ARCHIWUM KRYMINOLOGII, T. XXVIII, 2005-2006
PLISSN 0066-6890

ANDRZEJ ADAMSKI, JERZY KOSIŃSKI

OSZUSTWA INTERNETOWE W OCENIE POLSKICH I AMERYKAŃSKICH POLICJANTÓW

Ściganie przestępstw popełnianych z wykorzystaniem internetu i innych technologii informacyjnych jest zadaniem skomplikowanym, które wymaga od funkcjonariuszy policji odpowiedniego przygotowania, potrzebnego często już w chwili przyjmowania zawiadomienia o popełnieniu cyberprzestępstwa. Czy i na ile dysponują nim polscy policjanci? Pytanie to stanowiło impuls do przeprowadzenia badań, których wyniki przedstawia niniejsze opracowanie.

Pytanie, czy polscy policjanci są przygotowani do prowadzenia postępowań karnych w sprawach przestępstw popełnianych z wykorzystaniem internetu, może wydawać się retoryczne na tle coraz częstszych doniesień prasowych o zatrzymaniu przez policjantów handlarzy cyberpornografią dziecięcą[1], aresztowaniu grupy hakerów[2] lub ujęciu dzięki internetowi podejrzanego o dokonanie zabójstwa[3]. Trzeba jednak mieć na uwadze okoliczność, że relacjonowane przez media zdarzenia dotyczą wyłącznie czynów, które zostały ujawnione i wywołały reakcję organów ścigania prowadzącą do zatrzymania osób podejrzanych o popełnienie przestępstwa. Chodzi więc o zdarzenia stanowiące niewielką, szacowaną na około 5-10%, część zjawiska cyberprzestępczości, które tak jak przestępczość konwencjonalna charakteryzuje się dużą „ciemną liczbą" czynów nieujawnionych[4]. Enuncjacje prasowe o sukcesach organów ścigania w walce z cyberprzestępczością lub dane statystyki policyjnej wskazujące na 70-procentową wykrywalność oszustw komputerowych[5] nie mogą zatem uzasadniać uogólnień, że policja kontroluje sytuację i z reguły skutecznie reaguje na napływające do niej zgłoszenia o łamaniu prawa w cyberprzestrzeni. Nie wiadomo bowiem, jaki jest faktyczny zakres tej kontroli nad zjawiskiem, które w jeszcze większym stopniu niż przestępczość tradycyjna wymyka się percepcji społecznej (Goodman 1997, s. 478 i nast.).

Zagadnienie ścigania przestępstw związanych z technologiami informacyjnymi jest w literaturze kryminologicznej tematem stosunkowo licznych opracowań teoretycznych[6], rzadziej stanowi przedmiot badań. Autorzy zajmujący się tą problematyką

---

[1] „Podkarpaccy policjanci zatrzymali pedofilów", *Gazeta Wyborcza* z 7 czerwca 2004, http://miasta.gazeta.pl/rzeszow/1,34975,2112271.html#dalej.

[2] „Policja złapała grupę polskich hakerów", PAP 14 lutego 2004, http://serwisy.gazeta.pl/metro-on/1,0,1914234.html.

[3] „Dzięki internetowi policjanci ujęli podejrzanego o zabójstwo", PAP 16 kwietnia 2004, http://dziennik.pap.com.pl/index.html?dzial=INT&poddzial=POL&id_depeszy= 14095470

[4] Szerzej na ten temat: Adamski, Warszawa 2000, s. 10-24; Kabay 2001.

[5] Komenda Główna Policji, *Statystyka - przestępstwa komputerowe,* http://www.kgp.gov.pl.

[6] Zob. Smith, Grabosky, Urbas 2004 i powołaną tam literaturę.

są zgodni, że ściganie cyberprzestępstw nie należy do priorytetowych zadań policji w żadnym państwie. Sugerują, że jest to prawidłowość uniwersalna o podobnych uwarunkowaniach, które mają charakter zarówno subiektywny, jak i obiektywny. Na przykład mało entuzjastyczne nastawienie policjantów do ścigania cyberprzestępstw tłumaczy się ich „technofobią", wynikającą z braku odpowiedniej wiedzy informatycznej i umiejętności korzystania ze sprzętu komputerowego (Huey 2002). Źródeł niechęci do zajmowania się cyberprzestępstwami upatruje się też w rozpowszechnionych w środowisku funkcjonariuszy policji stereotypach myślowych, do których zalicza się popularne wśród nich przekonanie, że nie są to „prawdziwe" przestępstwa (Goodman 1997). Z kolei niska ranga przestępstw komputerowych na liście priorytetów organów ścigania jest przypisywana ich technicznej naturze, trudnościom związanym z identyfikacją sprawców, brakowi wystarczających środków finansowych na szkolenie funkcjonariuszy i utrzymanie wyspecjalizowanych jednostek, wysokim kosztom prowadzonych postępowań, tolerancyjnemu stosunkowi opinii publicznej do technoprzestępców i łagodnym karom wymierzanym im przez sądy (ibidem; Davis 1998, s. 48; Sommer 2004, s. 10). Niektóre z tych intuicyjnych wyjaśnień i zdroworozsądkowych hipotez znajdują potwierdzenie w oficjalnych statystykach[7] oraz badaniach kryminologicznych (Correia, Bowling 1999; Hinduja 2004).

Cyberprzestępczość jest zjawiskiem relatywnie nowym, nic więc dziwnego, że pozostaje poza głównym nurtem zainteresowań badawczych kryminologii (Adamski 1999, s. 214). Eksploracja tego problemu skupia się najczęściej na aspektach fenomenologicznych, dotyczy pomiaru rozpowszechnienia i opisu jego nieustannie ewoluujących przejawów, przybierających niekiedy postać autentycznie wirtualnych zachowań i interakcji przestępczych (Ying-Chien Chen i in. 2005, s. 246). Ciągle jeszcze nieliczne badania nad ściganiem przestępstw internetowych stanowią domenę kryminologii amerykańskiej. Najczęściej stosowaną w tym celu metodą badawczą jest ankietyzacja funkcjonariuszy policji. Zadawane respondentom pytania odwołują się do ich zawodowych doświadczeń związanych z przestępstwami teleinformatycznymi. Dotyczą trudności i problemów, na jakie napotyka przeciwdziałanie temu zjawisku oraz postulowanych sposobów ich rozwiązywania. Gromadzone w ten sposób informacje są publikowane w postaci syntetycznych raportów i stanowią podstawę formułowanych tam wniosków i zaleceń dotyczących zmian organizacyjnych i prawnych, jakie należałoby wprowadzić w celu zwiększenia skuteczności działania organów powołanych do walki z cyberprzestępczością (Stambaugh i in. 2000).

Charakterystyczna dla Stanów Zjednoczonych i wielu innych państw metoda kształtowania polityki przeciwdziałania różnym formom przestępczości za pomocą narzędzi i technik badawczych właściwych kryminologii jest niestety rzadko stosowana w Polsce[8]. Ta gorzka konstatacja była impulsem do sięgnięcia po wzory amerykańskie i wypróbowania wykorzystywanych tam z powodzeniem instrumentów

[7] Przykładem mogą być dane statystyczne dotyczące Zjednoczonego Królestwa, w którym na 140 tys. policjantów tylko 1000 (0,7%) przeszło specjalistyczne szkolenie w zakresie ścigania cyberprzestępstw, a 250 stanowi personel wyspecjalizowanych jednostek policji do walki z przestępstwami komputerowymi („Skills not money needed to fight cybercrime", *ZD Net UK*, 18 maja 2004, http://news.zdnet.co.uk/intemet/security/0,39020375,3915513 8,00.htm).

[8] Przyczyny i następstwa tego stanu rzeczy zasługują na odrębną analizę, która nie mieści się ramach niniejszego opracowania.

badawczych w polskich warunkach. Źródłem inspiracji był projekt badawczy zrealizowany w Stanach Zjednoczonych w celu oceny przygotowania policjantów amerykańskich do ścigania oszustw popełnianych z wykorzystaniem intemetu. Na jego podstawie opracowano kwestionariusz ankiety, przy użyciu którego przeprowadzono badania polskich policjantów. Przyjęto założenie, że stanowić oni będą „grupę eksperymentalną", której rozkład odpowiedzi na zawarte w kwestionariuszu ankiety pytania zostanie porównany z odpowiedziami „grupy kontrolnej", składającej się z ich amerykańskich kolegów. W ten sposób starano się osiągnąć cel badań, jakim było uchwycenie podobieństw i różnic w podejściu polskich i amerykańskich policjantów do problemu oszustw internetowych oraz prawnych i organizacyjnych aspektów ścigania tych przestępstw. Oczekiwano, że rezultaty takiego porównania pozwolą nie tylko na udzielenie odpowiedzi na postawione na wstępie pytanie, lecz także na wyciągnięcie z ustaleń empirycznych wniosków praktycznych.

1. METODA BADAŃ, CHARAKTERYSTYKA BADANYCH POPULACJI

Podstawowy instrument badawczy, jakim był kwestionariusz ankiety składającej się ze 128 pytań i 445 wariantów odpowiedzi, został opracowany na podstawie raportu z badań amerykańskich, na co uzyskano zgodę ich autorów (Burns, Witworth, Thompson 2004, s. 477-493). Oryginalne badanie, zrealizowane w Stanach Zjednoczonych w 2001 r. w drodze ankiety pocztowej, objęło 700 jednostek policji zlokalizowanych w różnych regionach tego kraju. Replikę badań amerykańskich przeprowadzono w Polsce w kwietniu 2005 r. przy użyciu poczty elektronicznej. Kwestionariusz ankiety przesłano do wszystkich posiadaczy kont pocztowych w Policyjnej Sieci Transmisji Danych (PSTD) oraz w domenach: policja.gov.pl, wojewodztwo.policja.gov.pl[9].

Na ankietę odpowiedziało 217 respondentów w USA i 224 w Polsce[10]. Populacje, z jakich wywodzili się uczestniczący w badaniach policjanci amerykańscy i policjanci polscy były do siebie zbliżone pod jednym względem. W obu przypadkach były to duże, zatrudniające więcej niż stu funkcjonariuszy, jednostki policji (tabela 1). W Stanach Zjednoczonych większość z nich (55,2%) posiadała specjalne zespoły ds. przestępczości komputerowej. W Polsce wskaźnik ten był znacznie niższy (28,6%), przy czym połowa zespołów zajmujących się ściganiem przestępstw komputerowych miała charakter „nieetatowy". Stanowiły one zatem raczej grupy ochotników, składające się z funkcjonariuszy dysponujących pewną wiedzą informatyczną i umiejętnościami w zakresie posługiwania się komputerem, którzy na co dzień wykonywali „normalną pracę", niezwiązaną z prowadzeniem postępowań karnych w sprawach cyberprzestępstw[11].

---

[9] Według danych uzyskanych od administratorów poczty elektronicznej takich adresatów było ok. 3600, przy czym duża grupa użytkowników posiada konto w PSTD i domenie policja.gov.pl.

[10] Odpowiedzi na ankietę dotarły:

a.	e-mailem wysłanym przez Policyjnej Sieci Transmisji Danych	41	18,3%
b.	e-mailem wysłanym przez internet	37	16,52%
c.	tradycyjnym listem lub przez telefaks	146	65,18%

[11] Polscy respondenci (n = 222) w odpowiedzi na pytanie „jak oceniasz swoje umiejętności komputerowe?" w większości ocenili je jako „średnie" (43%) i „dobre" (32%), 6% badanych uznało się za „ekspertów", ok. 2% za „laików", natomiast 16% ankietowanych określiło własne umiejętności jako „słabe". Analogiczne pytanie nie występowało w ankiecie amerykańskiej.

Tabela 1

Pytanie: Ilu funkcjonariuszy zatrudnia jednostka, w której pracujesz?				
Odpowiedź:	USA		Polska	
do 100	-	-	50	22,62%
101-250	105	48,4%	78	35,29%
251-500	56	25,8%	38	17,19%
501-1000	27	12,4%	25	11,31%
1001 i więcej	29	13,4%	30	13,57%

Zespoły ds. przestępstw komputerowych istnieją w policji od niedawna. Dane uzyskane w badaniach amerykańskich wskazują, że 87,5% z nich powstało po 1995 r., co można wiązać z dynamicznym rozwojem internetu w latach dziewięćdziesiątych ubiegłego wieku i gwałtownym wzrostem liczby przestępstw popełnianych przez użytkowników tej globalnej sieci komputerowej. Idea tworzenia specjalnie wyszkolonych i odpowiednio wyposażonych grup policjantów zajmujących się ściganiem przestępstw komputerowych pojawiła się w Stanach Zjednoczonych w latach osiemdziesiątych, wkrótce po tym, gdy nadużycia komputerowe zostały skryminalizowane w ustawodawstwie federalnym tego państwa.

W Polsce pierwszy taki zespół powstał na szczeblu Komendy Głównej Policji w roku 1998[12]. Decyzja o jego powołaniu zbiegła się w czasie z wejściem w życie Kodeksu karnego z 1997 r., w którym stypizowano szereg przestępstw komputerowych. Z odpowiedzi uzyskanych od respondentów wynika, że w roku 2005 liczba zespołów zajmujących się ściganiem tej kategorii przestępstw przekroczyła 60, przy czym połowa z nich powstała w ciągu ostatnich trzech lat (tabela 2).

Tabela 2

Pytanie: **Czy w jednostce funkcjonuje grupa (zespół, wydział) ds. przestępczości komputerowej?**				
Odpowiedź:	USA		Polska	
Tak	117	55,2%	63	28,6%
Nie	100	46,8%	157	71,4%
Pytanie: **Jak długo?**				
Odpowiedź:	N = 120	100%	N = 55	100%
krócej niż 1 rok	21	17,5%	6	11%
1-3 lata	47	39,2%	21	38%
3-5 lat	37	30,8%	15	27%
5 i więcej lat	15	12,5%	13	24%
Pytanie: **Ilu liczy pracowników?**				
Odpowiedź:	N = 120	100%	N = 55	100%
1-5	112	93,3%	44	80,0%
6-12	7	5,8%	10	16,4%
13-25	1	0,8%	**1**	3,6%

[12] W ramach Biura ds. Przestępczości Gospodarczej powołano Samodzielną Sekcję ds. Przestępczości Komputerowej, która miała koordynować pracę podobnych sekcji na szczeblu Wydziałów ds. Przestępczości Gospodarczej Komend Wojewódzkich Policji.

W obu krajach ściganiem przestępstw komputerowych zazwyczaj zajmują się małe, najwyżej pięcioosobowe grupy policjantów. W Polsce przeważają zespoły mniejsze, jedno- lub dwuosobowe, na co wskazywało 41,5% respondentów. Biorąc pod uwagę, że byli to głównie pracownicy Komend Powiatowych i Komend Miejskich Policji, skromne siły, jakimi w omawianym zakresie dysponują te jednostki, wydają się odpowiadać raczej ich możliwościom niż potrzebom.

2. WYNIKI BADAŃ

Dokonanie kryminologicznej oceny przygotowania policji do stawienia czoła jednej z nowych form przestępczości, jaką są oszustwa internetowe, wymagało uwzględnienia szeregu zmiennych i przeanalizowania wielu zagadnień. Autorzy amerykańscy zredukowali je do pięciu następujących kategorii:

1. percepcja zjawiska oszustw internetowych przez policjantów, uwzględniająca również ocenę regulacji prawnych stanowiących podstawę ścigania tych przestępstw oraz aktualnej i postulowanej praktyki w tym zakresie;
2. wyszkolenie i wyposażenie policjantów zajmujących się ściganiem oszustw internetowych;
3. współpraca między jednostkami policji oraz ich współdziałanie z organizacjami cywilnymi w ramach prowadzonych postępowań karnych;
4. polityka informacyjna policji na temat oszustw internetowych wobec różnych grup społecznych i zawodowych;
5. struktura oszustw internetowych zgłaszanych przez pokrzywdzonych policji.

Mając na uwadze porównawcze ujęcie wyników obu badań, informacje i opinie pochodzące od polskich policjantów gromadzono na podstawie analogicznego schematu analizy. Treść pytań stawianych polskim respondentom w wielu wypadkach odpowiednio modyfikowano, m.in. ze względu na różnice w systemach prawnych i podziałach administracyjnych Polski i Stanów Zjednoczonych. Tam, gdzie różnice były fundamentalne, rezygnowano z bezpośrednich porównań na rzecz „równoległego" przedstawienia tych samych zagadnień z uwzględnieniem polskiej specyfiki, na przykład w zakresie podmiotów pomagających policji ścigać przestępstwa komputerowe. Niektóre z wyżej wymienionych zagadnień pominięto w niniejszym opracowaniu, kierując się przekonaniem, że próba ich porównawczego ujęcia byłaby zbyt ryzykowna metodologicznie bądź pozbawiona wystarczających podstaw w zgromadzonym materiale empirycznym. Dotyczy to m.in. polityki informacyjnej policji w zakresie przestępstw komputerowych, na temat której nie zdołano uzyskać od polskich respondentów danych umożliwiających dokonanie analizy porównawczej.

2.1. Ocena zjawiska

Polscy i amerykańscy policjanci w podobny sposób postrzegają problem oszustw internetowych. Zdecydowana większość z nich (odpowiednio: 74,1% i 76,5%) uważa, że jest to problem poważny (tabela 3). Sąprzy tym zgodni, że nie przypisuje się temu zjawisku podobnego znaczenia w ich w macierzystych jednostkach, ogólnie w policji, w prokuraturze, w szczególności zaś w sądach. Innymi słowy, *gros* policjantów w obu krajach nie uznaje ścigania tego typu przestępstw za priorytetowy kierunek

działania organów ścigania i wymiaru sprawiedliwości. Respondenci z obu państw są też zdania, że bardziej wyczulone na problem oszustw popełnianych przy użyciu sieci komputerowych jest społeczeństwo niż prokuratura i sądy.

Tabela 3. Stanowisko wobec oszustw komputerowych*

Kto uważa oszustwa internetowe za poważny problem	POLSKA		USA	
	dominanta	%	dominanta	%
1. Osobiście uważam oszustwa internetowe za poważny problem.	5	74,1	5	76,5
2. Moja jednostka organizacyjna (wydział) traktuje oszustwa internetowe jako poważny problem.	3	43,7	3	40,7
3. Policja traktuje oszustwa internetowe jako poważny problem.	3	38,8	3	41,0
4. Prokuratura traktuje oszustwa internetowe jako poważny problem.	2	20,8	2	20,6
5. Sądy traktują oszustwa internetowe jako poważny problem.	2	14,5	2	11,7
6. Społeczeństwo traktuje oszustwa internetowe jako poważny problem.	2	24,1	3	27,8

* Skala: 1- „zdecydowanie nie zgadzam się", 5 - „zdecydowanie zgadzam się";
% = odsetek respondentów, którzy „zgadzają się" i „zdecydowanie zgadzają się".

Zbieżność opinii policjantów z odległych od siebie jurysdykcji na temat niedoceniania problemu oszustw internetowych przez prokuratorów i sędziów jest uderzająca. Wydaje się, że odczucia respondentów w tym zakresie mogą mieć związek z ich doświadczeniami zawodowymi i wynikać z obserwacji wyniesionych przez policjantów z kontaktów z przedstawicielami wymiaru sprawiedliwości w sprawach o przestępstwa komputerowe.

2.2. Ocena przepisów prawnych dotyczących oszustw internetowych

Duże podobieństwo cechuje postawy polskich i amerykańskich policjantów wobec norm stanowiących ramy prawne ścigania oszustw internetowych. Respondenci na ogół krytycznie oceniają aktualny stan legislacji w tej dziedzinie. Większość badanych w Polsce i Stanach Zjednoczonych uznaje celowość wprowadzenia nowych regulacji prawnych, umożliwiających bardziej efektywne zapobieganie oszustwom internetowym oraz skuteczne ściganie i karanie ich sprawców. Pogląd taki jest bardziej rozpowszechniony wśród funkcjonariuszy policji amerykańskiej (74,7%; McGuire 2004) niż polskiej (68,3%), aczkolwiek różnica nie wydaje się istotna statystycznie (tabela 4).

Zbliżony do siebie rozkład odpowiedzi uzyskanych w obu badanych populacjach wskazuje na niezadowolenie respondentów z jakości aktualnie pozostających w ich dyspozycji instrumentów prawnych, ocenianych jako niewystarczające do realizacji zadań związanych z inkryminowaniem oszustw internetowych. Blisko trzy czwarte ankietowanych zdecydowanie zgadza się z twierdzeniem, że są w tym celu niezbędne dodatkowe przepisy prawne. Opinia ta nie wydaje się trafna, przynajmniej gdy chodzi o stan polskiej legislacji w tej dziedzinie. W swym obecnym kształcie, po nowelizacji

Kodeksu karnego z 18 marca 2004 r., wykazuje ona nawet pewną „nadmiarowość" w stosunku do potrzeb i nie wymaga istotnych zmian, w szczególności takich, które mogłyby ułatwić policji ściganie oszustw internetowych (Adamski 2005; 2006). Wydaj e się, że krytyka „złego prawa" ma w tym wypadku charakter zastępczy, aczkolwiek zagadnienie wymagałoby bardziej szczegółowej analizy.

Tabela 4. Ocena przepisów prawnych*

Niezbędne są dodatkowe przepisy prawne:	POLSKA		USA	
	dominanta	%	dominanta	%
1. definiujące pojęcie oszustwa internetowego	5	70,5	5	64,5
2. powstrzymujące sprawców od popełniania oszustw internetowych	5	75,4	5	69,4
3. umożliwiające bardziej efektywne ściganie /karanie sprawców oszustw internetowych	5	68,3	5	74,7
4. ułatwiające ściganie sprawców oszustw internetowych w skali międzynarodowej	5	73,6	5	72,9
5. określające obszar i granice działania organów ścigania przy ściganiu sprawców oszustw internetowych	5	62,3	5	70,0

* Skala: 1 - „zdecydowanie nie zgadzam się", 5 - „zdecydowanie zgadzam się";
% = odsetek respondentów, którzy „zgadzają się" lub „zdecydowanie zgadzają się".

2.3. Kto ściga oszustwa internetowe?

W USA ściganiem oszustw internetowych zajmują się głównie lokalne jednostki policji. Na tę okoliczność wskazała blisko połowa respondentów amerykańskich (47,4%). Nieco mniejszy odsetek ankietowanych był zdania, że postępowania karne w tych sprawach prowadzone są na wyższym szczeblu struktury organizacyjnej aparatu ścigania, tj. hrabstwa (ang. *county* - 42,8%) oraz agend federalnych (38,3%) i stanowych policji (33,7%). Nieznaczna część respondentów (2,6%) wskazała, że dochodzenia w sprawach o oszustwa internetowe prowadzą prywatni detektywi.

Wśród polskich policjantów dominuje opinia, że ściganie przestępstw komputerowych jest domeną funkcjonariuszy wydziałów do walki z przestępczością gospodarczą w komendach wojewódzkich (KWP - 67,7%) oraz komendach powiatowych (KPP) i miejskich (KMP - 59,5%). Znacznie mniejsza część badanych wskazywała w tym kontekście na komisariaty (25,8%) i jednostki pozapolicyjne (25,8%). Niewiele większe poparcie zyskał pogląd, że tym rodzajem przestępczości zajmuje się Centralne Biuro Śledcze - taką opinię wyraziło 28,7% policjantów.

Jak pokazują powyższe dane, instytucjonalnie ciężar odpowiedzialności za ściganie przestępstw komputerowych inaczej rozkłada się w Polsce niż w USA. W Polsce jest to przede wszystkim domena wojewódzkich struktur policji, które są bezpośrednio zaangażowane w prowadzenie dochodzeń w tych sprawach oraz koordynują i nadzorują działania jednostek im podległych. W Stanach Zjednoczonych, mimo właściwości rzeczowej FBI w odniesieniu do szerokiej klasy cyberprzestępstw, aktywność policji w tej dziedzinie nie koncentruje się tak wyraźnie jak w Polsce na wyższych szczeblach struktury organizacyjnej, lecz rozkłada się względnie równomiernie na wszystkich jej ogniwach. W istocie skupia się na lokalnych jednostkach policji, co

wydaj e się naturalne i prawidłowe ze względu na ich społeczne usytuowanie „blisko" osób pokrzywdzonych przestępstwami, w tym komputerowymi. Ten model, gdy chodzi o przestępstwa komputerowe, nie znajduje zastosowania w Polsce z powodu słabości podstawowych komórek organizacyjnych policji, jakimi są komisariaty.

Tabela 5. Kto ściga oszustwa internetowe?*

Kto ściga oszustwa internetowe:	POLSKA		USA	
	dominanta	%	dominanta	%
1. Jednostki lokalne/ komisariaty policji	1	25,8	5	47,4
2. Jednostki na szczeblu hrabstwa/ powiatu lub miasta [KPP, KMP]	5	59,5	3	42,8
3. Jednostki stanowe/ wojewódzkie [KWP]	5	67,7	3	33,7
4. Jednostki federalne (FBI)/ centralne (CBŚ)	3	28,7	3	38,3
5. Prywatni detektywi/ jednostki pozapolicyjne	1	25,8	1	2,6

* Skala: 1 - „zdecydowanie nie zgadzam się", 5 - „zdecydowanie zgadzam się";
% = odsetek respondentów, którzy „zgadzają się" lub „zdecydowanie zgadzają się".

2.4. Kto powinien ścigać oszustwa internetowe?

Opinie obu grup respondentów są wyraźnie podzielone w kwestii, na jakim szczeblu struktury organizacyjnej policji powinien spoczywać główny ciężar zadań związanych ze ściganiem oszustw internetowych. Policjanci amerykańscy byli w tej sprawie niemal jednomyślni. Aż 93% z nich wskazało na szczebel federalny, prawdopodobnie biorąc pod uwagę okoliczność, że znaczna część oszustw internetowych to przestępstwa „międzystanowe", które podlegają jurysdykcji FBI (Icove, Seger, VonStroch 1995, s. 71). Znaczna część badanych była również zdania, że jest to odpowiednie zajęcie dla organów ścigania na szczeblu stanowym (69,7%) i lokalnym (52,1%). Tylko nieliczni (6,8%) skłonni byli uznać właściwość podmiotów prywatnych w tym zakresie.

Zaskakująca na tym tle jest postawa polskich policjantów wobec propozycji, by ściganiem oszustw internetowych zajął się ktoś spoza policji. Równo połowa ankietowanych wyraziła poparcie dla takiego rozwiązania. Więcej niż połowa (51,8%) wypowiedziała się przeciwko obarczaniu tymi obowiązkami funkcjonariuszy zatrudnionych w komisariatach policji. Blisko dwie trzecie respondentów (63,9%) uznało za najbardziej właściwy szczebel średni (KWP - wydziały do walki z przestępczością gospodarczą), nieomal połowa (47,7%) - komendy powiatowe i miejskie policji. Wiele było też negatywnych opinii na temat powierzenia tych zadań CBŚ (29,2% respondentów okazało się temu zdecydowanie przeciwnych).

Polscy respondenci pytani „kto to powinien robić?" wskazują najczęściej na te agendy, na których aktualnie spoczywa główny ciężar zadań związanych ze ściganiem oszustw internetowych. Z jednej strony można zatem sądzić, że *status quo* w tym zakresie uważają za praktykę prawidłową, którą należy utrzymać. Z drugiej strony nie sposób oprzeć się wrażeniu, że takie stanowisko jest wyrazem realnej oceny kondycji, w jakiej pod względem kadrowym i sprzętowym znajdują się niższe szczeble struktury organizacyjnej policji, w szczególności komisariaty. Okazuje się jednak, że ocena ta jest bardzo niska nie tylko w odniesieniu do komisariatów. Symboliczną,

ale i niepokojącą wymowę ma w tym kontekście stanowisko połowy respondentów, którzy byli zdania, że policję w dziedzinie ścigania oszustw internetowych powinny wyręczyć inne podmioty.

Tabela 6. Jednostki właściwe do ścigania oszustw internetowych*

Kto powinien ścigać oszustwa internetowe:	POLSKA		USA	
	dominanta	%	dominanta	%
1. Jednostki lokalne/ komisariaty policji	1	19,3	5	52,1
2. Jednostki na szczeblu hrabstwa/ powiatu lub miasta (KPP, KMP)	5	47,7	5	48,3
3. Jednostki stanowe/ wojewódzkie (KWP)	5	63,9	5	69,7
4. Jednostki federalne (FBI)/ centralne (CBŚ)	1	29,2	5	93,0
5. Prywatni detektywi/jednostki pozapolicyjne	5	50,0	1	6,8

* Skala: 1 - „zdecydowanie nie zgadzam się", 5 - „zdecydowanie zgadzam się";
% = odsetek respondentów, którzy „zgadzają się" lub „zdecydowanie zgadzają się".

2.5. Zasoby kadrowe i sprzętowe

Ocena przygotowania jednostek policji do ścigania oszustw internetowych była w obu badanych populacjach bardzo niska (tabela 7). Mniej niż jedna piąta respondentów (17,1% w Polsce i 15,3% w USA) wykazała w tej materii optymistyczne nastawienie. W przypadku Stanów Zjednoczonych pozytywne opinie na temat dostatecznej obsady kadrowej i należytego poziomu jej wyszkolenia wyraziło odpowiednio 6,5% i 17,6% ankietowanych. Niższą wartość mają oba te wskaźniki w przypadku polskich badań (odpowiednio 5,4% oraz 6,3%). Uczestniczący w nich policjanci w odpowiedzi na stawiane im pytania zajmowali najczęściej skrajnie negatywne stanowisko („zdecydowanie się nie zgadzam"). I tak na przykład 62% respondentów było przeciwnych i zdecydowanie przeciwnych tezie, że ich jednostka posiada odpowiednie wyposażenie sprzętowe (komputery, łącza, inny sprzęt) do ścigania oszustów komputerowych, więcej niż 80% badanych udzieliło analogicznej odpowiedzi na pytanie o specjalistyczne oprogramowanie komputerowe używane do ścigania oszustów internetowych.

Tabela 7. Kadra, sprzęt i oprogramowanie*

Moja jednostka organizacyjna:	POLSKA		USA	
	dominanta	%	dominanta	%
1. jest przygotowana do ścigania oszustw internetowych	1	17,1	2	15,3
2. posiada właściwą obsadę kadrową (ilościowo) do ścigania oszustw internetowych	1	5,4	2	6,5
3. posiada odpowiednio przeszkoloną kadrę do ścigania oszustw internetowych	1	6,3	2	17,6
4. posiada odpowiednie wyposażenie sprzętowe do ścigania oszustw internetowych	1	12,6	2	16,2
5. posiada odpowiednie oprogramowanie komputerowe do ścigania oszustów internetowych	1	3,6	-	-

* Skala: 1 - „zdecydowanie nie zgadzam się", 5 - „zdecydowanie zgadzam się";
% = odsetek respondentów, którzy „zgadzają się" lub „zdecydowanie zgadzają się".

Ogólny charakter pytań i mało zobiektywizowane kryteria oceny nie pozwalają na kategoryczne stwierdzenie, że poziom przygotowania polskich i amerykańskich policjantów do ścigania oszustw internetowych istotnie różni się od siebie bądź że jest do siebie zbliżony. Bliżej nieznane są bowiem standardy, do których respondenci należący do każdej z badanych grup relatywizowali swoje oceny dotyczące „właściwej obsady kadrowej" czy „odpowiedniego wyposażenia". Istnieją jednak podstawy, by sądzić, że gorsze wskaźniki przygotowania polskich organów ścigania do walki z cyberprzestępczością niż te, jakie uzyskano w badaniach amerykańskich, są adekwatne do rzeczywistości. Wskazują na to również odpowiedzi respondentów na pytania zawarte w dalszej części ankiety.

2.3. Szkolenie funkcjonariuszy

Już na pierwszy rzut oka dane zawarte w tabeli 8 wskazują, że w Polsce i USA funkcjonuje inny model szkolenia policjantów, przynajmniej w zakresie ścigania oszustw internetowych. O ile w USA większość respondentów (65,9%) uczestniczy w tym celu w warsztatach, seminariach i konferencjach, a blisko połowa (47%) - w innych formach kształcenia organizowanych poza własną jednostką, w Polsce niemal połowa badanych (46,9%) zdobywa wiedzę na ten temat w ramach szkoleń realizowanych siłami macierzystej komórki organizacyjnej.

Tabela 8. Organizacja szkoleń*

Szkolenia funkcjonariuszy mojej jednostki dotyczące ścigania oszustw internetowych były realizowane przez:	POLSKA %	USA %
1. udział w warsztatach, seminariach lub konferencjach	31,7	65,9
2. inną jednostkę policji / resort	11,6	47,0
3. moją jednostkę	46,9	23,5
4. prywatnych detektywów / instytucje i osoby współpracujące z policją (np. CERT Polska, Allegro, biegli sądowi)	22,3	3,2

* % = odsetek respondentów uczestniczących w szkoleniu.

To rezultat zastanawiający, skoro tylko 6% respondentów stwierdziło, że ich jednostki posiadają odpowiednio przeszkoloną kadrę do ścigania oszustów komputerowych (por. tabela 7, pkt 3). Kto zatem szkoli policjantów? Pytanie to jest o tyle zasadne, że szkolenia realizowane przez wyspecjalizowane w tym zakresie instytucje zaspokajają zaledwie ułamek potrzeb - korzystało z nich w zakresie prawnym i technicznym niewielu badanych (odpowiednio 11,6% i 22,3%). Natomiast szkolenia resortowe i udział w specjalistycznych konferencjach obejmowały mniej niż jedną trzecią jednostek. Wydaje się, że przytoczone liczby nie mogą pozostawiać złudzeń co do ogólnego poziomu przygotowania funkcjonariuszy policji do prowadzenia postępowań karnych w sprawach przestępstw związanych z użyciem komputera.

2.7. Współpraca z innymi jednostkami policji i sektorem prywatnym

Oszustwa internetowe są często popełniane na szkodę wielu osób zamieszkałych w różnych częściach kraju, niekiedy poza jego granicami. Warunkiem skutecznego ścigania sprawców tych przestępstw jest odpowiednia koordynacja działań różnych jednostek policji oraz ich ścisła współpraca z innymi podmiotami spoza policji.

Rezultaty badań amerykańskich dotyczące intensywności wzajemnych kontaktów jednostek policji w sprawach oszustw internetowych wskazują, że były one częste i miały na ogół charakter horyzontalny. Blisko jedna piąta ankietowanych (19,1%) komunikowała się w tych sprawach co najmniej raz w tygodniu z inną jednostką policji, na ogół tego samego, lokalnego szczebla (tabela 9).

Tabela 9. Intensywność kontaktów (USA)*

Częstotliwość kontaktów z innymi podmiotami w sprawach oszustw internetowych:	USA	
	dominanta	%
1. Jednostki lokalne	4	19,1
2. Jednostki na szczeblu hrabstwa	4	17,0
3. Jednostki stanowe	3	6,6
4. Jednostki federalne (np. FBI)	3	8,9
5. Prywatni detektywi	1	0,5
6. Internet Fraud Compliant Center (FBI/NWCC)[13]	1	12,3

* Skala: 1 - „nigdy", 5 - „co najmniej raz w tygodniu";
% = odsetek respondentów deklarujących kontakt cotygodniowy.

Ocena efektów tej współpracy również wypadła zadowalająco, najbardziej w odniesieniu do najniższego szczebla struktury organizacyjnej policji. Kooperację z lokalnymi jednostkami policji większość respondentów (64,2%) oceniła (w czterostopniowej skali) jako „efektywną" lub „bardzo efektywną". Niewiele mniejszy odsetek ankietowanych (55,1%) równie wysoko ocenił współpracę z federalnymi organami ścigania. Najmniej pozytywnych ocen dotyczyło współpracy z prywatnymi detektywami (tabela 10).

Tabela 10. Efektywność współpracy (USA)*

Jak oceniasz skuteczność współpracy Twojej jednostki z następującymi podmiotami w zakresie ścigania oszustw internetowych?	USA	
	dominanta	%
1. Jednostki lokalne	3	64,2
2. Jednostki na szczeblu hrabstwa	2	62,0
3. Jednostki stanowe	2	54,5
4 Jednostki federalne (np. FBI)	3	55,1
5. Prywatni detektywi	2	30,9
6. Internet Fraud Compliant Center (FBI/NWCC)	2	45,5

* Skala ocen = 1 - „bezwartościowa", 4 - „bardzo efektywna";
%= odsetek respondentów oceniających współpracę jako „efektywną" lub „bardzo efektywną".

[13] Centrum Skarg na Oszustwa Internetowe - utworzone w 2000 r. z inicjatywy FBI oraz Narodowego Centrum ds. Przestępczości Białych Kołnierzyków (National White Collar Crime Center) zajmuje się zarówno przyjmowaniem zgłoszeń o oszustwach internetowych od pokrzywdzonych, jak i przekazywaniem gromadzonych na ten temat informacji i statystyk, organom ścigania. Zob. http://www.ifccfbi.gov/index.asp.

Wyniki polskich badań częściowo różnią się od rezultatów badań amerykańskich, a częściowo nie są z nimi porównywalne. Przede wszystkim wskazują na ograniczony zakres współpracy struktur policyjnych oraz małą częstotliwość kontaktów funkcjonariuszy policji prowadzących postępowania karne w sprawach przestępstw komputerowych z innymi podmiotami. Jeżeli już do takich kontaktów dochodzi, co - jak pokazują dane zawarte w tabeli 11 - jest raczej rzadkością, to są one w zasadzie nawiązywane tylko z wydziałami do walki z przestępczością gospodarczą KWP. Współpraca z Centralnym Biurem Śledczym praktycznie nie istnieje. Brak też współpracy ze szkołami policyjnymi. Jest to zrozumiałe w zakresie pracy wykrywczej policjantów, ale niezrozumiałe w kontekście wskazanych wcześniej braków odpowiednio przeszkolonej kadry. Może jednak stanowić sygnał, że szkoły policyjne nie są w stanie zaoferować takiej specjalistycznej współpracy. Na stosunkowo częste kontakty policjantów z cywilnymi specjalistami w zakresie przestępczości komputerowej wskazało 29,7% respondentów. Jest to wskaźnik 60-krotnie wyższy od uzyskanego w badaniach amerykańskich w odpowiedzi na podobnie sformułowane pytanie.

Tabela 11. Intensywność kontaktów (Polska)*

W zakresie przestępczości komputerowej, w szczególności oszustw internetowych, współpracujesz (inni funkcjonariusze Twojej jednostki współpracują) z:	POLSKA	
	dominanta	%
1. Wydziałami do walki z przestępstwami gospodarczymi KWP w swoim województwie	3	40,1
2. Centralnym Laboratorium Kryminalistycznym KGP	1	4,1
3. Laboratorium kryminalistycznym w swoim województwie	1	7,7
4. Centralnym Biurem Śledczym	1	7,7
5. Policyjnymi specjalistami od przestępczości komputerowej	1	2,2
6. Szkołami policji	1	7,5
7. Cywilnymi specjalistami od przestępczości komputerowej	1	29,7

* Skala: 1 - „nigdy", 5 - „zawsze";
% = odsetek respondentów deklarujących częste kontakty.

Bliższa analiza tego zagadnienia prowadzi jednak do mniej pokrzepiających spostrzeżeń (tabela 12).

Dominująca odpowiedź na pytanie, jak często policjanci współpracowali z podmiotami reprezentującymi sektor prywatny, brzmiała: „nigdy". Wielokrotnie policjanci wskazywali na współpracę z Allegro[14]. Więcej niż jedna trzecia (38%) ankietowanych uznała kontakty z administratorami tej największej polskiej aukcji internetowej za częste. Niepokojąco słaba okazała się współpraca z bardzo istotnymi organizacjami mogącymi wspomóc lokalizację oszustów internetowych - CERT Polska i Abuse TP SA. Nieco częściej policjanci zwracali się z prośbą o pomoc do portali internetowych i banków internetowych, choć i w tych wypadkach kontakty deklarowane jako „częste" były udziałem względnie nielicznej grupy respondentów (odpowiednio 17,3% i 11,9%).

[14] Zob. http://www.allegro.pl/.

Tabela 12. Kontakty policji z sektorem prywatnym - (Polska)*

Czy w ostatnim roku (2004) w zakresie przestępczości komputerowej, w szczególności oszustw komputerowych, kontaktowałeś się (lub inni funkcjonariusze Twojej jednostki) z prośbą o pomoc z:	POLSKA	
	dominanta	%
1. CERT Polska	1	4,2
2. Zespół Abuse TP SA	1	8,4
3. Portal Allegro	1	38,0
4. Centra rozliczeniowe (Polcard, eCard itp.)	1	8,3
5. Bank internetowy (mBank, Inteligo itp.)	1	11,9
6. Portale internetowe (onet, wp, interia itp.)	1	17,3

* Skala: 1 - „nigdy", 5 - „zawsze";
% = odsetek respondentów deklarujących częste kontakty.

Zasadniczym elementem oceny każdego rodzaju współpracy, w tym policji z sektorem prywatnym, są jej rezultaty. Poniższe dane wskazują (tabela 13), że nie zostały one dobrze ocenione przez respondentów.

Tabela 13. Efektywność współpracy policji z sektorem prywatnym (Polska)*

Jak oceniasz skuteczność współpracy Twojej jednostki z następującymi podmiotami w zakresie ścigania oszustw internetowych?	POLSKA	
	dominanta	%
1. CERT Polska	1	1,3
2. Zespół Abuse TP SA	1	13,8
3. Portal Allegro	5	52,0
4. Centra rozliczeniowe (Polcard, eCard itp.)	1	13,4
5. Banki internetowe (mBank, Inteligo itp.)	1	10,6
6. Portale internetowe (onet, wp, interia itp.)	1	15,0

* Skala: 1 - „bezwartościowa", 5 - „bardzo efektywna";
% = odsetek ocen współpracy jako „efektywna" lub „bardzo efektywna".

Pozytywne oceny dotyczą jedynie Allegro. Współpraca z tym portalem aukcyjnym uznana została przez większość badanych (52%) za „bardzo efektywną". We wszystkich pozostałych przypadkach respondenci stwierdzili, że najczęściej współpraca z organizacjami, o które ich pytano, była bezwartościowa.

2.8. Oszustwa internetowe

Ostatnie pytanie ankiety odwoływało się do wiedzy respondentów na temat rozmiarów i struktury zjawiska oszustw internetowych, ocenianych na podstawie zawiadomień składanych ich macierzystym jednostkom przez osoby pokrzywdzone tego rodzaju przestępstwami. Było to pytanie zamknięte, oparte na typologii oszustw występujących w amerykańskiej domenie internetu, które miało na celu oszacowanie częstości zgłoszeń o zdarzeniach odpowiadających (zdaniem respondentów) kryteriom poszczególnych rodzajów oszustw. Przedmiotem badania była więc percepcja tego zjawiska przez policjantów.

Tabela 14. Zgłoszenia o oszustwach składane policji*

Jak często zgłaszane są w Twojej jednostce wymienione niżej oszustwa internetowe:	POLSKA		USA	
	dominanta	%	dominanta	%
1. Kradzież tożsamości	1	1,2	5	81,1
2. Związane z kartami płatniczymi	2	5,6	5	79,0
3. Związane z zakupami towarów przez sieć	3	27,9	4	65,9
4. Związane z aukcjami internetowymi	4	40,2	4	39,5
5. Oferty inwestycyjne i finansowe	1	0,6	2	25,7
6. Piramidy finansowe	1	1,9	1	11,7
7. Oferty podróży, wakacji	1	1,3	1	8,7
8. Oferty pracy w domu	1	0,6	1	7,7

* Skala: 1 - „nigdy", 5 - „częściej niż raz w tygodniu";
% = zgłoszenia otrzymywane co najmniej raz w miesiącu.

Amerykańska typologia oszustw internetowych ma swoją specyfikę. Nie wszystkie występujące w niej kategorie były więc w pełni rozpoznawalne dla polskich policjantów. W szczególności dotyczyło to „kradzieży tożsamości" - czynu polegającego na bezprawnym zdobyciu i wykorzystaniu informacji identyfikujących inną osobę[15]. W przypadku tej kategorii oszustwa różnica w rozkładzie odpowiedzi obu badanych grup była największa (1,2% Polska, 81,1% USA). Wartość drugiego z tych wskaźników okazała się też zaskakująco wysoka na tle statystyk Centrum Zgłoszeń Oszustw Internetowych (IFCC), w których przeważają oszustwa związane z aukcjami internetowymi, natomiast przypadki „kradzieży tożsamości" stanowią niewielki odsetek zgłoszeń[16].

Oszustwa aukcyjne uzyskały najbardziej zbliżoną do siebie ocenę policjantów polskich i amerykańskich, jako najczęściej zgłaszana organom ścigania kategoria oszustw internetowych. Pozostałe ich odmiany, z wyjątkiem polegających na niedostarczeniu zamówionego towaru lub zapłaty za zakupy w ramach handlu elektronicznego, nie spotkały się z podobną oceną polskich respondentów (tabela 14).

Ocena ta odpowiada rezultatom badań praktyki prokuratorskiej w sprawach przestępstw związanych z internetem, jakie przeprowadzono w Polsce w 2003 r. (Stefański 2006, s. 121-127). Badania obejmowały 658 spraw o przestępstwa internetowe[17], w których w latach 2001-2002 zakończono postępowanie przygotowawcze postanowieniem o jego umorzeniu bądź skierowaniem aktu oskarżenia do sądu. Zdecydowana większość spraw - 524 (79%) - dotyczyła oszustw (art. 286 § 1 k.k.) na ogół związanych z aukcjami internetowymi. Efektywność ścigania karnego tych czynów okazała się stosunkowo niska. Na ogólną liczbę 658 spraw - w 290 przypadkach (44,1%) postępowanie zostało umorzone z powodu niewykrycia sprawców (dotyczy-

[15] „What are identity theft and identity fraud?", http://www.usdoj.gov/criminal/fraud/text/idtheft.html; Newman 2004.

[16] Odsetek oszustw związanych z aukcjami internetowymi zgłoszonych IFCC wynosił: 42,8% w 2001 r., 46,1% w 2002 r., 61,0% w 2003 r. i 71,2% w 2004 r. - por. http://www.ifccfbi.gov/strategy/statistics.asp.

Autorzy badań amerykańskich, na których wzorowano niniejsze badania, również odnotowali tę różnicę, lecz nie zdołali jej wyjaśnić - zob. Burns i in. 2004, s. 488.

[17] Tj. zarówno skierowanych przeciwko bezpieczeństwu sieci i systemów komputerowych, jak i popełnionych z ich wykorzystaniem.

ło to głównie oszustw dokonanych na aukcjach internetowych), w 234 przypadkach (35,6%) postępowanie przygotowawcze zakończyło się wniesieniem aktu oskarżenia do sądu (ibidem).

3. DYSKUSJA I WNIOSKI

Przedstawione wyniki badań ankietowych potwierdzają potoczne wyobrażenia na temat różnic w poziomie przygotowania i sposobie funkcjonowania polskich i amerykańskich jednostek policji zaangażowanych w ściganie przestępstw komputerowych. Zdają się również uzasadniać stwierdzenie, że różnice te mają charakter systemowy, wynikają z odmiennej organizacji życia społecznego, poziomu ekonomicznego i odrębności kulturowej obu państw. Jednocześnie uzyskane wyniki, dzięki ujęciu porównawczemu, pokazują nieoczekiwany element w postawie polskich policjantów, który zdecydowanie odróżnia ich od policjantów amerykańskich. Polskich respondentów cechuje mianowicie głęboki deficyt poczucia satysfakcji z warunków, w jakich wykonują swoją pracę. Do tego stopnia negatywnie oceniają stan wyposażenia swoich jednostek, poziom szkoleń i celowość współpracy z innymi, że nie dostrzegają niczego niestosownego w akceptowaniu propozycji, by problem, z którym nie mają „jak" i „czym" walczyć, przekazać w gestię podmiotów prywatnych, wraz z częścią swych ustawowych uprawnień i obowiązków. Niestety, generalizacja ta znajduje oparcie nie tylko w przedstawionych wyżej wynikach badań. Są one w zasadzie jedynie „barometrem nastrojów" panujących wśród polskich funkcjonariuszy policji pytanych o to, jak dają sobie radę ze zwalczaniem przestępczości internetowej. Miejsca na bardziej szczegółowe wypowiedzi, odnoszące się do konkretnych mankamentów rozwiązań prawno-organizacyjnych obecnego systemu, kwestionariusz ankiety nie przewidywał. Mimo to część respondentów przedstawiła swoje uwagi na ten temat. Starano się je wykorzystać w poniższym podsumowaniu rezultatów badań, w szczególności przy formułowaniu postulatów i sugestii dotyczących zmian aktualnego stanu rzeczy.

3.1. Organizacja i koordynacja

Jak wynika z ankiety, zwalczanie oszustw internetowych w ramach istniejących aktualnie w polskiej policji struktur jest nie najlepsze i rodzi szereg konfliktów natury prawnej i organizacyjnej. Specyfika wykrywania, ścigania i zwalczania przestępstw z wykorzystaniem technik komputerowych jest odmienna od procedur wykrywczych stosowanych w wydziałach kryminalnych czy też wydziałach do walki z przestępczością gospodarczą (PG). Coraz częściej dowody popełnienia przestępstwa mają charakter cyfrowy. Dochodzi do sytuacji, że wydziały PG prowadzą postępowania o zabójstwa, narkotyki czy handel żywym towarem tylko dlatego, że ślady tych przestępstw mogą znajdować się w internecie lub na nośnikach cyfrowych. Przekazanie tych zadań CBŚ nie jest najlepszym rozwiązaniem, chociaż w ostatnich latach to właśnie w CBŚ KGP znajdowała się jednostka organizacyjna, która mogłaby koordynować zwalczanie cyberprzestępczości. Mogłaby, gdyż w praktyce nie miała żadnych możliwości wpływania na wydziały spoza CBŚ, a dodatkowo jej stan etatowy nie był zbyt liczny. W praktyce wciąż jest trudno o jakąkolwiek koordynację na szczeblu centralnym, na przykład rolę koordynatora spraw związanych z użytkownikiem

dokonującym oszustw na aukcjach allegro.pl gra Allegro. Policjanci występujący do Allegro o udzielenie informacji o oszukańczej aukcji lub oszuście od Allegro dowiadują się, że inne jednostki również prowadzą sprawy w związku z działaniem tego użytkownika. Centralna jednostka w składzie CBŚ częściej pełniła funkcję punktu kontaktowego z zagranicą oraz dobrze reprezentowała polską policję na wszelkiego rodzaju szkoleniach i konferencjach zagranicznych.

Od listopada 2005 r. funkcjonuje Wydział Zaawansowanych Technologii Informatycznych Biura Wywiadu. Czy będzie realizował zadania koordynacyjne? Działając w strukturach Biura Wywiadu, raczej nie. Działając w innej strukturze, mógłby pełnić funkcje koordynacyjne w zakresie cyberprzestępczości wobec wydziałów PG lub kryminalnych. Uzasadniony wydaje się w tej sytuacji postulat stworzenia w policji odrębnych jednostek organizacyjnych, na przykład wydziałów do zwalczania cyberprzestępczości w strukturach komend wojewódzkich, z powołaniem ich delegatur w komendach miejskich i powiatowych, które z kolei objęłyby nadzorem komisariaty policji[18].

3.2. Szkolenia

Policyjne szkolenia w zakresie zwalczania przestępczości komputerowej, zdaniem wielu respondentów, to raczej towarzyskie spotkania z różnymi grupami lobbingowymi niż autentyczne, odpowiednio przygotowane pod względem merytorycznym formy kształcenia policjantów. Skuteczne szkolenia winny być prowadzone przez praktyków zajmujących się różnymi aspektami cyberprzestrzeni. Powinny być bardziej ukierunkowane na techniczną, praktyczną stronę zagadnienia. Szkolenia powinny dawać biorącym w nich udział konkretne uprawnienia (w postaci świadectw, certyfikatów), tak aby policjanci ci mogli później występować przed sądami w charakterze biegłych lub ekspertów. Namiastką takiego szkolenia jest specjalistyczny kurs nt. uzyskiwania informacji z internetu prowadzony od 2005 r. przez Wyższą Szkołę Policji w Szczytnie przy współpracy z CERT Polska, allegro.pl, onet.pl, wp.pl, VISA Europe.

3.3. Przepisy prawne

Obowiązujące przepisy karne dotyczące przestępczości komputerowej są raczej wystarczające. Brak jest natomiast stosownych przepisów związanych z procedurami postępowania z nośnikami informacji, ich zabezpieczenia oraz współpracy z instytucjami z innych państw. Przewlekłość procedur i brak wdrożonych międzynarodowych regulacji uniemożliwiają szybki dostęp do informacji, a w konsekwencji ustalenie i ujęcie sprawcy czynu. Kłopotliwe jest respektowanie właściwości miejscowej orga-

[18] Zaplanowana w 2007 r. kolejna reforma zakłada, że w Komendach Wojewódzkich Policji powstaną zespoły wsparcia zwalczania cyberprzestępczości, których zadaniem będzie „uzyskiwanie i przetwarzanie informacji (w szczególności z sieci Internet), ustalanie danych abonenta, adresów IP oraz danych ruchowych, a także monitoring i rozpoznanie sieci Internet". Na szczeblu centralnym, w KGP funkcjonować będzie Wydział Zaawansowanych Technologii Biura Kryminalnego, nadzorujący pracę zespołów wojewódzkich, spośród których część będzie odgrywała rolę koordynatorów zwalczania określonego rodzaju przestępczości, np. pornografii dziecięcej, propagowania nielegalnych treści, oszustw internetowych. Reforma zakłada również wzmocnienie etatowe komórek stanowiących podstawę nowych zespołów i przeprowadzenie specjalistycznych szkoleń dla funkcjonariuszy tych zespołów.

nów ścigania związanej z miejscem popełnienia przestępstwa, zwłaszcza gdy mamy do czynienia z przypadkami zaangażowania w działalność przestępczą w sieci wielu osób o różnym miejscu zamieszkania. Niestety, właściwość miejscowa jest „świętością" samą w sobie dla prokuratur i ważniejszym staje się spór kompetencyjny niż podjęcie sprawy i wydanie stosownych decyzji. Obserwacja praktyki wyraźnie wskazuje, że w tym zakresie powinny zostać zmienione przepisy, aby właściwą do prowadzenia postępowania była prokuratura dla miejsca ujawnienia czynu lub pierwsza, która o czynie została powiadomiona (grozi to jednak tym, że sprawę prowadzić będzie jednostka zupełnie do tego nieprzygotowana).

3.4. Wyposażenie

Aby mówić o efektywnym wykrywaniu sprawców przestępstw komputerowych oraz śladów i dowodów cyfrowych, niezbędne jest bardzo poważne podejście do zagadnienia wyposażenia policji w odpowiednie środki techniczne. Bez specjalistycznego wyposażenia w sprzęt komputerowy (nie tylko same komputery) i odpowiednie aplikacje nie można myśleć o rzetelnym podejściu do zwalczania przestępczości komputerowej. Posiadanie przez policję takiego sprzętu i odpowiednio przeszkolonych funkcjonariuszy z uprawnieniami daje możliwość szybkiego reagowania, zapewnia niezależność od instytucji zewnętrznych i pewność działania. Pamiętać należy, że w zakresie technik komputerowych wielu policjantów dysponuje dużą wiedzą nabytą na szkoleniach zagranicznych realizowanych w ramach PHARE.

3.5. Współpraca

Współpraca policjantów zwalczających oszustwa komputerowe w większości przypadków dotyczy osób prywatnych, z którymi policjanci nawiązali osobiste kontakty i od których nauczyli się wielu rzeczy. Formalna współpraca w ramach policji praktycznie nie istnieje, poza nie najlepiej funkcjonującą oficjalną wymianą informacji (wielokrotnie powielanej, często niekompletnej i bardzo opóźnionej). Informacje w większości przypadków traktowane są marginalnie i lakonicznie - jako przestępstwo gospodarcze lub komputerowe - w takiej postaci są wprowadzane do systemów informatycznych policji (Kosiński 2003, s. 547). Więcej pożytku daje wymiana informacji z instytucjami pozapolicyjnymi niż z samymi jednostkami policji. Zresztą w niejednym przypadku jest to najlepszy i najszybszy sposób uzyskania różnych informacji.

Z doświadczeń respondentów wynika, że warto mówić, w kontekście wyników tej ankiety, nie tylko o oszustwach komputerowych. Czynności podejmowane przez policję w zakresie przestępczości komputerowej dotyczą spraw o groźby karalne, pornografię, narkotyki, rozpowszechnianie treści rasistowskich i antyżydowskich, szerzenie idei nazistowskich, rozbojów, awantur ulicznych z udziałem kibiców, skończywszy na handlu żywym towarem, samochodami bądź innymi przedmiotami pochodzącymi z kradzieży i wyłudzeń oraz na sprawach o rozpowszechnianie utworów i produktów wbrew przepisom, oszustwach bankowych i wielu innych. Ten „uniwersalizm" polskich policjantów zwalczających cyberprzestępczość zapewne w sposób pozytywny odróżnia ich od policjantów amerykańskich.

LITERATURA

Adamski A. (1999). „Crimes related to computer network. Threats and opportunities: A criminological perspective", w: M. Joutsen (red.), *Five Issues in European Criminal Justice: Corruption, Women in the Criminal Justice System, Criminal Policy Indicators, Community Crime Prevention, and Computer Crime.* Helsinki: HEUNI, Publication Series No. 34.

Adamski A. (2001). *Prawo karne komputerowe.* Warszawa: C.H. Beck.

Adamski A. (2005). „Oszustwo komputerowe a oszustwo internetowe", w: J. Kosiński (red.), *Przestępczość teleinformatyczna.* VIII Seminarium naukowe, Szczytno.

Adamski A. (2006). „Cyberprzestępczość, aspekty prawne i kryminologiczne", *Studia Prawnicze* 2005, nr 4(166).

Burns R.G., Witworth K.H., Thompson C.Y. (2004). „Assessing law enforcement preparedness to address Internet fraud", *Journal of Criminal Justice,* nr 32.

Chen Ying-Chieh i in. (2005). „An analysis of online gaming crime characteristics", *Internet Research,* t. 15, nr 3.

Correia M., Bowling C. (1999). „Veering towards digital disorder: Computer-related crime and law enforcement preparedness", *Police Quarterly,* t. 2, nr 2.

Davis D.J. (1989). „Criminal law and the Internet: The investigator's perspective, *The Criminal Law Review,* Special edition, *Crime, Criminal Justice and the Internet.*

Goodman M. (1997). „Why the police don't care about computer crime", *Harvard Journal of Law and Technology,* t. 10, nr 3, http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech465.pdf.

Hinduja S. (2004). „Perceptions of local and state law enforcement concerning the role of computer crime investigative teams", *Policing: An International Journal of Police Strategies & Management,* t. 27, nr 3.

Huey L.J. (2002). „Policing the abstract: Some observations on policing cyberspace", *Canadian Journal of Criminology,* t. 44, nr 3.

Icove D., Seger K., Von Stroch W. (1995). *Computer Crime. A Crimefighter's Handbook.* Sebastopodl, CA.

Kabay M.E. (2001). *Studies and surveys of computer crime,* http ://www.securitystats.com/reports/Studies_and_Surveys_of_Computer_Crime.pdf.

Kosiński J. (2003). „Przestępczość komputerowa w statystyce policyjnej", w: T. Zasępa, R. Chmura (red.), *Internet i nowe technologie - ku społeczeństwu przyszłości.* Częstochowa: Edycja świętego Pawła.

McGuire D. (2004). „House OKs More Jail Time for ID Thieves", *Washington Post,* 23 czerwca, http://www.washingtonpost.com/wp-dyn/articles/A190-2004Jun23.html.

Newman G.R. (2004). „Identity theft, U.S. Department of Justice", *Office of Community Oriented Policing Services.*

Smith R., Grabosky P, Urbas G. (2004). *Cyber Criminals on Trial.* The Press Syndicate of the University of Cambridge.

Sommer P. (2004). „The future for the policing of cybercrime", *Computer Fraud and Security,* nr 1.

Stambaugh H., Beaupre D., Icove D.J., Cassaday W., Williams W.P. (2000). „State and local law enforcement needs to combat electronic crime". National Institute of Justice, *Research in Brief,* sierpień.

Stefański R.A. (2006). „Przestępstwa internetowe w Polsce. Analiza praktyki", *Studia Prawnicze,* nr 4(166) 2005.