NPH
Lt. Ph.D. Aneta Trojanowska	Deputy Head of the Department for Fighting Against Cybercrime, Criminal Service Bureau of the NPH

Meeting 5 February 2016

Venue: Ministry of Interior and Administration, Warsaw

Person	Function/Organisation represented
Łukasz Olszewski	Senior expert, Ministry of Interior and Administration
Izabela Iglewska	Senior expert, Ministry of Interior and Administration
Rafał Kierzynka	Judge, Department of Legislation, Ministry of Justice
Jarosław Łuba	Counsellor of the Minister, Ministry of Digital Affairs
Maj. Irmina Gołebiewska	Deputy Director of the International Police Cooperation Bureau of the NPH

Lt Col. Marcin Golizda – Bliziński	Head of the Department for Fighting Against Cybercrime, Criminal Service Bureau of the NPH
Lt. Ph.D. Aneta Trojanowska	Deputy Head of the Department for Fighting Against Cybercrime, Criminal Service Bureau of the NPH
Cpt. Jarosław Kończyk	Department for Fighting Against Human Trafficking, Criminal Service Bureau of the NPH
2d WO Marta Krakowian	Department for Fighting Against Economic Crime, Criminal Service Bureau of the NPH
Maj. Marzena Kordaczuk- Wąs	Prevention and Road Traffic Bureau of the NPH
Lt. Marcin Kuskowski	IT and Communication Bureau of the NPH
Jacek Bilewicz	Prosecutor, Prosecution General
Konrad Gołębiowski	Prosecutor, Appellate Prosecutor's Office in Warsaw
Sławomir Piwowarczyk	Prosecutor, Prosecution General

Załącznik C: Lista skrótów/wykaz terminów

Lista skrótów/wykaz terminów	Pełna nazwa w języku angielskim	Akronim w języku polskim lub oryginalnym	Pełna nazwa w języku polskim
CAM	Child Abuse Material	brak	materiały prezentujące niegodziwe traktowanie dzieci
CCP	Code of Criminal Procedure	KPK	Kodeks postępowania karnego
CI	Critical Infrastructure	IK	infrastruktura krytyczna
CSE	Child Sexual Exploitation	brak	wykorzystywanie seksualne dzieci
ENLETS	the European Network of Law Enforcement Technology Services	ENLETS	Europejska Sieć Służb Technologii Bezpieczeństwa Wewnętrznego
ENU	Europol National Unit	ENU	krajowa jednostka Europolu
GCD	Governmental Committee for Digitalization	KRMC	Komitet Rady Ministrów ds. Cyfryzacji
ISA	Internal Security Agency	ABW	Agencja Bezpieczeństwa Wewnętrznego
ISP	Internet Service Provider	brak	dostawca usług internetowych
MDA	Ministry of Digital Affairs	MC	Ministerstwo Cyfryzacji
MIA	Ministry of Interior and Administration	MSWiA	Ministerstwo Spraw Wewnętrznych i Administracji
MND	Ministry of National Defence	MON	Ministerstwo Obrony Narodowej
NASK	Research and Academic Computer Network	NASK	Naukowa i Akademicka Sieć Komputerowa
NBP	National Bank of Poland	NBP	Narodowy Bank Polski

Lista skrótów/wykaz terminów	Pełna nazwa w języku angielskim	Akronim w języku polskim lub oryginalnym	Pełna nazwa w języku polskim
NPH	National Police Headquarters	KGP	Komenda Główna Policji
NPIS	National Police Information System	KSIP	Krajowy System Informacyjny Policji
OEC	Office of Electronic Communications	UKE	Urząd Komunikacji Elektronicznej
PC	Penal Code	KK	Kodeks karny
PG	Prosecution General	PG	Prokuratura Generalna

Annex D: The Polish Legislation

The provisions of Penal Code (dated June 6, 1997) regarding combatting cybercrime:

Article. 190a.

§ 1. Who by the persistent harassment of another person or persons, its nearest stirs in her circumstances justified sense of danger or indeed violates her privacy, shall be punishable by imprisonment for 3 years.

§ 2. The same punishment shall be subject to the who, pretending to be another person, uses her image or other personal data for the purpose of causing her injury or personal.

§ 3. If the consequence of the Act specified in § 1 or 2 is make an attempt on one's life by victim, the offender shall be imprisonment from one year to 10 years.

§ 4. The prosecution of the offence specified in § 1 or 2 followed by at the request of the victim.

Article. 200.

§ 1. Who sexually communion with minors below 15 years or allow such person to another sexual act or brings it to undergo such an operation or to execute them, shall be punishable by imprisonment from 2 to 12 years

§ 3. Who juvenile less than 15 years presents a pornographic content or provides him with items of such a nature or disseminate pornographic content in such a way that such juvenile to become acquainted with them, shall be punishable by imprisonment for 3 years.

§ 4. The penalty referred to in section 3 shall be subject to, who to his sexual gratification, or sexual gratification of another person presents juvenile below 15 years implementation of the sexual act.

§ 5. The penalty referred to in section 3 shall be subject to, who runs the advertising or promotion of business of distributing pornographic content in such a way as to become acquainted with them juvenile below the age of 15.

Article. 200A.

§ 1. Who in order to commit the offences referred to in article 1. 197 § 3 paragraph 2 or article. 200, as well as the manufacture or the perpetuation of pornographic content, through an it system or telecommunications network contacts with minors below the age of 15, in order, by means of the introduction of it, exploiting an error or inability to comprehend the situation either by using the threat of unlawful, to meet with him, shall be punishable by imprisonment for 3 years.

§ 2. Who through the it system or telecommunications network juvenile below 15 years includes a proposal for associating, surrender or another sexual act or participate in production or perpetuating pornography, and tends to its implementation shall be subject to a fine, the penalty of restriction of liberty or imprisonment for 2 years.

Article. 200B

Who publicly propagates or applauds the behaviour of an paedophile, is subject to a fine, the penalty of restriction of liberty or imprisonment for 2 years.

Article. 202.

§ 1. Who publicly presents a pornographic content in such a way that it can impose their receipt to the person who you do not wish, shall be subject to a fine, the penalty of restriction of liberty or imprisonment for 2 years.

§ 3. Who to distribute produces, perpetuates or comes down, keeps or has or disseminates or presents pornography involving a minor or pornographic content related to the presentation of violence or handling the animal, shall be punishable by imprisonment from 2 to 12 years.

§ 4. Who perpetuates the pornography involving a minor, shall be punishable by imprisonment from one year to 10 years.

§ 4a. Who holds, has or obtains access to pornography involving a minor, shall be punishable by imprisonment from 3 months to 5 years.

§ 4b. Who produces, disseminates, shows, stores or have pornographic content depicting manufactured or processed image of a minor involved in the sexual act is subject to a fine, the penalty of restriction of liberty or imprisonment for 2 years.

§ 4 c. The penalty referred to in section 4b shall be subject to the who for the purpose of sexual gratification involved in pornographic presentations involving a minor.

§ 5. The Court may declare the forfeiture of tools or other objects, which served or were designed for committing the offences referred to in § 1-4b, even if they do not constitute the property of the offender.

Article. 256. §1. Whoever publicly promotes a fascist or other totalitarian regime, Member States or calls for hatred against the background of ethnic differences, ethnic, racial, religious, or due to the non-religion, is subject to a fine, the penalty of restriction of liberty or imprisonment for 2 years.

§ 2. The same punishment shall be subject to the who for distribution produces, perpetuates or comes down, acquires, stores, showcases, carries or transmits printing, recording or any other object containing the content referred to in § 1, or being a carrier of the symbolism of fascist, Communist or other totalitarian.

§ 3. Does not commit a crime the perpetrator of the criminal act referred to in

§ 2, if he is guilty of the Act in respect of the artistic, educational, scientific, or a collector's Edition.

§ 4. In the event of a conviction for an offence referred to in § 2, the Court shall order the forfeiture of the items referred to in § 2, even if they do not constitute the property of the offender.

Article 267.

§ 1. Whoever, without being authorised to do so, acquires information not destined for him, by opening a sealed letter, or connecting to a wire that transmits information or by breaching electronic, magnetic or other special protection for that information shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.

§ 2. The same punishment shall be imposed on anyone, who, in order to acquire information to which he is not authorised to access, installs or uses tapping, visual detection or other special equipment.

§ 3. The same punishment shall be imposed on anyone, who imparts to another person the information obtained in the manner specified in § 1 or 2 discloses to another person.

§ 4. The prosecution of the offence specified in § 1 – 3 shall occur on a motion of the injured person.

Article. 268.

§ 1. Who, without being entitled to do so, destroys, damages, deletes, or modifies the record material information or otherwise thwarts, or significantly impedes a person empowered to become acquainted with it, is subject to a fine, the penalty of restriction of liberty or imprisonment for 2 years.

§ 2. If the Act specified in § 1 applies to information on data medium, the perpetrator shall be subject to imprisonment for 3 years.

§ 3. Who, while allowing to act referred to in § 1 or 2, causing significant damage to property, shall be punishable by imprisonment from 3 months to 5 years.

§ 4. The prosecution of the offence specified in § 1-3 followed by at the request of the victim.

Article. 268a.

§ 1. Who, without being entitled to do so, destroys, damages, removes, alters, or impedes the access to computer data or substantially interferes with or prevents automatic processing, collection or transmission of such data, shall be punishable by imprisonment for 3 years.

§ 2. Who, while allowing to act referred to in § 1, causing significant damage to property, shall be punishable by imprisonment from 3 months to 5 years. § 3. The prosecution of the offence specified in § 1 or 2 followed by at the request of the victim.

Article. 269.

§ 1. Whoever destroys, damages, deletes, or modifies the information data of particular interest to national defence, security, the functioning of the Government, other State body or institution of the State or local government or disrupts or prevents automatic processing, collection or transmission of such data, shall be punishable by imprisonment from 6 months to 8 years.

§ 2. The same punishment shall be subject to, who may be an act referred to in § 1, destroying or replacing data media information or destroying or damaging the device for automatic processing, storage or transmission of computer data.

Article. 269a.

Who, without being entitled to do so, by transmission, destruction, removal, damage, making it more difficult to access or change the data, it substantially interferes with the work of the computer system or the ICT network, shall be punishable by imprisonment from 3 months to 5 years.

Article. 269b.

§ 1. Who produces, acquires, disposes of or make available to others the device or computer programs designed for committing the offence referred to in article 1. 165 section 1, paragraph 4, art. 267 § 3, art. section 268a 1 or § 2 in conjunction with § 1, art. 269 section 2(1) or article. 269a, as well as computer passwords, access codes or other data used to access information stored on a computer system or network communication shall be subject to imprisonment for 3 years.

§ 2. In the event of a conviction for an offence referred to in paragraph 1, the Court shall order the forfeiture of the items specified therein, and declare their forfeiture, if they do not constitute the property of the offender.

Article. 271.

§ 1. A public officer or other person authorized to issue a document, which certifies the truth in it as to the circumstances of the relevant law, punishable by imprisonment from 3 months to 5 years.

§ 2. In the case of a minor, the perpetrator shall be subject to a fine or penalty of restriction of liberty.

§ 3. If the perpetrator of an act may be referred to in paragraph 1 in order to achieve material advantage or personal, shall be punishable by imprisonment from 6 months to 8 years.

Article. 286.

§ 1. Who, in order to achieve the material benefits, brings another person into the negative regulation of their own or someone else's property with the introduction of its error or exploiting error or inability to sound understanding of action, shall be punishable by imprisonment from 6 months to 8 years. § 2. The same punishment shall be subject to who requests the material benefits in return for reimbursement of wrongly took things. § 3. In the case of a minor, the perpetrator shall be subject to a fine, the penalty of restriction of liberty or imprisonment for 2 years.

§ 4. If the Act specified in § 1-3 has been committed to the detriment of the person nearest, prosecution follows at the request of the victim.

Article 287.

§ 1. Whoever, in order to gain material benefits, affects automatic processing or transmitting information, or changes or deletes record or introduces a new record on an electronic information carrier, without being authorised to do so, shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

§ 2. In the event that the act is of a lesser significance, the perpetrator shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to one year.

§ 3. If the fraud has been committed to the detriment of a next of kin, the prosecution shall occur on a motion of the injured person.

Article 294.

§ 1. Whoever commits the offence specified in Article 278 § 1 or 2, Article 284 § 1 or 2, Article 285 § 1, Article 286 § 1, Article287 § 1, Article 288 § 1 or 3, or in Article 291 § 1, with regard to property of considerable value shall be subject to the penalty of deprivation of liberty for a term of between 1 and 10 years.

§ 2. The same punishment shall be imposed on the perpetrator who commits the offence specified in § 1 with regard to a property of significant cultural value.

Article 310.

§ 1. Whoever counterfeits or alters Polish or foreign money, other legal tender, or a document which entitles one to obtain a sum of money or contains an obligation to pay capital, interest, share of profits, or verifies a share in a company, or whoever removes a sign of cancellation from money, other legal tender or from such document shall be subject to the penalty of deprivation of liberty for a minimum term of 5 years or the penalty of deprivation of liberty for 25 years.

§ 2. Whoever releases into circulation money or other legal tender or document as specified in § 1 or for such purpose receives, stores, transports, carries, dispatches it or assists in selling or concealing it shall be subject to the penalty of deprivation of liberty for a term of between 1 and 10 years.

§ 3. In the event that the act is of a lesser significance, the court may apply an extraordinary mitigation of the penalty.

§ 4. Whoever makes preparations to commit the offence specified in § 1 or 2 shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

List of Polish provisions corresponding with crimes defined in Table 2 of the questionnaire – annex to the answer to question 2A.1 with comments.		
Acts unique to information systems, in particular those related to cyber attacks	Illegal access to information system	PC, Art. 267 (1): 1. Whoever, without being authorised to do so, acquires information not destined for him, by opening a sealed letter, or connecting to a wire that transmits information or by breaching electronic, magnetic or other special protection for that information shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.
		Comments: This offence may only be committed intentionally (both direct intent or potential intent are possible). Penalties for committing an offence defined in art. 267 (1) of the PC are: fine, the penalty of restriction of liberty (between 1 month and 3 years) or the penalty of deprivation of liberty (from 1 month) for up to 2 years. Attempt to commit an offence defined in art. 267 (1) of the PC is punishable.
	Illegal system interference	PC, Art. 269a: Whoever, without being authorised to do so, by transmitting, damaging, deleting, destroying or altering information data, significantly disrupts a computer system or telecommunications network shall be subject to imprisonment for three months to five years.
		Comments: This offence may only be committed intentionally (both direct intent or potential intent are possible). Penalty for committing an offence defined in PC, Art. 269a is a deprivation of liberty between 3 months and 5 years. Attempt to commit an offence defined in PC, Art. 269a is punishable.
	Illegal data interference	PC, Art. 268a: 1. Whoever, without being authorised to do so, destroys, damages, deletes or alters or hinders access to information data, or who hinders or prevents the automatic collection and transmission of such data shall be subject to imprisonment for up to three years. 2. Whoever, by committing the offence specified in § 1, causes a significant loss of property shall be subject to imprisonment for between three months and five years.
		Comments: This offences may only be committed intentionally (both direct intent or potential intent are possible). Penalty for committing an offence defined in PC, Art. 268a (1) is a deprivation of liberty (from 1 month) for up to 3 years and, in case of qualified type defined

		in PC, Art. 268a (2) the penalty is a deprivation of liberty between 3 months and 5 years. Attempt to commit an offences defined in PC, Art. 268a is punishable.
	Illegal interception of computer data	Same as illegal access to information system.
	Misuse of devices - production, distribution, procurement for use, import or otherwise making available or possession of computer misuse tools	PC, Art. 269b.1: 1. Whoever creates, obtains, transfers or allows access to hardware or software adapted to commit the offences specified under Article 165 § 1 section 4, Article 267 § 2, Article 268a § 1 or § 2 in connection with § 1, Article 269 § 2 or Article 269a, including also computer passwords, access codes or other data enabling access to the information collected in the computer system or telecommunications network shall be subject to imprisonment for up to three years.
		Comments: This offence may only be committed intentionally (both direct intent or potential intent are possible). Penalty for committing an offence defined in PC, Art. 269b is a deprivation of liberty (from 1 month) for up to 3 years. Attempt to commit an offence defined in PC, Art. 269b is punishable. Forfeiture of assets: PC, Art. 296b (2) In the event of a conviction for the offence specified in § 1, the court orders the forfeiture of the items referred to therein, and may order the forfeiture even if they do not constitute the property of the offender.
Content-related acts, in particular those related to child sexual abuse online and child pornography	Computer-related production, distribution or possession of child pornography	PC, Art. 202 (1), (3), (4a) and (4b) 1. Whoever publicly presents pornographic material in such a manner that it is imposed upon a person who may not wish so shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to one year. 3. Whoever for the purpose of dissemination produces or imports or stores, possesses, distributes or presents pornographic material, in which minors participate, or pornographic material associated with the use of violence or the use of an animal shall be subject to the penalty of the deprivation of liberty for a term of between 2 and 12 years. 4a. Whoever stores, possesses or obtains access to pornographic content involving a minor shall be punished by the deprivation of liberty for a term of 3 months to 5 years. 4b. Whoever manufactures, distributes, presents, stores

		or possesses pornographic material containing a generated (fabricated) or transformed (processed) image of a minor image of a minor participating in sexual activity shall be punishable by a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to two years.
		Comments: This offences may only be committed intentionally (both direct intent or potential intent are possible). However, the offence defined in PC, Art. 202 (3) requires a direct intent – acting for the purpose of dissemination. Penalty for committing an offences related to child sexual abuse and exploitation vary between particular types of offences. Attempt to commit an offences defined in PC, Art. 202 is punishable. According to the nomenclature of the PC a person who has not reached 18 years is described as a "minor". Term "child" is not used for this purpose.
	Computer-related solicitation or "grooming" of children	PC, Art. 200a: 1. Whoever, in order to commit the offence specified in Article 197 § 3 section 2 or Article 200, as well as for the purpose of producing or preserving pornographic materials, by an information system or telecommunications network, establishes a connection with a minor under the age of 15, with the intention of using deceit or an illegal threat to meet with him or her, shall be subject to imprisonment for up to three years. 2. Whoever, through an information system or telecommunications network, makes an offer to a minor under the age of 15 of sexual intercourse, submission or performance to another sexual act, or participation in the production or preservation of pornographic material and intends to carry through this offer, shall be subject to a fine, the restriction of liberty or imprisonment for up to two years.
		Comments: This offences may committed intentionally (a direct intent – a purpose of producing or preserving pornographic materials – is required under PC, Art. 200a (1), and a material act leading to meeting with a child is required under PC, Art. 200a (2)). Penalty for committing an offence defined in art. 200a (1) is imprisonment for up to three years, and relation to the offence defined in art. 200a (1) – a fine, the restriction of liberty or imprisonment for up to two years. Attempt to commit aforementioned offences is punishable. According to the nomenclature of the PC a person who has not

			reached 18 years is described as a "minor". Term "child" is not used for this purpose.
Acts where computer/IT systems were involved as tool or target, in particular online card fraud	Computer-related	forgery	The conduct described as "computer-related forgery" falls under definition of forgery set out in the PC, Art. 270 (1) – material forgery and Art. 271 (1) – intellectual forgery: PC, Art. 270 (1): 1. Whoever forges, counterfeits or alters a document with the intention of using it as authentic, or who uses such a document as authentic, is liable to a fine, the restriction of liberty or imprisonment for between three months to five years. PC, Art. 271 (1): 1. A public official, or another person authorised to issue a document, who certifies an untruth therein, in circumstances of legal significance, is liable to imprisonment for between three months and five years.
			Comments: This offences may committed intentionally (a direct intent – an aim to use a forged document as it was authentic – is required under PC, Art. 270 (1)). Penalty for committing an offence defined in art. 270 (1) and 271 (1) of the PC is a deprivation of liberty between 3 months and 5 years. In case of forgery (PC, Art. 2710 (1)) penalties of fine and restriction of liberty are also foreseen. Attempt to commit aforementioned offences is punishable. The term "document" (used in PC, Art. 270 and Art. 271) is defined in the PC, Art. 115 (14) as: an object or record on a computer data carrier to which is attached a specified right, or which, in connection with the subject of its content, constitutes evidence of a right, a legal relationship or a circumstance that may have legal significance.
		fraud	Article 287 (1) of the PC: 1. Whoever, in order to gain material benefits, affects automatic processing or transmitting information, or changes or deletes record or introduces a new record on an electronic information carrier, without being authorised to do so, shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years
			Comments: This offence may only be committed intentionally (a direct intent – an aim of gaining material benefits is required). Penalty for committing an offence defined in art. 287 (1) of the PC is a deprivation of liberty between 3 months and 5 years. Attempt to commit an offence defined in art. 287 (1) of the PC is punishable. Privileged type of the offence: PC, Art. 287(2) § 2. In the event that the act is of a lesser significance, the perpetrator shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to one year.

	Computer-related identity offences	The conducts described as “computer-related identity offences” fall under the definition of forgery or fraud.
	Sending or controlling sending of Spam	Art 24 (1) of the Act of 18th of June 2002 on services provided through ICTs: Who sends by means of electronic communication unsolicited commercial, shall be subject to a fine.
		Comments: The conduct defined in aforementioned provision is a petty offence. The attempt to commit this offence is not punishable.