PRZESTĘPCZOŚĆ TELEINFORMATYCZNA 2016

pod redakcją
Jerzego Kosińskiego

Szczytno 2017

Recenzenci
dr hab. Andrzej Adamski
dr hab. Grzegorz Krasnodębski

Redakcja Wydawcy
Piotr Cyrek
Beata Miszczuk
Robert Ocipiński

ISBN 978-83-7462-562-3
e-ISBN 978-83-7462-563-0

Druk i oprawa:
Dział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie
ul. Marszałka Józefa Piłsudskiego 111, 12-100 Szczytno
tel. 089 621 51 02, faks 089 621 54 48
e-mail: wwip@wspol.edu.pl
Objętość: 17,81 ark. wyd. (1 ark. wyd. = 40 tys. znaków typograficznych)

SPIS TREŚCI

WSTĘP

Z badania Centrum Badania Opinii Społecznej nt. korzystania z Internetu[1], które było przeprowadzone w dniach 5–12 maja 2016 roku wynika, że z Internetu regularnie (przynajmniej raz w tygodniu) korzysta dwie trzecie dorosłych Polaków (65%). Większość korzystających z Internetu (86%, czyli 56% ogółu badanych) łączy się z siecią bezprzewodowo — poprzez takie urządzenia, jak smartfon, tablet czy laptop. Przynajmniej raz kupiła coś przez Internet ponad połowa ogółu dorosłych (53%, czyli 81% użytkowników Internetu), a sprzedała — jedna piąta (20%, czyli 31% internautów). Dwie trzecie korzystających z Internetu (66%), czyli 43% ogółu dorosłych, korzysta z bankowości elektronicznej. Niemal co trzeci użytkownik Internetu (31%, czyli 20% ogółu badanych) wypowiadał się w ostatnim miesiącu na forach dyskusyjnych lub stronach portali społecznościowych. Znajomość w Internecie zawarł co siódmy dorosły (14%, czyli 22% korzystających z Internetu), a z osobą poznaną online spotkał się osobiście niemal co dziesiąty badany (9%, czyli 13% użytkowników Internetu).

Jednocześnie z badania tej samej firmy przeprowadzonego w dniach 1–8 lipca 2015 roku nt. bezpieczeństwa w Internecie[2] wynika niemal powszechne wśród internautów (91%) poczucie, że sposób, w jaki korzystają z Internetu, można określić jako bezpieczny. Odmiennie swoją obecność w sieci postrzega zaledwie sześciu na stu badanych (6%), przy czym prawie wszyscy z nich (5%) wskazują na umiarkowany poziom ryzyka. Dwie trzecie użytkowników sieci (a 55%, jeśli pominąć dość często deklarowane, ale w największym stopniu zależne od użytkownika nadużywanie Internetu i kontakt z nieprawdziwymi informacjami) miało jakieś negatywne doświadczenia związane z obecnością online. Najczęściej dotyczyły one zainfekowania komputera wirusem lub innym szkodliwym programem (41%), rzadziej — bycia przez kogoś obrażonym (13%) lub nieintencjonalnego kontaktu z obraźliwymi treściami (10%), zawarcia znajomości z osobą, która podawała się za kogoś innego, niż była w rzeczywistości (9%), jeszcze rzadziej — zostania oszukanym (8%), a sporadycznie — spotkania się z nieprawdziwymi informacjami na swój temat (7%), podszycia się pod nich korzystając z ich poczty lub konta w portalu społecznościowym (6%) lub padnięcia ofiarą kradzieży (5%).

Zupełnie inny obraz, dużo bezpieczniejszy, wynika z Polskiego Badania Przestępczości zrealizowanego na przełomie stycznia i lutego 2016 roku[3]. Według tego badania jedynie co szósty Polak zetknął się w jakiś sposób z cyberprzestępczością

---

[1] <http://www.cbos.pl/SPISKOM.POL/2016/K_092_16.PDF>, dostęp: 28 października 2016 r.

[2] <http://cbos.pl/SPISKOM.POL/2015/K_109_15.PDF>, dostęp: 28 października 2016 r.

[3] <http://www.gazeta.policja.pl/997/informacje/128932,GUS-CBOS-Polskie-Badanie-Przestepczosci.html>, dostęp: 28 października 2016 r.

w Internecie (16,4%). Również struktura obserwowanych zagrożeń wygląda w tym badaniu inaczej. 40% spośród badanych z tej grupy natknęło się w Internecie na obraźliwe wypowiedzi użytkowników sieci lub zakłócenia (paraliż) funkcjonowania systemu informatycznego (odpowiednio 40,9% i 39,6% wskazań). Około jedna czwarta została przekierowana na fałszywą stronę internetową, np. w celu wyłudzenia pieniędzy lub zetknęła się z bezprawnym kopiowaniem, rozpowszechnianiem lub publikowaniem prawnie chronionej własności intelektualnej (odpowiednio 28,9% i 22,9% wskazań). Relatywnie rzadziej ankietowani wskazywali na przypadki włamania na konto społecznościowe (16,7%) lub pocztę elektroniczną (12,7%) czy wyłudzania/nieuczciwego wykorzystywania danych (np. numeru karty kredytowej, danych osobowych). Najrzadziej badani doświadczali: włamań na konto bankowe (6,9%), kradzieży przedmiotów lub postaci z gier komputerowych (8,0%), zamieszczania przez niepowołane osoby ich prywatnych filmów, zdjęć lub wartości intelektualnej (9,4%), kontaktu ze stronami zawierającymi pornografię dziecięcą (9,5%) oraz sytuacji związanych z przestępczością telekomunikacyjną (10,7%).

W 2016 roku Polska gościła misję ewaluacyjną Grupy Roboczej ds. Ogólnych i Oceny (GENVAL) przy Radzie Unii Europejskiej. VII runda ocen wzajemnych jest poświęcona problematyce praktycznego wdrożenia i funkcjonowania europejskiej polityki prewencji i zwalczania cyberprzestępczości. Przedmiotem oceny są w tej rundzie przede wszystkim trzy kwestie: cyberataki, wykorzystywanie seksualne dzieci/pornografia dziecięca w Internecie oraz internetowe oszustwa dotyczące kart płatniczych, w tym kompleksowa prawno-operacyjna analiza walki z cyberprzestępczością, współpracy transgranicznej i współpracy z agencjami UE (Europol, Eurojust, ENISA). Ponadto zakres ewaluacji obejmuje współpracę z sektorem prywatnym oraz problematykę prewencji, szkoleń i kampanii informacyjnych w powyższym obszarze[4]. Ocena była dokonana na podstawie przygotowanego przez Ministerstwo Administracji i Cyfryzacji, Ministerstwo Edukacji Narodowej, Ministerstwo Finansów, Ministerstwo Nauki i Szkolnictwa Wyższego, Ministerstwo Obrony Narodowej, Ministerstwo Sprawiedliwości, Ministerstwo Spraw Wewnętrznych i ich jednostki podległe oraz nadzorowane kwestionariusza, a także wizyt studyjnych i spotkań. Dominującą rolę w sporządzeniu kwestionariusza odegrały Wydziały do Walki z Cyberprzestępczością i do Walki z Przestępczością Gospodarczą Biura Służby Kryminalnej Komendy Głównej Policji. Wstępna ocena przedstawiona przez członków misji ewaluacyjnej[5], wbrew wypowiedziom prokuratora krajowego[6], była bardzo pozytywna,

[4] Zgodnie z treścią dokumentu „VII runda wzajemnych ocen — kwestionariusz" (5335/1/14).

[5] Raport nie był jeszcze przedstawiany na spotkaniu GENVAL (31 lipca 2016 r.). Stan na 28 października 2016 r.

[6] <http://www.cyberdefence24.pl/344757,cybersec-pl-prokurator-krajowy-chce-powola nia-naro dowej-agencji-cyberbezpieczenstwa>, dostęp: 28 października 2016 r.

z pewnymi wyjątkami. Tę wstępną ocenę potwierdzają także informacje o kilku bezprecedensowych sukcesach Policji w walce z cyberprzestępcami. Niewiele Policji może pochwalić się serią zatrzymań czołowych przestępców działających w sieci TOR. Dzięki dobrej współpracy z sektorem prywatnym polska Policja zatrzymała w 2015 i wiosną 2016 roku:

— 25-letniego Artura P. (The Venom Inside) oraz 21-letniego Łukasza W. (Kyber)[7]. W okresie od listopada 2013 r. do lutego 2015 r. ukradli oni ponad 2 miliony złotych z kont bankowych 5 gmin;
— 33-letniego Tomasza G. (Polsilver)[8]. Polsilver był jednym z administratorów ToRepublic, dostawcą rachunków bankowych zarejestrowanych na podstawione osoby, tzw. słupy, a także uczestniczył we włamaniu do Plus Banku;
— 22-letniego Jakuba S. (CharlieTheUnicorn)[9]. Dostawca rachunków bankowych zarejestrowanych na podstawione osoby. Prawdopodobnie wcześniej występował na ToRepublic pod pseudonimem Francuz47;
— 35-letniego Mateusza C. (Polly Pocket)[10]. Pocket uczestniczył we włamaniu do Plus Banku, ale był znany w podziemiu internetowym głównie z kradzieży plików z listami należącymi do kapitana ABW i publikacji jego profilu.

Do tych sukcesów należy dodać rozbicie międzynarodowej zorganizowanej grupy przestępczej, która od 2012 roku okradała klientów banków[11]. Za pomocą wirusa Tinba i stron phishingowych wykradli łącznie ponad 94 mln zł.

Z dużą przyjemnością należy podkreślić, że w powyższych sukcesach aktywny udział miało wielu uczestników, w niektórych przypadkach można rzec regularnych, poprzednich edycji konferencji „Techniczne aspekty przestępczości teleinformatycznej".

W 2016 roku organizatorami XIX Międzynarodowej Konferencji Naukowej byli: Instytut Badań nad Przestępczością Kryminalną i Terroryzmem, działające w nim Centrum Analityczno-Wywiadowcze i Doskonalenia Zwalczania Cyberprzestępczości przy współpracy Grupy Allegro Sp. z o.o. W konferencji uczestniczyło 301 uczestników z Polski, Hiszpanii, Litwy, Rosji, Rumunii, Stanów Zjednoczonych, Wielkiej Brytanii. W czasie konferencji wygłoszono 32 referaty i przeprowadzono liczne warsztaty. Tradycyjnie, oprócz tematu przewodniego, na konferencji zostały poruszone także inne pokrewne tematy, m.in.:

---

[7] <https://zaufanatrzeciastrona.pl/post/ogromny-sukces-polskiej-policji-administratorzy-torepublic-zatrzymani/>, dostęp: 28 października 2016 r.

[8] <http://www.policja.pl/pol/aktualnosci/117795,Haker-quotPolsilverquot-w-rekach-Policji.html?search=404554223>, dostęp: 28 października 2016 r.

[9] <http://srodmiescie.policja.waw.pl/rs/aktualnosci/60520,Na-zakladane-konta-wyplywaly-pieniadze-pochodzace-z-przestepstwa.html>, dostęp: 28 października 2016 r.

[10] <http://cbsp.policja.pl/cbs/aktualnosci/125964,Pocket-w-rekach-policji-dzialal-z-Polsilverem.html>, dostęp: 28 października 2016 r.

[11] <http://www.policja.pl/pol/aktualnosci/125178,Policjanci-i-prokuratorzy-rozbili-miedzynarodowa-zorganizowana-grupe-przestepcza.html?search=79651>, dostęp: 28 października 2016 r.

obserwowane trendy cyberprzestępczości, bezpieczeństwo teleinformatyczne i elektronicznych instrumentów płatniczych (także kryptowalut), bezpieczeństwo danych osobowych, monitorowanie zagrożeń w Internecie, ujawnianie, pozyskiwanie, zabezpieczanie, analiza i prezentacja dowodów cyfrowych, praktyka zwalczania cyberprzestępczości oraz narzędzia wspomagające zwalczanie cyberprzestępczości (zarówno komercyjne, jak i opracowywane samodzielnie przez funkcjonariuszy). Wszystko było rozważane w kontekście i z podkreśleniem wagi współpracy publiczno-prywatnej w zwalczaniu cyberprzestępczości.

Wprowadzające w tematykę konferencji wystąpienia wygłosili zastępca komendanta — prorektor Wyższej Szkoły Policji w Szczytnie — insp. dr Danuta Bukowiecka oraz kierownik ds. Współpracy z Organami Ścigania, Grupa Allegro Sp. z o.o. — Jakub Pepłoński. W pierwszym dniu konferencji wygłoszono następujące referaty:

— *Wyniki kontroli NIK* — Joanna Karczewska, ISACA Warszawa;
— *Cyber Intelligence: what's this about?* — Raoul «Nobody» Chiesa, President, Security Brokers;
— *IRT: a definitive solution* — Alberto Pelliccione, ReaQta (wykład z demonstracją poprowadzony przez Internet);
— *Czym się różni SOC od CERT?* — Mirosław Maj, Tomasz Chlebowski, ComCERT;
— *Praktyczne aspekty szkolenia Policji w obszarze Cyber* — opis wdrożenia pilotażowego uruchomionego w szkole podczas TAPT — Sebastian Madden, PGI;
— *Malvertising — attacks' history and effective countermeasures* — Adam Nowak, EY;
— *Chip-off digital forensics. The myth about data deletion* — Sasha Sheremetov, Rusolut;
— *Bezprzewodowe niebezpieczeństwo* — Adam Ziaja, Deloitte; Maciej Grela, Exatel;
— *Bezpieczeństwo sieci radiowych w aspekcie nowych technologii i nowych ataków kryptograficznych* — Zbigniew Jakubowski, Compendium;
— *Wyłudzenia danych osobowych w serwisie OLX. Studium przypadku* — Paula Drozdowska, Grupa Allegro; Grzegorz Filipek, KWP w Opolu.

W pierwszym dniu konferencji rozpoczęły się także warsztaty przygotowane przez firmy PGI i Matic z zakresu technik śledczych. Uczestnicy warsztatów szkolili się z zakresu poprawnego tworzenia kopii dysku lokalnego (obraz), a następnie wykonywali obrazy dysków zdalnych z wykorzystaniem połączenia sieciowego. Dokonywali zrzutu pamięci operacyjnej (*memory capture*) systemu w trakcie jego pracy, w celu przystąpienia do analizy jej zawartości i ekstrakcji informacji systemowych, np. rejestrów i połączeń sieciowych. W czasie warsztatów zatytułowanych „Metasploit dla oficerów śledczych" poznawali wykorzystanie Metasploit do celów ofensywnych, w celu zrozumienia *modus operandi*

przestępców wykorzystujących to narzędzie. Uczyli się, jak nawigować i posługiwać się Metasploit, jak wybierać cele, atakować, jak gromadzić informacje z zaatakowanego systemu oraz jak zakładać backdoor'y na komputerach, do których włamali się, a także jak utrzymać długoterminowy dostęp do nich.

Drugiego dnia, oprócz sesji plenarnej, na której wygłoszono cztery wystąpienia:

— *Wielki skok na impulsy telefoniczne… czyli zarabianie przez przełamanie* — studium przypadku — Krzysztof Śliwa, Orange; Grzegorz Dzikowski, KSP;
— *Specyfika funkcjonowania giełdy kryptowalut. Współpraca giełdy z organami ścigania w obszarze wykrywania sprawców cyberprzestępstw* — Sylwester Suszek, BitBay.pl; Maciej Bojczuk, KWP we Wrocławiu;
— *Virtual Currencies and Western Union assistance to Law Enforcement in identifying suspects* — Ričardas Pocius, Western Union;
— *Studia przypadków* — Piotr Gradkowski, KSP;

przeprowadzono cztery sesje w dwóch równoległych ścieżkach. W ścieżce „bankowej" wygłoszono następujące wystąpienia:

— *Nowe trendy w zakresie płatności z perspektywy instytucji płatniczej* — Anna Adamska, Jarosław Biegański, PayU;
— *Incydent cieszyński, czyli jak upiec dwie pieczenie na jednym ogniu* — Maria Ciempka, ING Bank Śląski; Marcin Cyganek, KWP w Katowicach;
— *Możliwości pozyskania i wykorzystania danych kart płatniczych w Internecie, studium przypadku* — Maciej Bojczuk, KWP we Wrocławiu; Jakub Kalinowski, Grupa Allegro oraz Virgiliu Pintea, oficer łącznikowy Policji rumuńskiej;
— *Przestępczość bankomatowa z użyciem technologii teleinformatycznych* — Tomasz Kielich, Euronet Polska; Robert Jabłoński, KSP;
— *Ataki tinbą na systemy księgowe* — Kamila Grudnik, KWP Kielce;
— *Studium przypadku — fałszywa sprzedaż w Internecie* — Piotr Gradkowski, KSP, Wiesław Siedzik, Pekao SA;
— *Metodyka odzyskiwania nagrań z rejestratorów monitoringu* — Bartosz Kowalski, IES Kraków;
— *Techniki deanonimizacji w Internecie* — Piotr Konieczny, Niebezpiecznik.pl;
— *Kto kryje się za awatarem?* — Maciej Kołodziej, E-detektywi.

Natomiast w sesji poświęconej zarządzaniu bezpieczeństwem:

— *Zarządzanie incydentami* — Krzysztof Liderman, Wydział Cybernetyki, Wojskowa Akademia Techniczna;
— *Automatyzacja procesów bezpieczeństwa kluczem do minimalizacji ryzyk w IT* — Marek Krauze, TrendMicro;
— *Jednostki typu Security Operation Center jako odpowiedź na zwiększające się cyberzagrożenia* — Bartosz Zieliński, EY;
— *Security Operations Centers* — Albert Borowski, Comp SA;
— *Trudności w ustaleniu tożsamości użytkownika usługi telekomunikacyjnej* — Paweł Baraniecki, Polkomtel;

— *Analiza logów systemów teleinformatycznych w procesie analizy kryminalnej — dostępne narzędzia* — Aleksander Goszczycki, Matic; Tomasz Rostkowski, IBM Polska;
— *Wirtualna tożsamość administracji państwowej* — Joanna Karczewska, ISACA Warszawa;
— *Duńska szklarnia* — Jarosław Cholewiński, KWP Lublin;
— *Konsekwencje Dyrektywy NIS* — Krzysztof Silicki, NASK.

W drugim dniu przeprowadzono także drugą serię warsztatów, w których pojawiły się dwa nowe tematy — malware oraz botnety i narzędzia zdalnego dostępu (RAT). W pierwszym z tematów wykorzystano malware (Dark Comet), by zainfekować system ofiary oraz doświadczyć ataku zarówno z perspektywy przeprowadzającego atak oraz ofiary. W drugim z warsztatów utworzono, uruchomiono oraz operowano narzędziami zdalnego dostępu oraz botnetami z jednego centrum kontroli, a celem było zrozumienie techniki wykorzystywanej przez cyberprzestępców jako krok przygotowawczy do popełniania przestępstwa właściwego.

W ostatnim, trzecim dniu konferencji wygłoszono następujące referaty:
— *Triage i alternatywa dla mniej zaawansowanych* — Tomasz Boroń, KWP w Bydgoszczy;
— *Artefakty z polskiej przestrzeni internetowej* — Daniel Konwiński, KWP w Bydgoszczy;
— *Data recovery from broken Windows Phone with TexFAT* — Piotr Rzuchowski, MiP Data Recovery;
— *BitLocker z perspektywy informatyki śledczej* — Krzysztof Bińkowski, NetComputer;
— *Analiza śledcza drona* — Witold Sobolewski, VS Data;
— *Metodyka badania podobieństwa oprogramowania systemów IT na potrzeby procesu sądowego o naruszenie praw autorskich* — Andrzej Stasiak, Zbigniew Zieliński, Wydział Cybernetyki, Wojskowa Akademia Techniczna;
— *Deanonimizacja bitcoin* — Stefan Dziembowski, Instytut Informatyki, Uniwersytet Warszawski.

Zebranie w monografii 18 rozdziałów będących rozwinięciem i uszczegółowieniem wystąpień z konferencji TAPT, ale także poruszających nieprezentowane na konferencji tematy powinno być atrakcyjne dla wielu czytelników zainteresowanych cyberprzestępczością. Będą one także przydatne dla studentów i wszystkich osób, które zajmują się zapewnieniem bezpieczeństwa wykorzystania nowoczesnych technologii teleinformatycznych oraz ściganiem sprawców cyberprzestępstw.

Jerzy KOSIŃSKI

Rozdział 1

ANALIZA PERCEPCJI CYBERPRZESTĘPCZOŚCI W ŚRODOWISKU EKSPERCKIM

dr inż. Paweł CISZEK[1]

STRESZCZENIE: W rozdziale przedstawiono omówienie wyników badań nad percepcją zjawiska cyberprzestępczości przez środowisko eksperckie przeprowadzonych metodą ankietową i pogłębionego wywiadu w 2015 roku. Głównym celem badań było znalezienie odpowiedzi na kwestie dotyczące poglądów i opinii środowiska wobec samego zjawiska cyberprzestępczości, jak i opinii co do uprawnionych służb i organów w zakresie zwalczania cyberprzestępczości z uwzględnieniem kwestii działań organizacyjnych oraz wsparcia tych służb przez środowiska naukowe i sektor prywatny, z podkreśleniem roli, miejsca, zakresu i formy działań Policji.

SŁOWA KLUCZOWE: cyberprzestępczość, Policja, bezpieczeństwo narodowe, system, współpraca.

Niepowtarzalna okazja wykorzystania potencjału intelektualnego, jaki zogniskowany jest wokół cyklicznej międzynarodowej Konferencji Techniczne Aspekty Przestępczości Teleinformatycznej organizowanej w Wyższej Szkole Policji pozwoliły autorowi na przeprowadzenie badań ankietowych oraz pogłębionych wywiadów eksperckich, w których starał się znaleźć odpowiedzi na nurtujące pytania związane ze zjawiskiem cyberprzestępczości. Do głównych zagadnień, również w aspekcie bezpieczeństwa narodowego, należały:

— percepcja definicji zjawiska cyberprzestępczości;
— związki cyberprzestępczości z bezpieczeństwem narodowym;
— rola, miejsce, zadania i zakres działań służb zajmujących się przeciwdziałaniem cyberprzestępczości;
— identyfikacja zakresu i poziomu organizacji przeciwdziałania cyberprzestępczości w Policji;
— przesłanek pozwalających na doskonalenie organizacji przeciwdziałania cyberprzestępczości w Policji;
— poziom wiedzy oraz zakres wykorzystania możliwości świata nauki we wspomaganiu przeciwdziałania cyberprzestępczości;
— poziom wiedzy oraz zakres wykorzystania możliwości podmiotów sektora prywatnego we wspomaganiu przeciwdziałania cyberprzestępczości.

Kwestionariusz ankiety zawierał sporządzone i poddane wszechstronnej analizie pytania, stwierdzenia i określenia obejmujące sformułowany i uzasadniony

[1] Wyższa Szkoła Policji w Szczytnie, p.ciszek@wspol.edu.pl.

problem badawczy[2]. Celem poprawienia jakości ankiety sporządzono pierwszą, próbną wersję, która została poddana wstępnej weryfikacji pod kątem jasności zadanych pytań, możliwości udzielenia jednoznacznej odpowiedzi oraz weryfikacji, czy zdaniem respondentów, zasadne jest umożliwienie im umieszczenia komentarza do poruszanych w pytaniach kwestii. Tak przygotowana ankieta testowana była na grupie słuchaczy kursów nt. „Zwalczania przestępczości w cyberprzestrzeni" organizowanych w Wyższej Szkole Policji. W etapie drugim, na podstawie zebranych sugestii oraz wstępnych badań zebranych wyników sporządzono drugą wersję ankiety, którą konsultowano z nauczycielami akademickimi w Wyższej Szkole Policji zajmującymi się kwestiami cyberprzestępczości. Po kolejnych badaniach, dzięki przychylności dra hab. Jerzego Kosińskiego po przedstawieniu dotychczasowych analiz powstała wersja trzecia ankiety, która jest przedmiotem analiz zamieszczonych w niniejszym rozdziale.

Ostateczne badania ankietowe prowadzone były w formie elektronicznej, zaś zaproszenie do badań przesłane zostało w formie e-mail do 173 osób, uczestników wspomnianej konferencji w 2014 roku oraz dodatkowo, pracowników wydziałów zwalczania cyberprzestępczości, zarówno w Komendzie Głównej Policji, jak i w komendach wojewódzkich.

W odpowiedzi wypełnionych zostało 86 ankiet, przy czym tylko 67 spośród nich zostało zakończonych przez respondentów, pozostałe zaś z nieznanych przyczyn zostały przerwane w trakcie udzielania odpowiedzi i w związku z tym nie zostały poddane szczegółowej analizie.

Opracowując uzyskane wyniki badań autor przyjął założenie, że wystąpią statystycznie istotne związki pomiędzy niektórymi odpowiedziami, dodatkowo w budowie ankiety uwzględniono logikę obejmującą pomijanie niektórych pytań w zależności od udzielonych wcześniej odpowiedzi. Takie możliwości zbudowania inteligentnej ankiety dała platforma Laboratorium Społeczno-Ekonomicznego LabSEE[3]. W badaniu respondenci poproszeni byli o ocenę zjawiska cyberprzestępczości, jego związków z bezpieczeństwem narodowym, ocenę faktycznej realizacji obowiązków państwa w zakresie przeciwdziałania temu zjawisku, jak i w szczególności wskazania relacji pomiędzy zjawiskiem cyberprzestępczości a działaniami Policji, zarówno w zakresie organizacyjnym, jak i technicznym,

[2] Por. T. Majewski, *Ankieta i wywiad w badaniach wojskowych,* Warszawa 2002, s. 15.

[3] LabSEE jest niezależnym centrum badawczym opartym o nowoczesne rozwiązania informatyczne. Stworzone zostało z myślą o zapewnieniu możliwości prowadzenia niezależnych badań jak najszerszemu gronu odbiorców. LabSEE pozwala skupić się na problemie badawczym, usuwając konieczność ciągłego poszukiwania odpowiedniego narzędzia. Zespół LabSEE tworzy i udostępnia bez opłat profesjonalny serwis ankietowy Moje-Ankiety.pl Serwis ten powstał, aby zaoferować wszystkim zainteresowanym badaniami narzędzie potrzebne do przeprowadzania ankiet przez Internet. Ze swojej strony staramy się, aby funkcje serwisu charakteryzowały się jak największym profesjonalizmem oraz przejrzystością i łatwością obsługi, <http://labsee.pl/>, dostęp: 16 maja 2014 r.

które ma podstawowe znaczenie dla realizacji celów ustawowych związanych z przeciwdziałaniem i zwalczaniem zjawiska. W części ostatniej zebrane zostały informacje dotyczące zarówno wieku, wykształcenia, jak i doświadczenia badanych.

Charakterystyka badanej populacji

Jak wspomniano wcześniej ankieta została rozesłana do 173 osób. W rezultacie pełną ankietę wypełniło 67 respondentów.

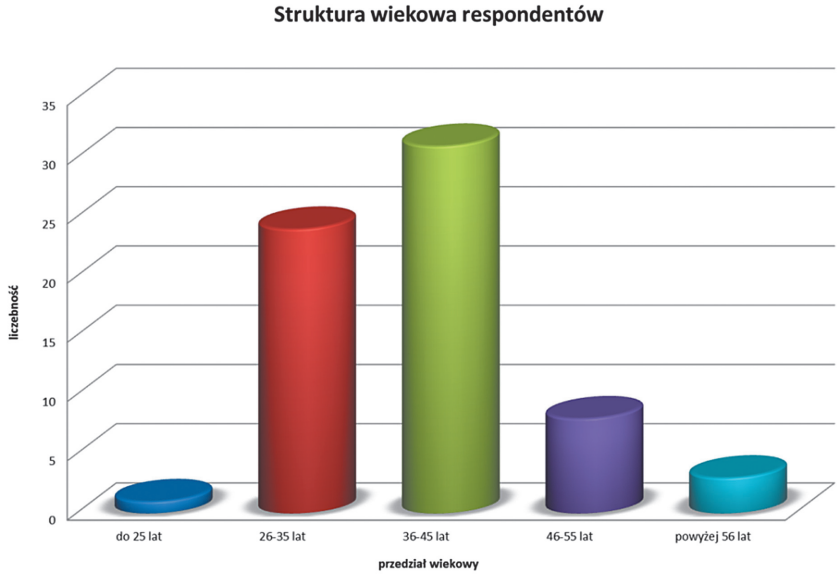
W przyjętej klasyfikacji wiek respondentów rozkłada się następująco:

Tabela 1. Struktura wiekowa respondentów badań ankietowych

Przedział wiekowy respondentów	Liczba respondentów
do 25 lat	1
26–35 lat	24
36–45 lat	31
46–55 lat	8
powyżej 56 lat	3
Razem	67

Źródło: badania własne

Wykres 1. Struktura wiekowa respondentów badań ankietowych



Źródło: badania własne

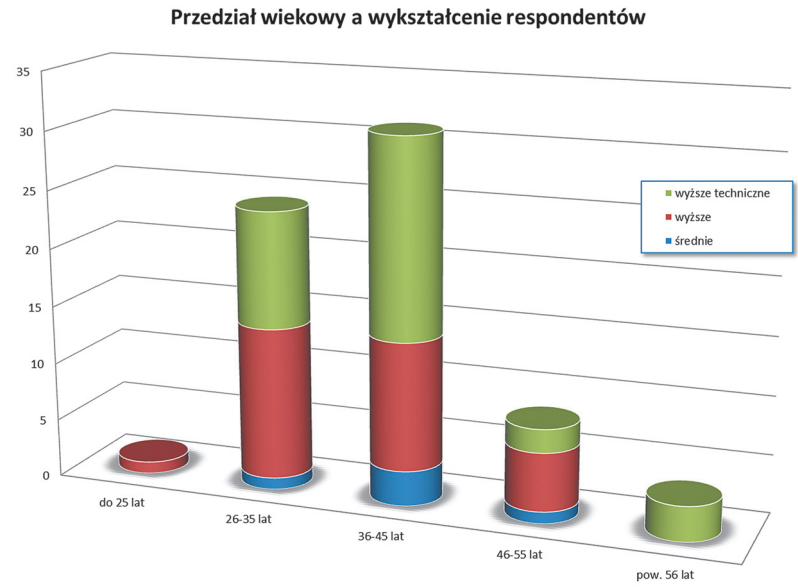
Znacząca większość badanych jest w przedziale od 26 do 45 lat. Są to osoby, które posiadają już w miarę ustabilizowaną sytuację zawodową, w większości z wyższym wykształceniem.

Tabela 2. Struktura wiekowa a wykształcenie respondentów badań ankietowych

Przedział wiekowy	Wykształcenie średnie	Wyższe	Wyższe techniczne	Razem
do 25 lat		1		1
26–35 lat	1	13	10	24
36–45 lat	3	11	17	31
46–55 lat	1	5	2	8
powyżej 56 lat			3	3
Razem	5	30	32	67

Źródło: badania własne

Wykres 2. Struktura wiekowa a wykształcenie respondentów badań ankietowych



Źródło: badania własne

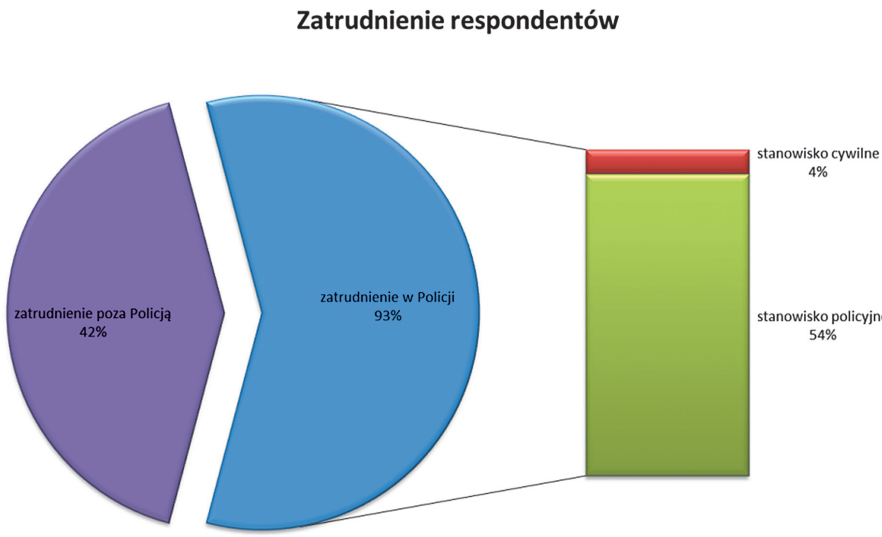
Istotne w badaniach było rozróżnienie na osoby będące i niebędące pracownikami Policji.

Tabela 3. Zatrudnienie respondentów badań ankietowych

Cenzus zatrudnienia	Liczba respondentów
zatrudnienie poza Policją	28
stanowisko cywilne w Policji	3
Policjant	36
Razem	67

Źródło: badania własne

Wykres 3. Zatrudnienie respondentów badań ankietowych



Źródło: badania własne

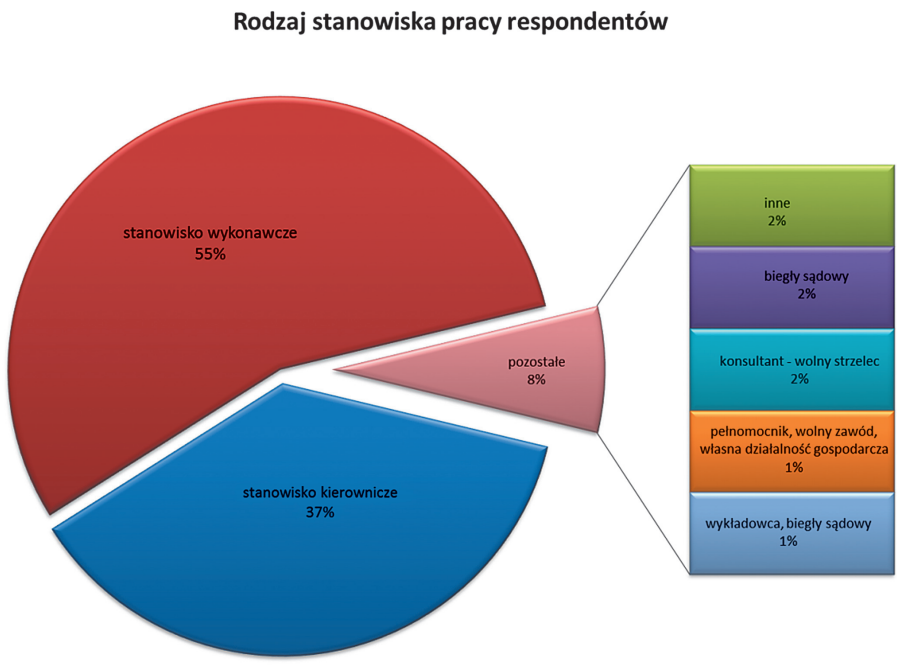
Istotne było także ustalenie rodzaju stanowiska, na którym pracują respondenci. Istotne było zbadanie, czy sposób postrzegania może być zależny od miejsca i rodzaju stanowiska, jakie zajmują badani.

Tabela 4. Rodzaj stanowiska zajmowanego przez respondentów badań ankietowych

Cenzus zatrudnienia	Liczba respondentów
stanowisko kierownicze	25
stanowisko wykonawcze	37
inne	1
biegły sądowy	1
konsultant — wolny strzelec	1
pełnomocnik, wolny zawód, własna działalność gospodarcza	1
wykładowca, biegły sądowy	1
Razem	67

Źródło: badania własne

Wykres 4. Rodzaj stanowiska zajmowanego przez respondentów badań ankietowych



Źródło: badania własne

Aby zachować pełny obraz zbiorowości osób będących pracownikami Policji wprowadzono pytanie, które pozwoliło podzielić tę część zbiorowości na osoby,

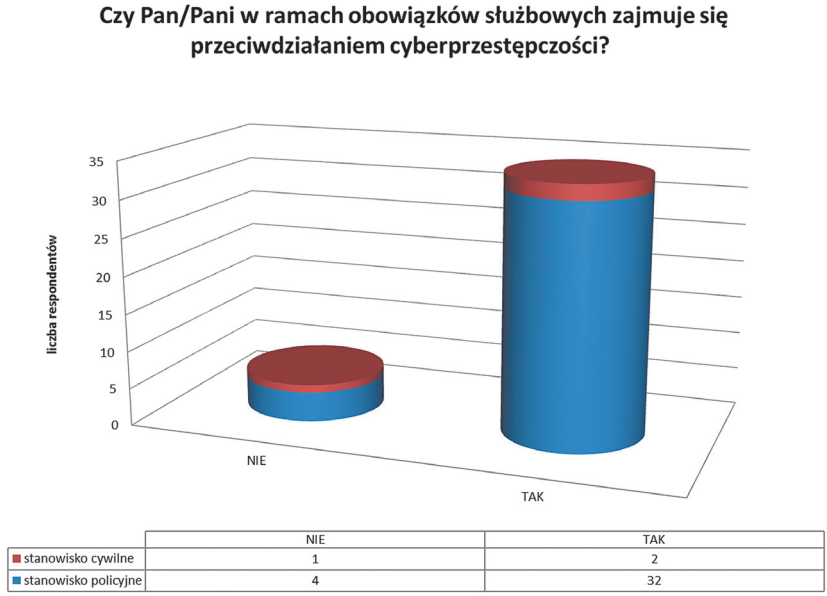
które w ramach obowiązków służbowych zajmują się bądź nie zajmują się przeciwdziałaniem cyberprzestępczości.

Tabela 5. Pracownicy Policji a rodzaj stanowiska respondentów badań ankietowych

Czy Pan/Pani w ramach obowiązków służbowych zajmuje się przeciwdziałaniem cyberprzestępczości?			
Rodzaj stanowiska	Nie	Tak	Razem
stanowisko policyjne	4	32	36
stanowisko cywilne	1	2	3
Razem	5	34	39

Źródło: badania własne

Wykres 5. Pracownicy Policji a rodzaj stanowiska respondentów badań ankietowych



Źródło: badania własne

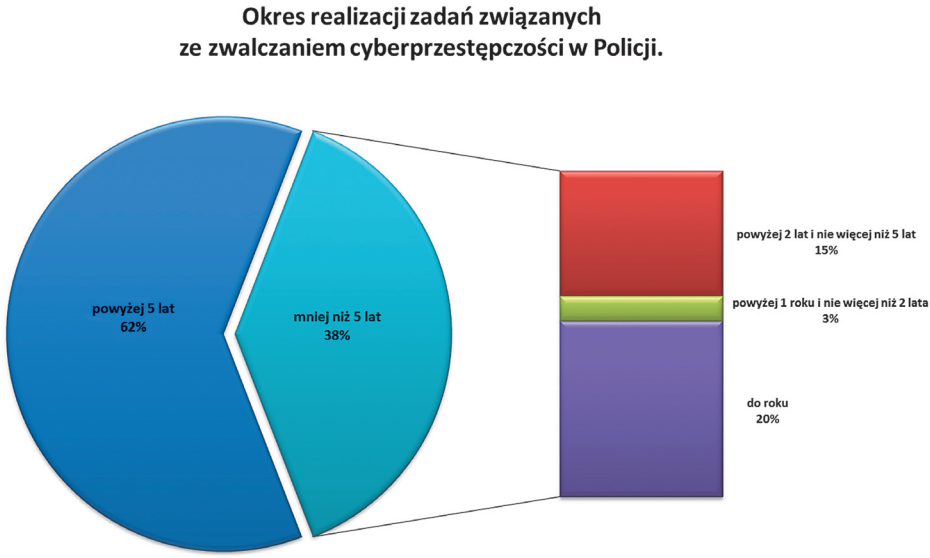
Dodatkowo, wśród pracowników Policji ważkim zagadnieniem było określenie doświadczenia, czyli czasu, przez jaki dana osoba zajmuje się przeciwdziałaniem cyberprzestępczości.

Tabela 6. Rodzaj stanowiska zajmowanego przez respondentów badań ankietowych

Czas zwalczania cyberprzestępczości w Policji	Liczba respondentów
powyżej 5 lat	21
powyżej 2 lat i nie więcej niż 5 lat	5
powyżej 1 roku i nie więcej niż 2 lata	1
do roku	7
Razem	34

Źródło: badania własne

Wykres 6. Rodzaj stanowiska zajmowanego przez respondentów badań ankietowych



Źródło: badania własne

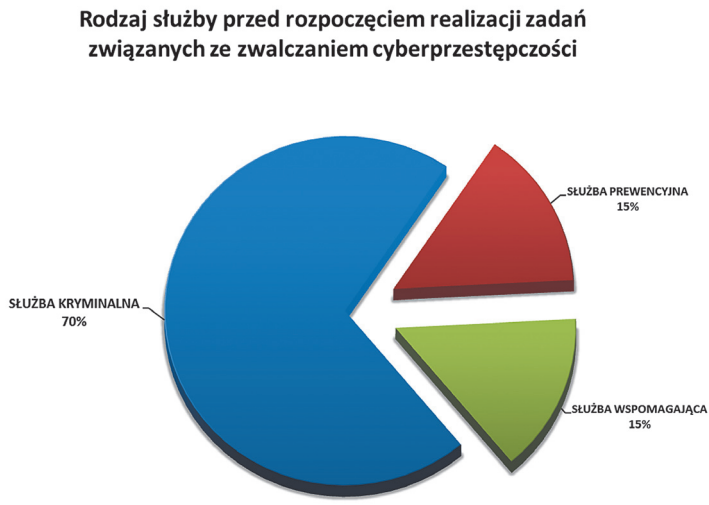
Ciekawym zagadnieniem, które warto poddać uwadze, jest to, jakie obowiązki osoby te pełniły przed rozpoczęciem służby i pracy związanej z przeciwdziałaniem cyberprzestępczości.

Tabela 7. Rodzaj stanowiska zajmowanego przez respondentów badań ankietowych

Rodzaj służby przed rozpoczęciem realizacji zadań związanych ze zwalczaniem cyberprzestępczości	Liczba respondentów
służba kryminalna	24
służba prewencyjna	5
służba wspomagająca	5
Razem	34

Źródło: badania własne

Wykres 7. Rodzaj stanowiska zajmowanego przez respondentów badań ankietowych



Źródło: badania własne

Uzyskane wyniki

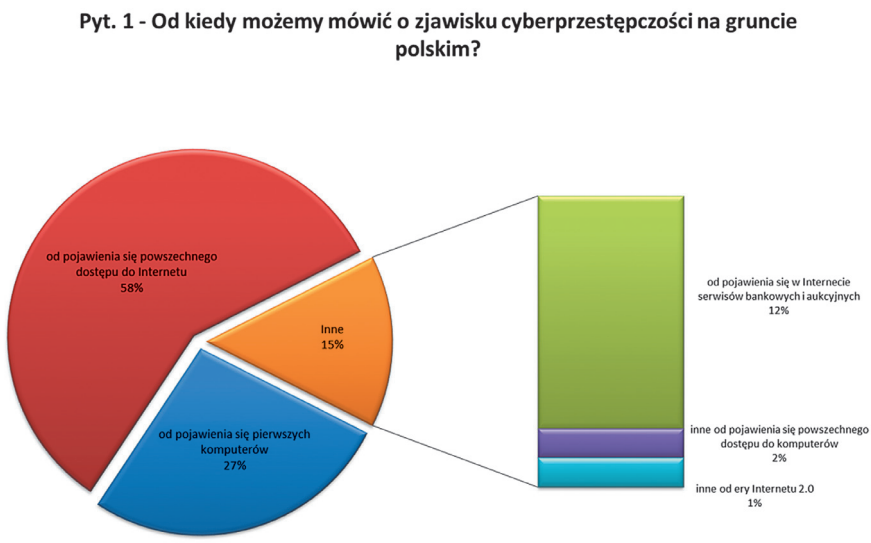
Zasadniczym pytaniem, które determinowało dalsze rozważania było rozumienie samego pojęcia cyberprzestępczości. W świetle istniejących problemów definicyjnych wynikających z różnorodnego podejścia do definiowania zjawiska, wyznaczania elementów przedmiotowo i podmiotowo istotnych dla bytu tego zjawiska, spodziewać się można było niejednorodnej odpowiedzi na to pytanie.

Tabela 8. Rozkład odpowiedzi na pytanie 1. ankiety

Pytanie 1. Od kiedy możemy mówić o zjawisku cyberprzestępczości na gruncie polskim?	Odpowiedzi
od pojawienia się pierwszych komputerów	18
od pojawienia się powszechnego dostępu do Internetu	39
od pojawienia się w Internecie serwisów bankowych i aukcyjnych	8
inne od pojawienia się powszechnego dostępu do komputerów	1
inne od ery Internetu 2.0	1
Razem	67

Źródło: badania własne

Wykres 8. Rozkład odpowiedzi na pytanie 1. ankiety



Źródło: badania własne

Co ciekawe, większość respondentów wskazuje na pojawienie się powszechnego dostępu do Internetu, jako wyznacznika wskazującego na pojawienie się cyberprzestępczości w Polsce. Trudno oprzeć się wrażeniu, że przedrostek „cyber" stanowi wyznacznik zjawiska, zaś przyjęte i funkcjonujące klasyfikacje, zarówno w Konwencji RE o cyberprzestępczości, jak i te wynikające z kodeksu karnego schodzą na plan dalszy wobec potocznego rozumienia zjawiska. Tylko 27% respondentów upatruje początków cyberprzestępczości z pojawieniem się pierwszych komputerów.

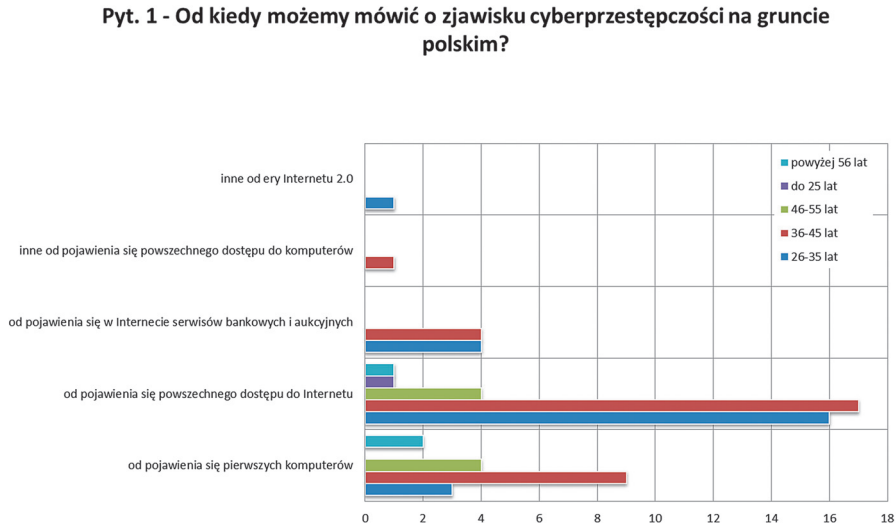
Ciekawy wydaje się przekrój odpowiedzi na to pytanie z uwzględnieniem wieku.

Tabela 9. Rozkład odpowiedzi na pytanie 1. ankiety a wiek respondentów

Odpowiedzi/przedział wiekowy	26–35 lat	36–45 lat	46–55 lat	do 25 lat	Powyżej 56 lat	Odpowiedzi
od pojawienia się pierwszych komputerów	3	9	4		2	18
od pojawienia się powszechnego dostępu do Internetu	16	17	4	1	1	39
od pojawienia się w Internecie serwisów bankowych i aukcyjnych	4	4				8
inne od pojawienia się powszechnego dostępu do komputerów		1				1
inne od ery Internetu 2.0	1					1
Razem	24	31	8	1	3	67

Źródło: badania własne

Wykres 9. Rozkład odpowiedzi na pytanie 1. ankiety a wiek respondentów



Źródło: badania własne

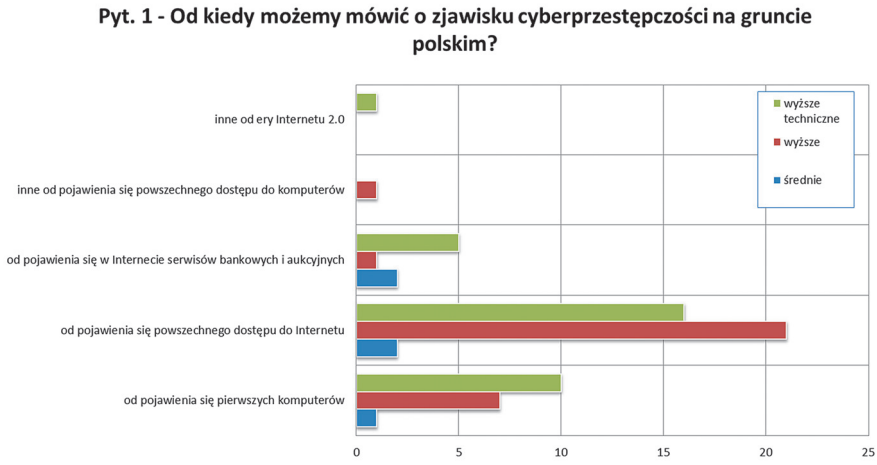
Co prawda rozkład odpowiedzi po przebadaniu testem χ^2 daje odpowiedź pozytywną, wiek miał związek z udzieloną odpowiedzią, to jednak po wyznaczeniu wartości współczynnika V-Cramera na poziomie 0,0605 widać, że siła tego związku jest statystycznie bardzo słaba, co przekłada się na możliwość jej pominięcia w rozważaniach. Oczywiście można postawić pytanie, czy wykształcenie ma wpływ na znajomość definicji zjawiska cyberprzestępczości.

Tabela 10. Rozkład odpowiedzi na pytanie 1. ankiety a wykształcenie respondentów

Odpowiedzi/przedział wiekowy	Średnie	Wyższe	Wyższe techniczne	Odpowiedzi
od pojawienia się pierwszych komputerów	1	7	10	18
od pojawienia się powszechnego dostępu do Internetu	2	21	16	39
od pojawienia się w Internecie serwisów bankowych i aukcyjnych	2	1	5	8
inne od pojawienia się powszechnego dostępu do komputerów		1		1
inne od ery Internetu 2.0			1	1
Razem	5	30	32	39

Źródło: badania własne

Wykres 10. Rozkład odpowiedzi na pytanie 1. ankiety a wykształcenie respondentów



Źródło: badania własne

Po przeprowadzeniu obliczeń hipoteza o braku związku została odrzucona na poziomie istotności p=0,05 zaś siła związku wyniosła (V-Cramer) 0,238, co wskazuje na jego niewielką siłę. Zarówno na podstawie obliczeń, jak i na podstawie obserwacji wykresu można stwierdzić, iż osoby z wykształceniem wyższym sytuują w większości pojawienie się cyberprzestępczości w Polsce wraz z pojawieniem się Internetu, zaś osoby z wykształceniem wyższym technicznym wraz z pojawieniem się pierwszych komputerów.

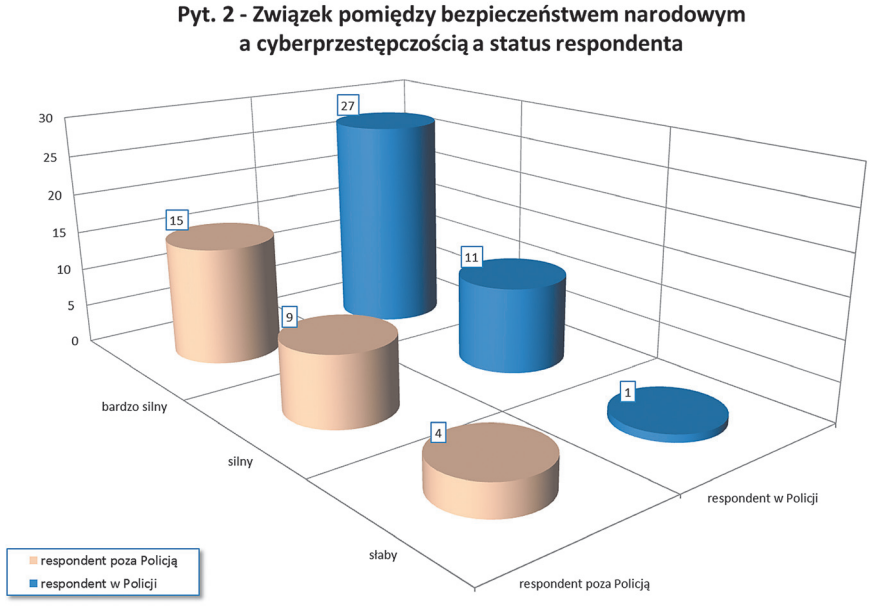
Pytanie drugie jest nie mniej istotne, gdyż odnosi się do szerszego rozumienia bezpieczeństwa oraz wpływu zjawiska cyberprzestępczości na bezpieczeństwo narodowe. Z racji zakładanego, różnego pojmowania bezpieczeństwa narodowego przez osoby pracujące w Policji, jak i poza nią, sporządzono analizę właśnie pod tym kątem. Zarówno obserwacja wykresu, jak i badania testem χ^2 dostarczają potwierdzenia wspomnianych założeń. Osoby pracujące w Policji widzą zjawisko cyberprzestępczości szerzej i dostrzegają możliwe oraz występujące zagrożenia dla bezpieczeństwa narodowego, które niesie ze sobą cyberprzestępczość.

Tabela 11. Rozkład odpowiedzi na pytanie 2. ankiety a status respondentów

Związek pomiędzy bezpieczeństwem narodowym a cyberprzestępczością	Respondent poza Policją	Respondent w Policji	Odpowiedzi
bardzo silny	15	27	42
silny	9	11	20
słaby	4	1	5
Razem	28	39	67

Źródło: badania własne

Wykres 11. Rozkład odpowiedzi na pytanie 2. ankiety a status respondentów



Źródło: badania własne

W rozpatrywanym przypadku siła związku jest znacząca, co potwierdza współczynnik V-Cramera na poziomie 0,455.

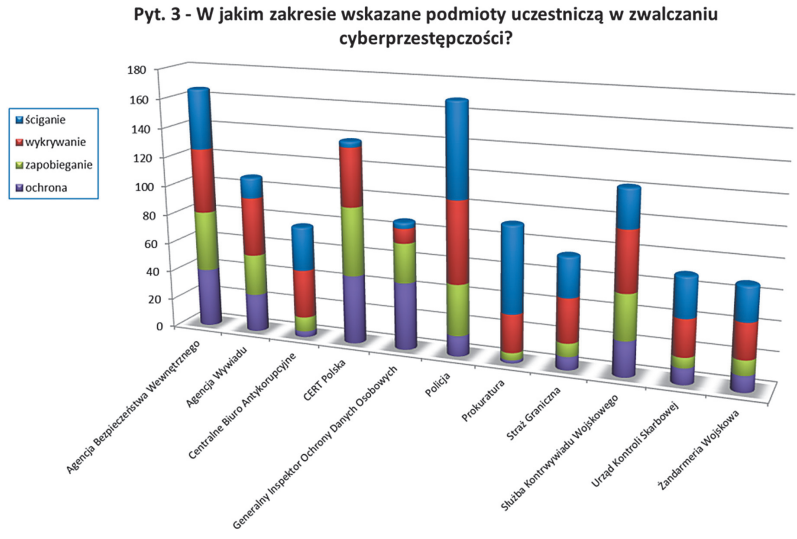
Pytanie trzecie dotyczyło zauważalnego miejsca i roli organizacji, które zdaniem autora mają swój znaczący wkład w przeciwdziałanie cyberprzestępczości. Na zadane pytanie „W jakim zakresie wskazane podmioty uczestniczą w zwalczaniu cyberprzestępczości?" rozkład odpowiedzi był następujący (tabela 12).

Tabela 12. Rozkład odpowiedzi na pytanie 3. ankiety

Podmioty uczestniczące w przeciwdziałaniu cyberprzestępczości	Ochrona	Zapobieganie	Wykrywanie	Ściganie
Agencja Bezpieczeństwa Wewnętrznego	59,70%	61,20%	65,70%	61,20%
Agencja Wywiadu	38,80%	41,80%	59,70%	20,90%
Centralne Biuro Antykorupcyjne	6,00%	14,90%	49,30%	44,80%
CERT Polska	70,10%	70,10%	59,70%	6,00%
Generalny Inspektor Ochrony Danych Osobowych	68,70%	40,30%	14,90%	6,00%
Policja	20,90%	52,20%	83,60%	95,50%
Prokuratura	3,00%	7,50%	38,80%	88,10%
Straż Graniczna	13,40%	13,40%	44,80%	40,30%
Służba Kontrwywiadu Wojskowego	35,80%	46,30%	61,20%	38,80%
Urząd Kontroli Skarbowej	16,40%	10,40%	37,30%	40,30%
Żandarmeria Wojskowa	16,40%	14,90%	35,80%	34,30%

Źródło: badania własne

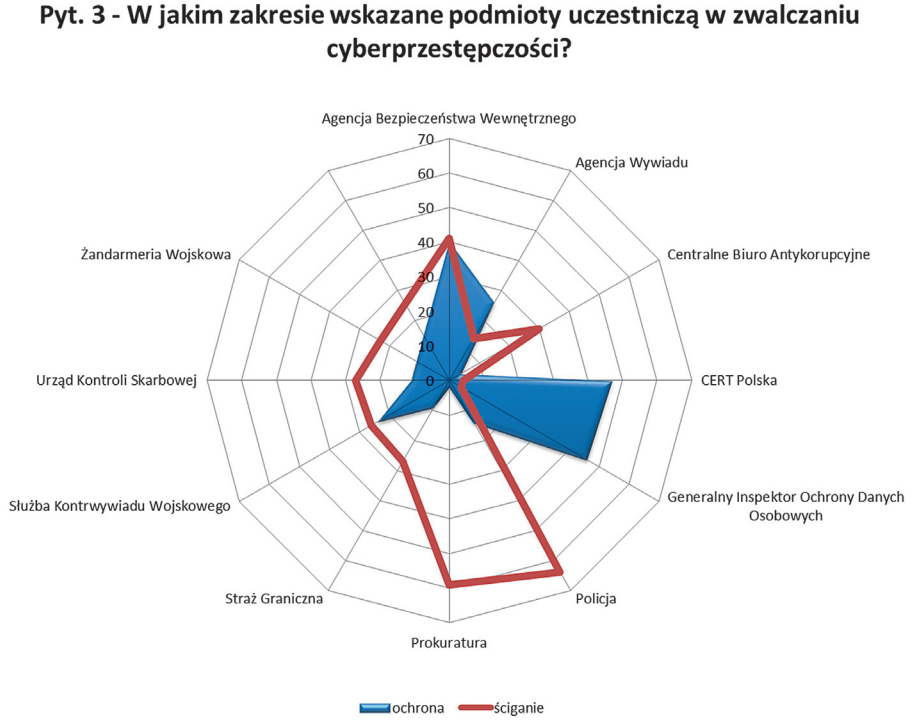
Wykres 12. Rozkład odpowiedzi na pytanie 3. ankiety



Źródło: badania własne

Widać wyraźnie, że zarówno Policja, jak i Agencja Bezpieczeństwa Wewnętrznego, to podmioty, które *per saldo* wybijają się na pierwsze miejsce w ogólnym zaangażowaniu. Jednak szczegółowa analiza pozwala na dalej idące wnioski.

Wykres 13. Rozkład odpowiedzi na pytanie 3. ankiety w odniesieniu do ochrony i ścigania

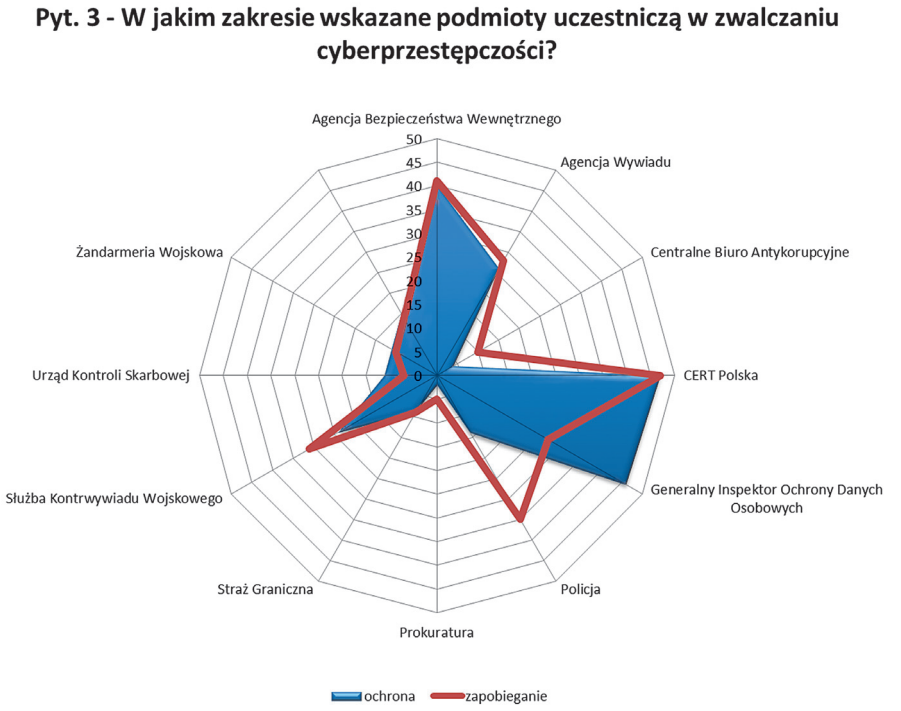


Źródło: badania własne

W odniesieniu do działań związanych z ochroną i ściganiem rysują się wyraźne różnice oraz specjalizacje poszczególnych podmiotów. I tak w opinii respondentów: ABW, GIODO i CERT stanowią szpicę, zaś CBA i prokuratura sytuują się na najniższym poziomie. W odniesieniu do ścigania Policja i prokuratura wiodą prym, zaś CERT i GIODO nie wykazują znaczącej aktywności.

Jeśli zaś analizować aktywności dotyczące zapobiegania na tle ochrony, to mamy do czynienia z sytuacją, którą obrazuje wykres 14. Na tle swoistej mizerii w tym zakresie, największe znaczenie respondenci przypisali CERT, który otrzymał „tylko" 70% wskazań. Należy wskazać, że funkcja ochrony, opisana w dokumentach strategicznych, winna być realizowana na wyższym poziomie, zaś CERT, Policja, ABW, SKW i AW winny być o wiele mocniej identyfikowane, jako podmioty, które zajmują się działaniami aktywnymi związanymi z szeroko rozumianą ochroną.

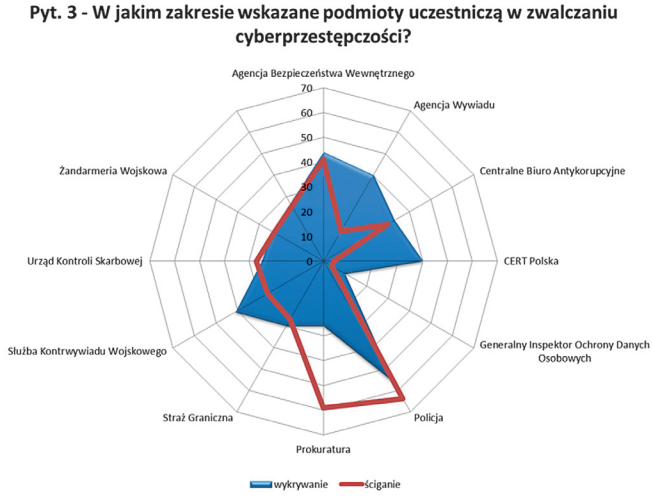
Wykres 14. Rozkład odpowiedzi na pytanie 3. ankiety w odniesieniu do ochrony i ścigania



Źródło: badania własne

Jeśli zaś przyjrzeć się szczegółowo rozkładowi odpowiedzi w odniesieniu do wykrywania i ścigania, to respondenci w odniesieniu do wykrywania plasują wysoko wiele podmiotów, jednak, co istotne prymat w zakresie wykrywania i ścigania dzierży Policja. Fakt ten nie dziwi, komentarza wymaga jednak pozycjonowanie Żandarmerii Wojskowej jako podmiotu, który na tle wymienionych razem z prokuraturą, Strażą graniczną i UKS w sposób nieznaczny zajmuje się procesem wykrywczym, co wymagałoby dodatkowych badań. Z racji, iż zarówno organizacja, jak i działania żandarmerii stoją na wysokim poziomie, jednak z racji zamkniętej sfery jej działania (Wojsko Polskie) wiedza o jej działaniach nie jest powszechna, nawet wśród ekspertów. Ciekawy jest jeden z komentarzy: „Należy rozgraniczyć co powinny robić (obowiązki) od tego co robią i w jaki sposób". W przypadku AW, CBA, SG, SKW i ŻW raczej w przypadku uzyskania informacji przekażą do innych właściwych służb", który świadczy o przekonaniu, że nie każdy z wymienionych podmiotów realizuje nałożone prawem obowiązki. Wynikać stąd może swoista gra sił, która prowadzi do zlecania realizacji procesu wykrywczego (postępowania karnego) wyspecjalizowanemu podmiotowi, jakim niewątpliwie jest Policja.

Wykres 15. Rozkład odpowiedzi na pytanie 3. ankiety w odniesieniu do wykrywania i ścigania



Źródło: badania własne

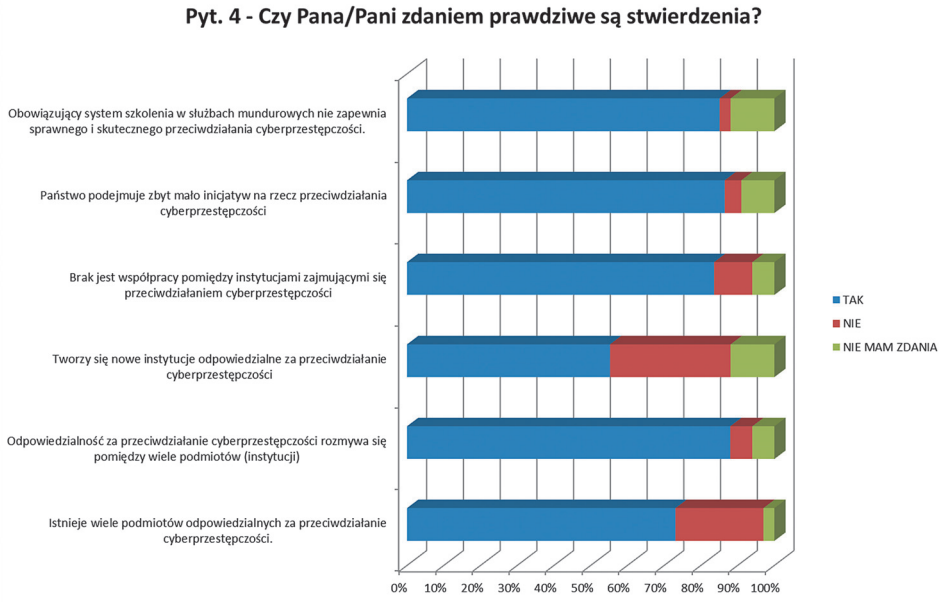
W pytaniu czwartym podjęto próbę zdiagnozowania stosunku ekspertów do wyrażonych poglądów w postaci sześciu twierdzeń, które dość często pojawiają się w przestrzeni publicznej, jednak nie poparte są kategorycznymi stwierdzeniami, na podstawie których można je uznać za prawdziwe.

Tabela 13. Rozkład odpowiedzi na pytanie 4. ankiety

Stwierdzenia/odpowiedzi	Tak	Nie	Nie mam zdania
Istnieje wiele podmiotów odpowiedzialnych za przeciwdziałanie cyberprzestępczości	73,10%	23,90%	3,00%
Odpowiedzialność za przeciwdziałanie cyberprzestępczości rozmywa się pomiędzy wiele podmiotów (instytucji)	88,10%	6,00%	6,00%
Tworzy się nowe instytucje odpowiedzialne za przeciwdziałanie cyberprzestępczości	55,20%	32,80%	11,90%
Brak jest współpracy pomiędzy instytucjami zajmującymi się przeciwdziałaniem cyberprzestępczości	83,60%	10,40%	6,00%
Państwo podejmuje zbyt mało inicjatyw na rzecz przeciwdziałania cyberprzestępczości	86,60%	4,50%	9,00%
Obowiązujący system szkolenia w służbach mundurowych nie zapewnia sprawnego i skutecznego przeciwdziałania cyberprzestępczości.	85,10%	3,00%	11,90%

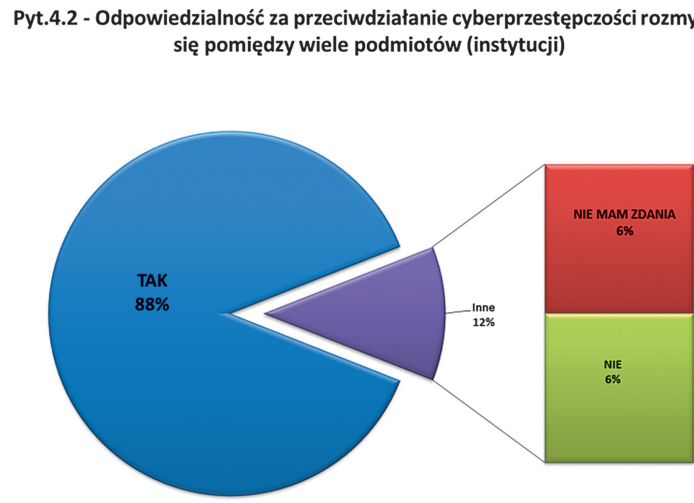
Źródło: badania własne

Wykres 16. Rozkład odpowiedzi na pytanie 4. ankiety



Źródło: badania własne

Wykres 17. Rozkład odpowiedzi na pytanie 4.2 ankiety



Źródło: badania własne

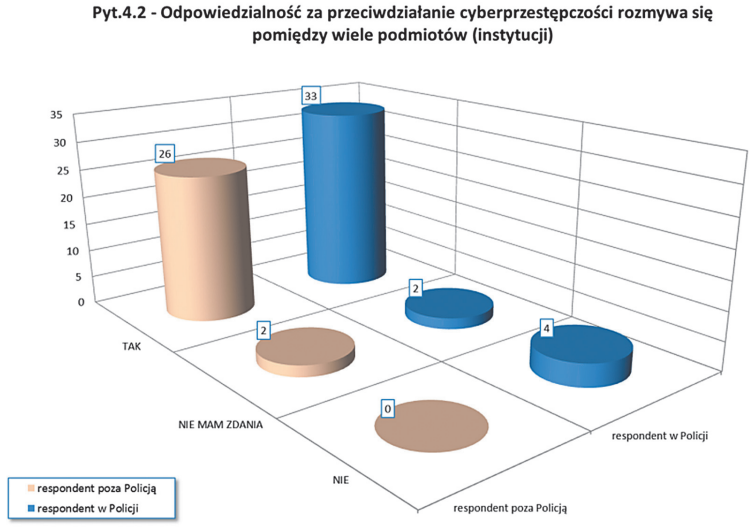
Na podstawie analizy odpowiedzi respondentów można stwierdzić, że mamy do czynienia z krytyką obecnego stanu rzeczy. Niekorzystne uwarunkowania

pogłębiają dodatkowo takie elementy, jak: brak współpracy oraz braki w przygotowaniu kadr zajmujących się przeciwdziałaniu zjawisku, które wyrażone są w komentarzach do tego pytania, np.: „Jeden kurs specjalistyczny. Uzyskiwanie informacji z Internetu to za mało" oraz „Działania Policji i prokuratury w zakresie ścigania cyberprzestępczości są iluzoryczne wobec skali zjawiska. Te działania niemalże nie istnieją w praktyce".

Niektóre ze stwierdzeń poddano bardziej wnikliwej analizie, aby zbadać związki pomiędzy rozkładem odpowiedzi z uwzględnieniem spojrzenia osób będących pracownikami Policji i tych, którzy nimi nie są. Dodatkowo we wskazanych poniżej przypadkach zbadano związek za pomocą testu χ^2 i wyznaczono jego siłę korzystając ze współczynnika V-Cramera.

W przypadku stwierdzenia „Odpowiedzialność za przeciwdziałanie cyberprzestępczości rozmywa się pomiędzy wiele podmiotów (instytucji)" zdecydowana część respondentów potwierdziła je.

Wykres 18. Rozkład odpowiedzi na pytanie 4.2 ankiety



Źródło: badania własne

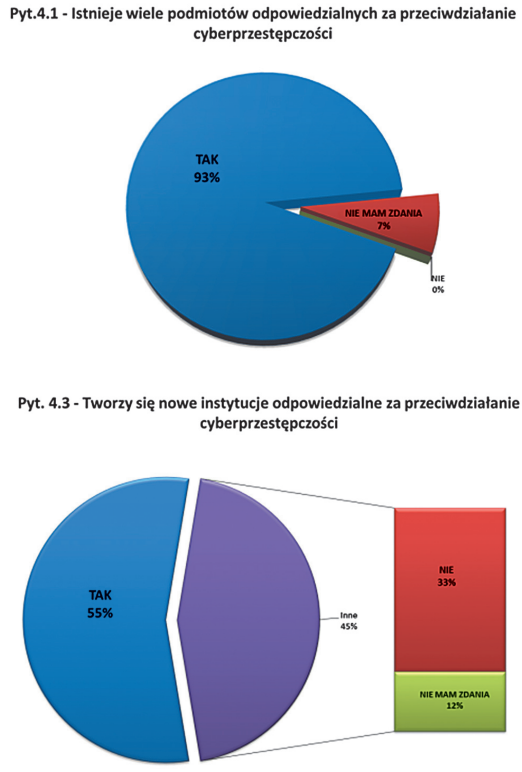
Obserwacja rozkładu odpowiedzi w zależności od tego czy respondent jest lub nie jest pracownikiem Policji, nie wskazuje wprost na związek pomiędzy statusem respondenta a udzieloną odpowiedzią. Po weryfikacji hipotezy za pomocą testu χ^2 na poziomie istotności 5,00% można przyjąć, że związek jest statystycznie istotny, zaś jego siła jest umiarkowana.

Oczywiście oprócz samego rozkładu odpowiedzi, ważniejsze jest to, iż eksperci widzą wiele podmiotów, które nie dość, że zajmują się przeciwdziałaniem cyberprzestępczości, to potwierdzają, że odpowiedzialność (w domyśle wynikająca z odpowiednich regulacji prawnych) „rozmywa się", co — niestety

— prowadzić może do swoistego chaosu, który nie sprzyja przeciwdziałaniu temu zjawisku.

Potwierdzeniem tej dość skomplikowanej sytuacji jest w większości akceptacja stwierdzenia: „Istnieje wiele podmiotów odpowiedzialnych za przeciwdziałanie cyberprzestępczości" oraz „Tworzy się nowe instytucje odpowiedzialne za przeciwdziałanie cyberprzestępczości".

Wykres 19. Rozkład odpowiedzi na pytanie 4.1 i 4.3 ankiety

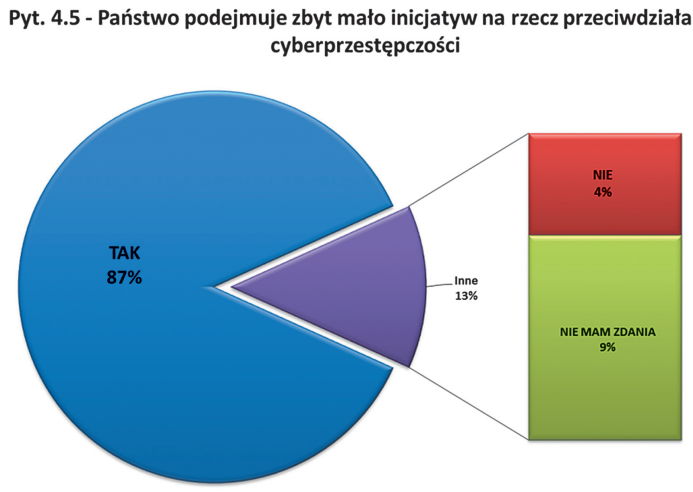


Źródło: badania własne

Co ciekawe, w jednym i drugim przypadku test χ^2 wskazuje na statystycznie istotny związek pomiędzy odpowiedzią na pytanie a przynależnością do Policji. W przypadku twierdzenia 4.1 aż 92,9% respondentów spoza Policji i 84,6% respondentów — pracowników Policji je potwierdza, a w przypadku twierdzenia 4.3 odpowiednio 42,9% i 64,1% odpowiedzi potwierdza jego treść.

Odpowiedzi na stwierdzenie obejmujące aktywność państwa w zakresie przeciwdziałania cyberprzestępczości widać wyraźnie, że jest ona (aktywność) oceniana bardzo nisko, a co za tym idzie występuje konieczność aktywizacji w tym zakresie.

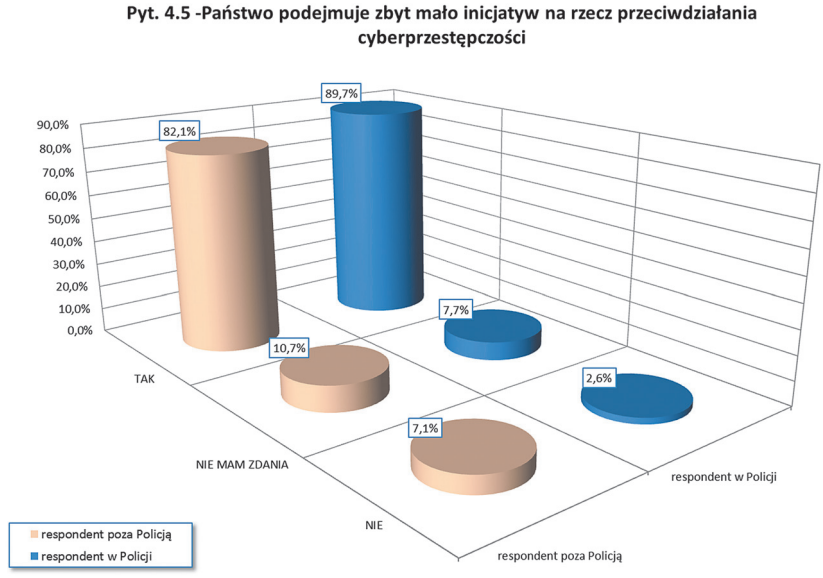
Wykres 20. Rozkład odpowiedzi na pytanie 4.5 ankiety



Źródło: badania własne

Co ciekawe, związek odpowiedzi na pytanie z zatrudnieniem w Policji jest statystycznie istotny, to jednak jest słaby, o czym świadczy wartość współczynnika V-Cramera na poziomie 0,1268.

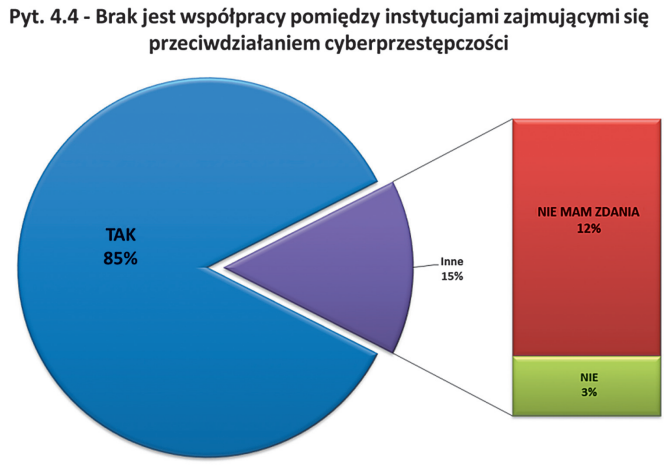
Wykres 21. Rozkład odpowiedzi na pytanie 4.5 ankiety



Źródło: badania własne

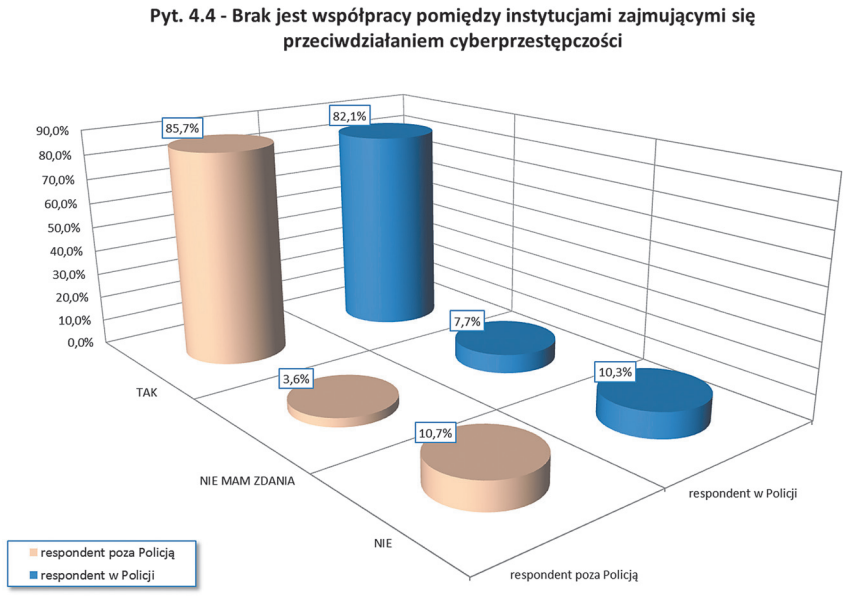
W przypadku zdania respondentów na temat współpracy pomiędzy podmiotami, które odpowiedzialne są za przeciwdziałanie cyberprzestępczości, dość jasno widać, że tej współpracy niestety nie ma, zaś rozkład odpowiedzi z uwzględnieniem statusu jest bardzo podobny.

Wykres 22. Rozkład odpowiedzi na pytanie 4.4 ankiety



Źródło: badania własne

Wykres 23. Rozkład odpowiedzi na pytanie 4.4 ankiety



Źródło: badania własne

Dalsza część badania miała na celu zdiagnozowanie roli, miejsca oraz funkcjonowania Policji na tle organizacji zajmujących się zwalczaniem cyberprzestępczości.

Zasadniczą kwestią, którą starano się wyjaśnić na początku, było zebranie odpowiedzi na pytanie, czy „Policja jest kluczową formacją, na której spoczywa obowiązek zwalczania cyberprzestępczości?".

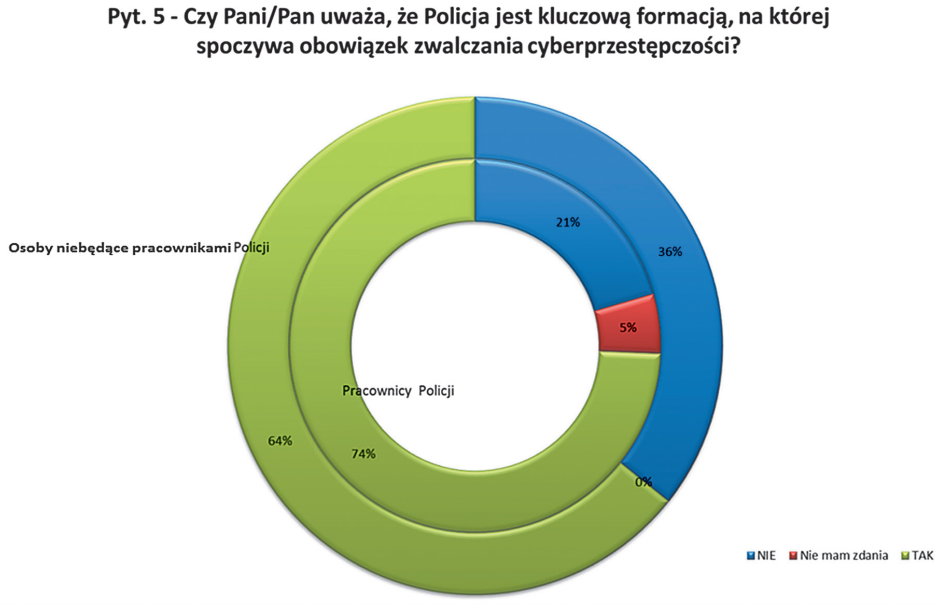
Prezentowany rozkład odpowiedzi potwierdza czołowe miejsce Policji.

Tabela 14. Rozkład odpowiedzi na pytanie 5. ankiety

Treść odpowiedzi	Respondent w Policji	Respondent poza Policją	Liczba respondentów
Nie	8	10	18
Nie mam zdania	2		2
Tak	29	18	47
Razem	39	28	67

Źródło: badania własne

Wykres 24. Rozkład odpowiedzi na pytanie 5. ankiety



Źródło: badania własne

Co ciekawe, wśród pracowników Policji panuje większe przekonanie o jej znaczeniu w zwalczaniu cyberprzestępczości, przy czym 5% respondentów nie miało zdania w badanej kwestii.

Uściśleniem pytania 5. jest kolejne z pytań, w którym respondenci oceniali działania Policji w trzech głównych obszarach działalności, a mianowicie w ochronie, ściganiu i współpracy w zwalczaniu cyberprzestępczości. Wydawać by się mogło, że skoro Policja jest kluczową organizacją zajmującą się zwalczaniem cyberprzestępczości, to jej funkcjonowanie we wszystkich trzech obszarach ocenione zostanie co najmniej jako poprawne, jednak wyniki badania nie okazały się tak wysokie.

Tabela 15. Rozkład odpowiedzi na pytanie 6. ankiety

Szczegółowa kategoria działalności	Bardzo dobrze	Dobrze	Słabo	Źle	Nie mam zdania
1. Ochrona (monitorowanie cyberprzestępczości)	6,0%	16,4%	31,3%	9,0%	7,5%
2. Ochrona (zapobieganie cyberprzestępczości)	4,5%	10,4%	31,3%	16,4%	7,5%
3. Współpraca krajowa — w zakresie przeciwdziałania cyberprzestępczości	6,0%	19,4%	29,9%	9,0%	6,0%
4. Współpraca krajowa — w zakresie ścigania cyberprzestępczości	9,0%	32,8%	19,4%	3,0%	6,0%
5. Współpraca międzynarodowa — w zakresie przeciwdziałania cyberprzestępczości	0%	4,5%	19,4%	34,3%	11,9%
6. Współpraca międzynarodowa — w zakresie ścigania cyberprzestępczości	0%	7,5%	20,9%	31,3%	10,4%
7. Ściganie cyberprzestępczości w kraju	4,5%	32,8%	25,4%	4,5%	3,0%
8. Ściganie cyberprzestępczości za granicą	0%	4,5%	13,4%	35,8%	16,4%

Źródło: badania własne

Po uogólnieniu wyników z tabeli 15 rozkład odpowiedzi można przedstawić następująco:

Tabela 16. Rozkład odpowiedzi na pytanie 6. ankiety

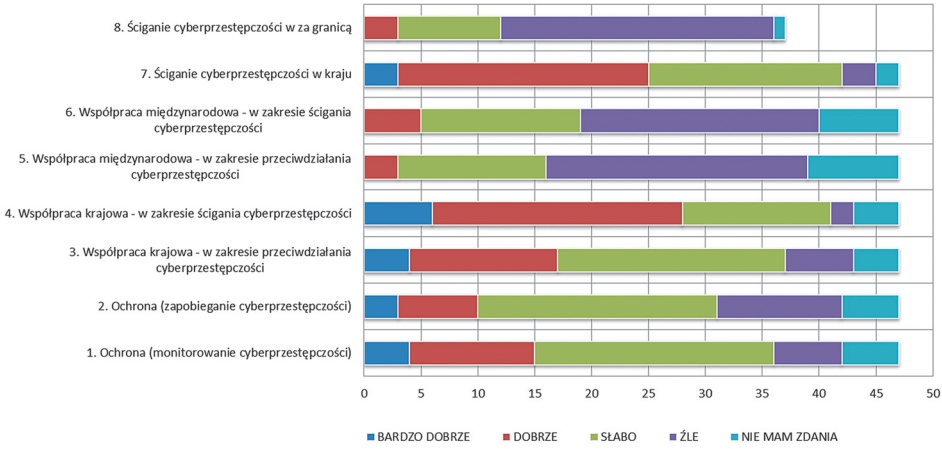
Uogólniona kategoria działalności	Bardzo dobrze	Dobrze	Słabo	Źle	Nie mam zdania
ochrona	5,22%	13,43%	31,34%	12,69%	7,46%
współpraca	3,73%	16,04%	22,39%	19,40%	8,58%
ściganie	2,24%	18,66%	19,40%	20,15%	2,24%

Źródło: badania własne

Graficzna prezentacja wartości zamieszczonych w tabelach 15 i 16 została zaprezentowana na wykresie 25.

Wykres 25. Rozkład odpowiedzi na pytanie 6. ankiety (kategorie szczegółowo)

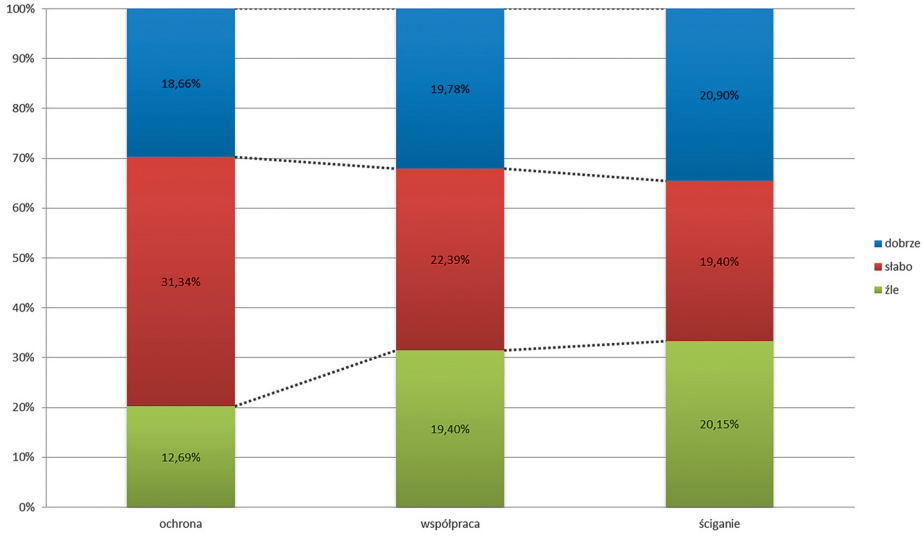
Pyt. 6 – Jak Pan/Pani ocenia działania Policji wśród podmiotów (na tle podmiotów) zajmujących się przeciwdziałaniem cyberprzestępczości?



Źródło: badania własne

Wykres 26. Rozkład odpowiedzi na pytanie 6 ankiety (kategorie uogólnione)

Pyt. 6 – Jak Pan/Pani ocenia działania Policji wśród podmiotów (na tle podmiotów) zajmujących się przeciwdziałaniem cyberprzestępczości?



Źródło: badania własne

Ocena Policji nie napawa optymizmem, współpraca krajowa i ściganie w kraju oceniane są najwyżej, jednak trudno podchodzić do tego wyniku optymistycznie, gdyż do takiej oceny skłonny jest tylko co trzeci badany, pozostałe dziedziny działalności oceniane są źle lub fatalnie.

W pytaniu 7 ankiety starano się znaleźć odpowiedź na to, jak oceniana jest praca Policji w reakcji na przestępstwa klasyfikowane jako cyberprzestępczość.

Tabela 17 prezentuje rozkład odpowiedzi na pytanie 7.

Tabela 17. Rozkład odpowiedzi na pytanie 7 ankiety

Szczegółowa kategoria działalności	Bardzo dobrze	Dobrze	Słabo	Źle	Nie mam zdania
1. Szybkość reakcji Policji na zgłoszenie o przestępstwie	7,5%	31,3%	37,3%	16,4%	7,5%
2. Profesjonalizm i fachowość policjantów	7,5%	34,3%	35,8%	16,4%	6,0%
3. Współdziałanie Policji z innymi podmiotami w zakresie pozyskania dowodów i ograniczania strat w wyniku działań niezgodnych z prawem	6,0%	32,8%	37,3%	17,9%	6,0%
4. Organizacja wydzielonych struktur zwalczających cyberprzestępczość	3,0%	22,4%	47,8%	20,9%	6,0%
5. Wyposażenie Policji w sprzęt i oprogramowanie specjalistyczne	0%	9,0%	40,3%	44,8%	6,0%
6. Wdrożone procedury związane z wybranymi typami cyberprzestępstw	0%	9,0%	40,3%	35,8%	14,9%
7. Czas załatwiania spraw (długość postępowań) prowadzonych przez Policję	0%	4,5%	43,3%	41,8%	10,4%
8. Przepływ informacji pomiędzy różnymi komórkami/jednostkami w Policji	0%	22,4%	35,8%	32,8%	9,0%
9. Współdziałanie Policji z innymi podmiotami zajmującymi się monitorowaniem cyberprzestrzeni i wykrywaniem przestępstw	0%	26,9%	40,3%	23,9%	9,0%

Źródło: badania własne

Podobnie jak w poprzednim przypadku ocena ta nie jest wysoka. Zastanawiające jest, że w przypadku oceny pracy samych policjantów, ludzi, którzy bezpośrednio realizują zadania wynikające z nałożonych przez ustawodawcę obowiązków ocena ta jest znacząco wyższa, aniżeli ocena organizacji (Policji), która powinna wyposażyć swoich pracowników w niezbędną wiedzę i umiejętności,